CIS Benchmarks

CIS Juniper OS Benchmark

v2.1.0 - 11-09-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This document, Security Configuration Benchmark for Juniper JUNOS Devices, provides prescriptive guidance for establishing a secure configuration posture for Juniper Networks Devices including a Core set of recommendations for all current JUNOS Platforms including ACX, EX, MX, PTX, QFX, SRX and T Series.

Additional configuration is suggested when securing some platforms. This Benchmark does not address topics such as SRX Security Policy and IPSEC VPN or EX/QFX Layer 2 Security and 802.1X configuration, however all Core Recommendations in this guide apply to these platforms. Additional Center for Internet Security Benchmarks to address additional requirements on these platforms will be released in the future or be included in a future version of this Benchmark.

Recommendations in this guide were tested extensively using a range of Juniper platforms including:

- SRX Series (SRX5400s (HA) running 15.1X49D100, SRX4100 (HA and stand alone) running 15.1X49D150, SRX300 running 15.1X49D150 and SRX110 running 13.3X48-D50, vSRX running 15.1X49D150 and 15.1X49D110)
- MX Series (MX240 running 15.1R7, vMX running 18.3R1.9)
- EX Series (EX2300 (VC and stand alone) running 15.1X53-D59)
- QFX Series (QFX5100 running 14.1X53-D47 (VCF), vQFX running 15.1X53-D63.9)

This guide does not address Juniper Networks platforms which do not run JUNOS, including ScreenOS Firewalls, Contrail, JSA Appliances or the Junos Space Network Management Platform.

To obtain the latest version of this guide, please visit http://cisecurity.org.

If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This guide is intended for individuals and organizations responsible for the security of Juniper Networks Devices running the JUNOS Operating System.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Level-I Benchmark recommendations are intended to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - do not negatively inhibit the utility of the technology beyond acceptable means

- **Level 2**

  Level-II Benchmark recommendations exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration.
The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Martin White Juniper Certified Instructor (JNCI), JNCIP-SEC, 3x JNCIS, 5x JNCIA, EC-Council C|ND Global Advisory Board, Martin White

Contributor
Darren Freidel
Martin White Juniper Certified Instructor (JNCI), JNCIP-SEC, 3x JNCIS, 5x JNCIA, EC-Council C|ND Global Advisory Board, Martin White

Recommendations

1 General Recommendations

This section provides general guidance on securing JUNOS Routers which does not apply to any particular hierarchy level or commands. These recommendations are not scored and do not provide any Audit advice.

This section is not intended to be a comprehensive source for non configuration related security considerations for JUNOS.

1.1 Ensure Device is running Current Junos Software (Manual)

Profile Applicability:

- Level 1

Description:

All JUNOS Devices should run the current Recommended Release of JUNOS.

Rationale:

As with any software, the JUNOS Operating System installed on Juniper Devices may be subject to Bugs, Instabilities and Security Vulnerabilities discovered over time.

Juniper periodically issues software patches for all Juniper Devices which are currently supported, and for which the operating organization has a valid support contract.

All JUNOS Devices in a production network should be kept up to date based on *Security Advisories* issued by the *Juniper Networks Security Incident Response Team (SIRT).*

SIRT publishes non-urgent *Security Bulletins* on a predefined quarterly schedule, but may also issue *out-of-cycle Security Advisories* in response to more urgent events such as malicious exploitation of Zero Day vulnerabilities, as described in Juniper Knowledge Base Article KB16613.

A list of Security Advisories can be viewed on the Juniper Knowledge Base here or as an RSS Feed here. No login is required, but additional information is available to users with a Juniper CSC or SSO account.

If you have a Login to the Juniper Customer Portal, you can Subscribe to Knowledge Base articles or to SIRT Security Advisories for your platform/s by going to the *Manage My*

Subscriptions section. You can also subscribe the RSS Feed to be notified of new Security Advisories without any login being required.

Organizations which utilize the Junos Space central management platform can use Service Insight to get proactive notifications for SIRT Advisories and End of Life Notifications impacting their managed, supported systems.

All administrators responsible for management of Junos devices should ensure that they have a process to keep up to date on SIRT Security Advisories and apply necessary patches in a timely manner.

For new device deployments, Juniper provide a regularly update list of supported Junos Software called the *Junos Software Versions - Suggested Releases to Consider and Evaluate* (formally known as the *JTAC Recommended Release*).

The Suggested Release is specified for each currently supported platform in Juniper Knowledge Base Article KB21476 and is intended as a starting point to help customers select a Junos Software version that meets their deployment needs and can be readily supported by JTAC should assistance be required.

The Junos Software Versions - Suggested Releases to Consider and Evaluate Knowledge Base article is regularly updated by Juniper and typically reflects current Security Advisories at the time of posting, but it is **strongly recommended** that administrators using the Suggested Releases as a starting point **should always check for any subsequent Security Advisories** which may have been issued in the interim to select the best version to deploy.

Impact:

During updates JUNOS Devices reboot to load the new software. In some instances this may result in loss of service. Please refer to the documentation for your platform *before* attempting to update software.

Audit:

This is an example process for deploying a new Junos device or for implementing patch management for the first time within an existing network.
For Junos systems already deployed in a production network, SIRT Security Advisories should be used to determine when additional patches are required on an ongoing basis.
Step 1: Collect the router chassis information

```
user@host> show version | match model
```

Example:

```
root@LAB-SRX300> show version | match model
Model: srx300
```

This device is an SRX300

Step 2: Check the software version running on the device

```
user@host> show version | match JUNOS
```

Example:

```
root@LAB-SRX300> show version | match JUNOS
Junos: 15.1X49-D150.2
JUNOS Software Release [15.1X49-D150.2]

root@LAB-SRX300>
```

For some devices, such as MX Routers, a large number of software components will be returned from the previous command. This can be filtered by looking for the "JUNOS Base" software

Example:

```
user@LAB-MX> show version | match "Base"

JUNOS Base OS boot [10.4R8.5] JUNOS Base OS Software Suite [10.4R8.5]
```

The Base OS software version on this MX Router is Junos 10.4R8.5

Step 3: Confirm that the installed Junos Release is still supported by Juniper

Visit Junos OS Dates & Milestones, where Juniper maintain a list of the support periods (during which Security Advisories and patches will be issued) for each Junos release.

Step 4: If the installed release has reached *End of Engineering* (EoE), select replacement release:

When a product or software release reaches the *End of Engineering (EoE)* date, it will no longer be actively maintained by Juniper and no new patches or other releases will be issued.

In selecting a replacement the *Junos Software Versions - Suggested Releases to Consider and Evaluate* will be used as a starting point in most deployments. The current Junos Software Versions - Suggested Releases to Consider and Evaluate can be found in http://kb.juniper.net/InfoCenter/index?page=content&id=KB21476&cat=&actp=LIST, and is regularly updated by Juniper.

Alternatively, you may wish to used *Juniper Pathfinder* tool at https://https://pathfinder.juniper.net/ to select a release that supports the features required by your environment.

Step 5: Check for any Juniper Security Incident Response Team (SIRT) Security Advisories which apply to the selected release:

Juniper Security Advisories can be found on the Knowledge base at https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

If the Junos device is running a supported version *and* no SIRT Security Advisories apply, the device is compliant.

Example Process:

The SRX300 shown in the sample output above is running Junos version 15.1X49-D150.2. Checking the *Junos OS Dates & Milestones* page, we find that the 15.1X49 release reaches End of Engineering on 31st December 2020.

I am checking in June 2020, so at the time of writing this version is still supported. However newer versions with improved features are available, so I opt to look at the Junos Software Versions - Suggested Releases to Consider and Evaluate Knowledge Base article.

The Suggested Release for the SRX300 is currently Junos 18.4R3-S2 and this was last updated on the 24th of April 2020.

Finally, I will check for Security Advisories applying to the SRX300 since this date. At the time of writing the most recent Security Advisory that applies was JSA11021.

Looking at the advisory we can see that this applied to "18.4 versions prior to 18.4R1-S7, 18.4R3-S2", so the current JTAC Recommended Release includes this patch and would be compliant with this recommendation. I can request this software image from Juniper or from my Support Partner.

If I wanted to stay on the 15.1X49 release, then the same advisory informs me that "15.1X49 versions prior to 15.1X49-D211, 15.1X49-D220" are impacted, so I could alternatively request this release from Juniper and remain complaint with this recommendation.

Remediation:

Software patching procedures may vary between different platforms or organizations and can be accomplished using the CLI, the JWeb GUI, centrally through Junos Space or other management platforms.

To update a standalone JUNOS Device through the CLI, first upload the desired software image (downloaded from Juniper or your Support Partner) to the JUNOS Device in the `/var/tmp/` folder.

In most cases an upgrade is performed with the following command, issued from Operational Mode:

```
user@host> request system software add /var/tmp/<image name>
```

Where <image name> is the filename of the JUNOS image provided by Juniper.

NOTE - *Updating JUNOS Software with this command* ***will result in a reboot*** *of the system*

and loss of service.
In platforms deployed with redundant Routing Engines, as Virtual Chassis or as HA Clusters, an In-Service Software Updates (or ISSU) *may* be supported. An ISSU update updates and reboots each node or RE separately, failing services on to the other node/RE prior to the reboot.
To perform an ISSU Update, on most platforms, issue the following command from Operational Mode:

```
user@host> request system software in-service-upgrade /var/tmp/<image name>
```

NOTE - *The specific procedure and prerequisites for ISSU varies by platform and deployment type. If some prerequisites (such as NSR or GRES) are not correctly configured **a loss of service** may still occur.*
Please refer to the documentation for your platform and network enviroment *before* attempting to update software.

Default Value:

JUNOS Devices do not always ship with the current JTAC Recommended Release or latest Software Patches installed.

References:

1. https://kb.juniper.net/InfoCenter/index?page=content&id=KB21476
2. https://kb.juniper.net/InfoCenter/index?page=content&id=KB16613&actp=METADATA
3. https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES
4. https://kb.juniper.net/InfoCenter/index?page=rss&channel=SECURITY_ADVISORIES&cat=SIRT_1&detail=content
5. https://support.juniper.net/support/eol/software/junos/#11

Additional Information:

Devices must not be End of Life (EoL)/End of Engineer (EoE) and a valid, current Juniper Support Agreement is required for access to JUNOS Software Updates.

CIS Controls:

Version 7

11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices
Install the latest stable version of any security-related updates on all network devices.

1.2 Ensure End of Life JUNOS Devices are not used (Manual)

Profile Applicability:

- Level 1

Description:

EoL JUNOS Devices should never be used in production networks

Rationale:

As with most vendors, Juniper Networks only support individual versions of Software and Hardware for a certain period of time in order to allow resources to be spent developing new products, rather than supporting old ones and because new features and technologies may not be supportable on older hardware.

Juniper will announce that support for a device, software version or platform is being discontinued by issuing an *End of Life Notice* for the product being retired. A typical EOL Notice will include details of:

- *Notification Date* - The official date that the EOLN was issued, all other timings are based on this date.
- *LOD* - the Last Order Date for the product - typically this is 180 days after the EOLN. After LOD, no *new* support services or contracts for the product can be purchased.
- *LSV* - the Last Software Version which will be supported for the product
- *EOSE* - the End of Software Engineering. After this date Juniper will not offer new bug fixes or software patches for the product. Typically this is 3 years after the EOLN.
- *LRD* - the Last Renewal Date. After this date, existing support contracts and services for the platform can no longer be renewed. Typically this is 4 years after the EOLN.
- *EOS* - the End of Support. Juniper will no longer provide any support or replacements for the platform. Typically this is 5 years after the EOLN.

Once a device has reached EOSE state, Juniper may no longer offer any patches, bug fixes or *fixes for security vulnerabilities*. This makes the device essentially unsupportable in a production environment, as any serious vulnerability discovered could not be patched.

It may not be practical in most cases to provide a work around without impacting services and it is rarely possible to instantly retire or replace affected platforms in response to a newly discovered vulnerability. This would leave networks vulnerable with no prospect of a timely fix.

You can confirm the current support status of your device by going to the Juniper Serial Number Entitlement Tool and entering the device Serial Number/s. Note, you may need to add columns to the default output to display EoL and EoS status.

You can also search End of Life Notices by platform or software version from the Juniper End of Life Products & Milestones page

Impact:

EOL Devices of any type present a significant risk to the security of the network.

Audit:

It is essentially that administrators follow Juniper EOLN announcements and plan to retire all EoL platforms following the timeline given in the EOLN by the EOSE date to ensure that this situation does not occur.
You can subscribe to EOL Notices in the Juniper Knowledge Base by logging in with your Juniper Customer Account, navigating to "Manage Subscriptions" and adding "EOL" to "Technical Bulletins" Subscriptions. Juniper will automatically email you a notification when a new EOLN is issued.
A full list of current EOLNs is also available here: https://support.juniper.net/support/eol/

Remediation:

Administrators should plan to retire all JUNOS Devices before they reach EOS/EOSE

References:

1. https://support.juniper.net/support/pdf/eol/990833.pdf
2. https://support.juniper.net/support/eol/
3. https://entitlementsearch.juniper.net/entitlementsearch

CIS Controls:

Version 7

2.2 Ensure Software is Supported by Vendor
Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

1.3 Ensure device is physically secured (Manual)

Profile Applicability:

- Level 1

Description:

Network Devices should be physically secured.

Rationale:

As with most information assets, it is vital that an attacker is prevented from gaining physical access to your Juniper JUNOS Devices.

With physical access an attacker may bypass firewalls by re-patching systems, power off your Device or connect to Console ports.

It is possible with almost all network equipment to reset the Root password if you have physical access.

Recommendations elsewhere in this document provide some mitigation against these attacks by, for example, Encrypting Configuration files and disabling Auxiliary Ports, but preventing or detecting physical access to your network devices should still be a fundamental element of a defense in depth strategy.

Audit:

Remediation:

While preventing all physical access is nearly impossible in some deployment scenarios, such as for a Service Provider supplying Customer Premises Equipment (CPE), in most cases the following minimum steps should be considered:

- The JUNOS Device should be deployed in a secure, locked room.
- Access logs should be maintained for the room, either electronically through use of access cards or through a manual process for access to the key.
- Access to the room should be limited to only those personnel absolutely required.
- Use of CCTV to monitor sensitive areas and comms rooms.
- The room should ideally be equipped with Uninterruptible Power Supply (UPS) and cooling facilities as well as be free from Electromagnetic Interference sources. Loss of power (either malicious or accidental) or cooling can result in a loss of service.

These methods should be a bare minimum and other physical security options considered when protecting a JUNOS Device which processes or transits sensitive data, such as

Encryption Keys, Credit Card or Personally Identifiable Information which may be in scope for regulatory/industry compliance standards such as PCI DSS, GDPR or HIPAA.
In these situation Secure Hosting or Co-Location Facilities may be required and options considered for Physical Security should include:

- 24/7 Security Guards and Monitoring
- Biometric and/or Multi Factor access control
- Private Caged areas for secure equipment
- Additional alarm and monitoring systems to detect equipment being removed from racks

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 9
2. Router Security Configuration Guide, Version 1.1b, Section 3.1.1 (page 33), National Security Agency (NSA)

Additional Information:

This is not an exhaustive list of Physical Security measures, this recommendation is intended to highlight that if configuration is heavily secured, an attacker may be able to bypass some or all of these protections by obtaining physical access to the device or its connections.

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

1.4 Ensure configuration is backed up on a regular schedule (Manual)

Profile Applicability:

- Level 1

Description:

Regular backups should be made of the router.

Rationale:

Backups of a routers configuration may be necessary when recovering from physical hardware failure, administrative errors or a successful attack. Preserving the evidence of an attack may also be necessary for regulatory compliance, forensic investigation or prosecution of the attacker.

By default, JUNOS routers save a local backup copy of your configuration every time you commit (save) a change. JUNOS maintains the 50 previous configuration files, 4 on the Routing Engines Flash drive and the remainder on the hard disk.

This provides a useful method to recover from many types of fault or error, however an attacker will, potentially, be in a position to compromise these backups along with the active configuration, so it is vital that you also keep a remote configuration backup beyond the attackers reach.

Audit:

Remediation:

A discussion of all possible backup methods is beyond the scope of this Benchmark. Consider the Archival section of this Benchmark for one method of obtaining remote backups whenever your configuration is changed.
CVS tools such as RANCID provide an alternative method to backup and manage configuration files from a central location as well as keeping track of changes over time.
Also consider a method of maintaining offline copies of your backup data, such as tape storage. This provides a vital tool in Disaster Recovery and is also extremely helpful when recovering from a successful attack, as you can be certain that the attacker was unable to alter the offline version.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 3.3.4 (page 45), National Security Agency (NSA)

CIS Controls:

Version 7

10.1 Ensure Regular Automated Back Ups
Ensure that all system data is automatically backed up on regular basis.

1.5 Ensure backup data is stored and transferred securely (Manual)

Profile Applicability:

- Level 1

Description:

Backups of router configuration should be secured.

Rationale:

If an attacker has access to your router configuration files they have gained a lot of sensitive information about your network topology, defenses, weaknesses, critical servers and possibly your VPN keys and login information.

Audit:

Remediation:

A discussion of securing your backup services is beyond the scope of this Benchmark, but at a minimum you should consider the following:

- Never transfer configuration files using plain text protocols such as Telnet or FTP. Use SSH or SCP instead.
- Restrict access to backups to the least number of administrative users possible.
- Store offline backups in a physically secure, fire resistant, air tight safe.
- Log access and changes to backups.
- Secure any server that stores backups using the appropriate Center for Internet Security Benchmark.
- Disable all unused services on the backup server.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 3.3.4 (page 45), National Security Agency (NSA)

CIS Controls:

Version 7

10.4 Ensure Protection of Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

1.6 Ensure maximum RAM is installed (Manual)

Profile Applicability:

- Level 1

Description:

The router should have the maximum RAM installed.

Rationale:

Some Denial of Service attacks rely on exhausting the target routers memory resources by bombarding the router with bogus requests or traffic, when the router runs out of memory it will stop being able to service genuine requests and may be unable to perform critical tasks like maintaining route tables.

Juniper routers are somewhat more resilient to this type of attack then some other systems due to the separation of the Control and Forwarding planes, but attacks against router services may still cause disruption.

Audit:

Remediation:

Installing the most RAM available for your system will both help to mitigate these attacks and boost performance of your routers. In most cases RAM upgrades are extremely cost effective way to increase router performance and survivability.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 3.1.1 (page 34), National Security Agency (NSA)

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

1.7 Ensure logging data is monitored (Manual)

Profile Applicability:

- Level 1

Description:

Logs and events should be monitored.

Rationale:

Even after you have applied all of the settings in this guide, there is no such thing as perfect security. All systems are potentially vulnerable, be it to undiscovered software bugs, social engineering or other risks.

System logs, SNMP traps and any other information generated by your network devices should be monitored for changes and suspicious activity at least daily. Remember that your TACACS+ or RADIUS server may also produce logs detailing logins and what commands users issue.

If your systems produce more logging then you can actively monitor, consider using a Security Information and Event Manager type system. SIEM software consolidates and analyzes log information from across your organization, detecting security incidents and providing detailed, joined up information to aide your incident response and investigation.

Some popular SIEM systems include:

- Juniper Secure Analytics (JSA)
- RSA NetWitness
- IBM QRadar (Which is also the basis of the Juniper JSA product)
- AlienVault USM
- OSSIM (now also operated by AlienVault)
- Splunk

This is not intended as a recommendation of individual SIEM or SIM products, nor as an exhaustive list.

Audit:

Remediation:

References:

1. Watch your Internet Routers!, Internet Storm Center Diary, SANS Institute https://isc.sans.org/diary.html?storyid=6100
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.6

CIS Controls:

Version 7

6.6 Deploy SIEM or Log Analytic tool
Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.7 Regularly Review Logs
On a regular basis, review logs to identify anomalies or abnormal events.

1.8 Ensure Retired JUNOS Devices are Disposed of Securely (Manual)

Profile Applicability:

- Level 1

Description:

JUNOS Devices must be disposed of securely

Rationale:

As with all systems, there will come a point where a JUNOS Device has reached the end of it's service and must either be redeployed, recycled or disposed of.

JUNOS Devices used in production will typically contain a significant store of sensitive information, which may include:

- Configuration details about your network and services
- Sensitive or Personal data traversing the network, stored in packet captures, trace output or log files
- Hashed Passwords and Shared Secrets for users, management platforms or Virtual Private Networks
- Encryption Keys and other sensitive keying material used for IPSEC VPNs, X.509 Certificates or other uses

Attackers may attempt to gain information on potential targets or sensitive data by acquiring retired network devices and servers through theft, recycling services or online auctions. It is not uncommon to purchase used JUNOS Devices on sites like Ebay and find that the old configuration, encryption keys, licenses and other details are still present.

Audit:

Remediation:

To ensure that sensitive data is not lost when disposing of or redeploying retired JUNOS Devices, it is essential that the system be fully *zeroized*. This process returns the system to its original factory default state, with no root password set and all configuration, backups, user specified options, encryption keys, etc deleted.
To zeroize a JUNOS Device, log in as a user with the `maintenance` permission or as `root` and issue the following command from Operational Mode:

```
root@host>request system zeroize media
```

The `media` option used above also undertakes a process to securely "scrub" onboard memory and persistent media (such as flash, HDDs or SSDs) using a method equivalent to "clearing" as specified in NIST SP800-88. Using the `media` option will take significantly more time, as it repeatedly overwrites every area of storage with random data, but is strongly recommended for all devices where the option is supported.

An increasing number of JUNOS Devices, such as the PTX5000 Series and some MX Series routers, utilize a Disaggregated JUNOS Operating System which hosts JUNOS as a Virtual Machine abstracting it from the physical Routing Engine hardware. In some instances the `request system zeroize` command will zeroize the Guest JUNOS VM *only*, and not the underlying Host OS. For these platforms the following command should be used from Operational Mode:

```
root@host>request vmhost zeroize
```

This command will clear both the JUNOS VM and the Host OS.

When some devices, such as EX or QFX Series, are deployed in Clusters, HA or Virtual Chassis environments the `request system zeroize media` command may be ignored or may operate on only the local node, so will need to be issued individually on each device being disposed of.

Ensure you check the current documentation for the `request system zeroize` command for your platform to ensure that all options are correctly specified and perform the operation as intended.

Where possible, devices which are being "returned to base" from a deployment using third parties for transport should be zeroized before shipping.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/request-system-zeroize.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

2 Firewall

All JUNOS Devices provide Stateless, per-packet Firewall functionality for IPv4, IPv6 and MPLS traffic.

In some environments a Router may be used to filter ingress or egress traffic for the network, although more often a Stateful Firewall such as the a Juniper SRX will perform this function while also providing additional Security Services. Junos Firewall filters may also be used to protect the Junos device itself.

Filters are applied inbound or outbound to an interface for each unit and address family.

When applied to a traffic interface the firewall inspects *Transit Traffic* traversing the Junos device through that interface.

When applied to a Loopback interface (`Lo0.x`), the Filter inspects *Exception Traffic* sent to or from the *Routing Engine*, no matter which physical interface it was actually received on.

Firewall Filters are configured under the `[edit firewall]` hierarchy.

A full discussion of Firewall Filter configuration is beyond the scope of this Benchmark, but is covered in detail in the *Designing Firewall Filters* and *Firewall Filter Building Blocks* sections of the Juniper DayOne Book "Hardening Junos Devices, 2nd Edition" which is available for free from the Juniper website.

Network Engineers have historically viewed adding Firewall Filters to routers and other non-Firewall network devices with trepidation, worried about unintended consequences. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the Day One: Juniper Ambassadors' Cookbook 2019 provides an in-depth discussion of deploying Firewall Filters without impacting on services, and is also available for free from the Juniper website.

2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine (Manual)

Profile Applicability:

- Level 1

Description:

Traffic to the Routing Engine should be filtered.

Rationale:

JUNOS Devices can provide a wide range of services to the network and, as with any computer system, the more services that are offered and the more hosts to which they are available, the wider attack surface is offered to a potential attacker.

To help protect the Junos Device from attack a *Firewall Filter* should be applied to all inbound traffic, restricting the services available and the hosts trusted to connect to them. Filtering traffic also removes potential resource usage, processing unwanted traffic or unused services.

On Junos, *Transit Traffic* (traffic passing *through* the Junos Device) is processed by the *Data Plane* (often referred to as the PFE). Traffic destined to the Junos Device itself, such as SSH sessions, SNMP Polling or Routing Protocol updates, is known as *Exception Traffic*.

Exception Traffic is passed to the *Routing Engine*, which is represented by the *Loopback* interface *Lo0*, for processing. By default traffic received on any interface to an address owned by the Junos Device will be passed to the RE and can connect to a service, such as SSH, if it is running.

By applying a Firewall Filter to inbound traffic on the Loopback interface, we can filter traffic to the RE arriving on any interface (whether a transit interface or a dedicated Out of Band Management Interface like *fxp0*). This Firewall Filter is commonly referred to as a "Protect RE" filter and is often named as such, though does not have to be.

Filters should be applied for every address family configured on the Junos Device. For example, a Router configured with both IPv4 (family *inet*) and IPv6 (family *inet6*) addresses *on any interfaces* should have inbound Firewall Filters applied to the Loopback interface for both address families.

A full discussion of Firewall Filter design and evaluation is beyond the scope of this Benchmark, but is covered in more detail in Chapter 4 of the Juniper DayOne book

Hardening Junos Devices 2nd Edition, available for free from the Juniper DayOne Tech Libary.

At a minimum a Firewall Filter should be applied which restricts management services to trusted hosts, while accepting all other traffic so as not to interfere with normal function of protocol updates and services. This is not a suitable approach in high security environments, where a default discard/deny should be used along with other restrictions covered in separate Level 2 Recommendations in this section.

For devices with multiple Loopback Interface Units configured in different Routing Instances, Logical Systems or similar, Firewall Filters should be applied inbound for *all* configured Loopback units.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

At a minimum a Firewall Filter should be applied for each configured IP protocol version.
***NOTE** - This audit procedure only checks that Firewall Filters are applied, not that the filters are correctly configured.*
To check if any IPv4 (inet) or IPv6 (inet6) processing is configured on the devices interfaces issue the following commands from the `[edit]` configuration hierarchy:

```
[edit]
user@host#show interfaces | match "family inet " | count
user@host#show interfaces | match "family inet6 " | count
```

Output from the first command reflects the number of interfaces configured for IPv4 processing, output from the second command the number of interfaces configured for IPv6. Note that the space after *family inet* in the first command is required in order to match correctly.
Next, confirm that an input filter is configured for each configured address family:

```
[edit]
user@host#show interfaces lo0 | display set | match "filter input"
```

If the system is configured for IPv4 only, then a filter must be returned for *family inet*.
If the system is configured for IPv6 only, then a filter must be returned for *family inet6*.
For Dual Stack systems, configured for both IPv4 and IPv6 processing, filters must be returned for both address families.
***NOTE** - For SRX Firewalls, Security Policy using the junos-host zone as a destination may be used to limit access as an alternative to the inbound Firewall Filter described here.*

Remediation:

A full discussion of Firewall Filters is beyond the scope of this Benchmark.
It is important to ensure that Firewall Filters include terms to match and accept all of your required Routing Protocols, Management Services and any other services used on your Junos Device. As noted elsewhere, it is strongly recommended that changes to Firewall Filters applied to the Loopback interface always be applied using *commit confirmed* so that the change will be automatically rolled back should the administrator lose connection after committing the change.
To create a IPv4 firewall filter enter the following command from the [`edit firewall`] hierarchy.

```
[edit firewall]
user@host#edit family inet
[edit firewall family inet]
user@host#edit filter <filter name>
[edit firewall family inet filter <filter name>]
user@host#edit term <term name>
[edit firewall family inet filter <filter name> term <term name>]
user@host#set from <match conditions>
user@host#set then <action>
```

An IPv6 firewall filter, if required, can be configured under the family *inet6* from the same hierarchy.
The following example filter allows SSH from the 192.168.1.0/24 network and OSPF from 10.0.0.0/8, while (implicitly) *discarding* all other traffic (without logging):

```
firewall {
      family inet {
            filter ProtectRE {
                  term AllowOSPF {
                        from {
                             protocol ospf;
                             source-address 10.0.0.0/8;
                        }
                        then {
                             accept;
                        }
                  }
                  term AllowSSH {
                        from {
```

```
                    protocol tcp;
                    source-address 192.168.1.0/24;
                    destination-port ssh;
                }
                then {
                    accept;
                    log;
                    syslog;
                }
            }
        }
    }
}
```

Once a suitable filter has been configured, it must be applied to the Loopback interface, using the following command from the `[edit]` hierarchy:

```
[edit]
user@host#set interface lo0 unit 0 family inet filter input <filter name>
```

If additional Loopback Interface Units are configured (in other Routing Instances), the filter should also be applied to these.
If IPv6 filters are also required, the same command is used but applying to *family inet6*.

Default Value:

No firewall filters are configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.1 (page 55), National Security Agency (NSA)
2. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](https://www.juniper.net/documentation/partners/ibm/junos11.4-oemlitedocs/config-guide-firewall-policer.pdf)
3. [Hardening Junos Devices 2nd Edition, Juniper DayOne](https://www.juniper.net/documentation/en_US/day-one-books/TW_HardeningJunosDevices_2ndEd.zip)
4. O'Reilly JUNOS Cookbook - Recipe 2.14. Restricting Inbound SSH and Telnet Access - https://www.oreilly.com/library/view/junos-cookbook/0596100140/
5. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)

Additional Information:

For SRX Firewalls, it is often desirable to configure more in-depth protection for Exception Traffic to and from the SRX device itself by using the additional security features included in the SRX such as Stateful Firewall, AppFW and IPS.

This additional protection is configured on the SRX using the special *junos-host* zone as the *To Zone* in one or more Security Policies. Discussion of these features is beyond the scope of this Benchmark, but more details can be found on the Juniper Tech Library Configuring Security Policies.

Where the Junos Device is an SRX Firewall and a security policies are configured for the junos-host zone, an inbound Firewall Filter may still be applied to the Loopback interface if desired, but is not required.

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports
Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

2.2 Ensure "Protect RE" Firewall Filter includes explicit terms for all Management Services (Manual)

Profile Applicability:

- Level 2

Description:

The Firewall Filter used to protect the Junos Device should include explicit terms for all Management, Automation and Monitoring Services used

Rationale:

Junos supports a wide range of Management, Monitoring and Automation Services, making it an extremely flexible and adaptable platform. However, as with any computer system, the more services that are offered and the more hosts to which they are available, the wider attack surface is offered to a potential attacker.

Because Management Services provide users the ability to remotely configure, monitor or otherwise control the Junos Device, it is important to restrict access to just trusted hosts for each individual service.

Examples of Junos Management Services include (but are not limited to):

- Telnet (which should not be used, as described elsewhere)
- SSH (a secure alternative to Telnet)
- JWeb GUI (a web based interface over HTTP or HTTPS)
- SNMP (Simple Network Management Protocol, typically used for monitoring)
- NETCONF (an XML-RPC based automation standard)
- gRPC (a Remote Procedure Call based automation interface)
- REST API (an HTTP/S based automation interface)
- DMI (Device Management Interface - used by Network Management Systems, including Junos Space)

Unused services should ideally not be running at all - for example, if you do not use the JWeb GUI to manage your device, the service should be disabled under the `[edit system services]` configuration hierarchy as described elsewhere in this Benchmark.

Service's which are in use to manage your network should be appropriately secured using recommendations elsewhere in this Benchmark and have access restricted to trusted hosts for that service, using explicit *terms* in the "Protect RE" Firewall Filter discussed in

Recommendation 2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine.

A full discussion of Firewall Filter design and evaluation is beyond the scope of this Benchmark, but is covered in more detail in Chapter 4 of the Juniper DayOne book *Hardening Junos Devices 2nd Edition*, available for free from the Juniper DayOne Tech Libary.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

Due to the range of options available for Management Service selection, management subnets and filter design, it is not possible to automatically score this recommendation. "Protect RE" Firewall Filters should be set for ingress traffic on all Loopback interfaces as discussed in Recommendation 2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine for IPv4 (inet) and IPv6 (inet6) as necessary.
You can confirm what filters are applied to all your Loopback interfaces issuing the following command from the `[edit]` hierarchy:

```
[edit]
show interfaces lo0 | display set | match filter
```

You can view the details of the configured filter/s using the following command:

```
[edit]
show firewall family <inet/inet6> filter <filter-name>
```

In the example below, the filter `CIS-Example-IPv4` is configured as the input filter for the `inet` address family (IPv4).
This example filter allows SSH and and HTTPS (JWeb) traffic from a prefix-list named `management-hosts` (which is configured under the `[edit policy-options]` hierarchy and shown at the end of the example).

```
[edit]
mwhite@SRX1# show interfaces lo0 | display set | match filter
set interfaces lo0 unit 0 family inet filter input CIS-Example-IPv4
```

```
[edit]
mwhite@SRX1#show firewall family inet filter CIS-Example-IPv4
term AcceptSSH {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port ssh;
    }
    then {
        count SSH-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptHTTPS {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port https;
    }
    then {
        count HTTPS-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptSNMP {
    from {
        source-prefix-list {
            snmp-servers;
        }
        destination-port snmp;
    }
    then {
        count SNMP-Poll-Allowed;
        accept;
    }
}
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*

Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.

The use of `prefix-list' entries for the source addresses is not required, but is highly recommended as it makes filters clearer and ongoing management much simpler.

The lists used in the example can be viewed by issuing the following command from the `[edit]` hierarchy:

```
[edit]
mwhite@SRX1# show policy-options | find prefix-list
prefix-list management-hosts {
    172.16.10.0/24;
    192.168.17.0/24;
}
prefix-list snmp-servers {
    apply-path "snmp community <*> clients <*>";
}
```

Remediation:

A full discussion of Firewall Filters is beyond the scope of this Benchmark.
It is important to ensure that Firewall Filters include terms to match and accept all of your required Routing Protocols, Management Services and any other services used on your Junos Device. As noted elsewhere, it is strongly recommended that changes to Firewall Filters applied to the Loopback interface always be applied using *commit confirmed* so that the change will be automatically rolled back should the administrator lose connection after committing the change.
To create a IPv4 firewall filter enter the following command from the [`edit firewall`] hierarchy.

```
[edit firewall]
user@host#edit family inet
[edit firewall family inet]
user@host#edit filter <filter name>
[edit firewall family inet filter <filter name>]
user@host#edit term <term name>
[edit firewall family inet filter <filter name> term <term name>]
user@host#set from <match conditions>
user@host#set then <action>
```

An IPv6 firewall filter, if required, can be configured under the family *inet6* from the same hierarchy.
Once a suitable filter has been configured, it must be applied to the Loopback interface, using the following command from the `[edit]` hierarchy:

```
[edit]
user@host#set interface lo0 unit 0 family inet filter input <filter name>
```

If additional Loopback Interface Units are configured (in other Routing Instances), the filter should also be applied to these.
If IPv6 filters are also required, the same command is used but applying to *family inet6*.
To configure the `CIS-Example-IPv4` shown previously in the *Audit Procedure*, we opted to first configure a `prefix-list` each for our `management-hosts` and `snmp-servers` using the following commands from the `[edit policy-options]` heirachy:

```
[edit policy-options]
mwhite@SRX1# set prefix-list management-hosts 172.16.10.0/24
mwhite@SRX1# set prefix-list management-hosts 192.168.17.0/24
mwhite@SRX1# set prefix-list snmp-servers apply-path "snmp community <*>
clients <*>"
```

The `management-hosts` prefix-list is a manual list of IP subnets which can be used in multiple policies or terms. If we add or remote IPs on the list, it will cause all of the terms to be updated, rather than having to manually update our management hosts in multiple locations.

The `snmp-servers` prefix-list used an `apply-path` to return all configured SNMP Clients (the Network Management Servers (NMS) which will be permitted to poll this Junos Device using Simple Network Management Protocol) from elsewhere in the configuration. The same technique can be used to create a list of all configured NTP Servers, BGP Peers and so on. Lists created using an `apply-path` will automatically update when the source does, so if we add a new SNMP Client, the prefix-list updated automatically.

We then created an IPv4 firewall filter from the `[edit firewall]` hierarchy:

```
[edit firewall]
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH from
source-prefix-list management-hosts
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH from
destination-port ssh
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH then
count SSH-Allowed
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH then log
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH then
syslog
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetSSH then
accept
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS from
source-prefix-list management-hosts
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS from
destination-port https
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS then
count HTTPS-Allowed
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS then
log
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS then
syslog
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS then
accept
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSNMP from
source-prefix-list snmp-servers
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSNMP from
destination-port snmp
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSNMP then
count SNMP-Poll-Allowed
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSNMP then
accept
```

The first two *terms* `AcceptSSH` and `AcceptHTTPS` accept SSH and HTTPS traffic respectively from any host listed in the the `management-hosts` prefix-list. Traffic matching these terms is also logged and separate *counters* incremented each time the term is hit.
Term 3, `AcceptSNMP` accepts SNMP Polling from SNMP Clients (SNMP Servers) which were automatically added to the `snmp-servers` prefix-list. As polling could be frequent, no logging is used, but a counter is incremented.
The filter can now be applied to the Loopback interface, using the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
mwhite@SRX1# set unit 0 family inet filter input CIS-Example-IPv4
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*
Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.

Default Value:

No firewall filters are configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.1 (page 55), National Security Agency (NSA)
2. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](https://www.juniper.net/documentation/partners/ibm/junos11.4-oemlitedocs/config-guide-firewall-policer.pdf)
3. [Hardening Junos Devices 2nd Edition, Juniper DayOne](https://www.juniper.net/documentation/en_US/day-one-books/TW_HardeningJunosDevices_2ndEd.zip)
4. O'Reilly JUNOS Cookbook - Recipe 2.14. Restricting Inbound SSH and Telnet Access - https://www.oreilly.com/library/view/junos-cookbook/0596100140/
5. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)

Additional Information:

For SRX Firewalls, it is often desirable to configure more in-depth protection for Exception Traffic to and from the SRX device itself by using the additional security features included in the SRX such as Stateful Firewall, AppFW and IPS.

This additional protection is configured on the SRX using the special junos-host zone as the To Zone in one or more Security Policies. Discussion of these features is beyond the scope of this Benchmark, but more details can be found on the Juniper Tech Library Configuring Security Policies.

Where the Junos Device is an SRX Firewall and a security policies are configured for the junos-host zone, an inbound Firewall Filter may still be applied to the Loopback interface if desired, but is not required.

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

9.4 Apply Host-based Firewalls or Port Filtering
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.3 Ensure "Protect RE" Firewall filter includes Rate-Limiting for Management Services terms (Manual)

Profile Applicability:

- Level 2

Description:

Policers should be applied to Management Services

Rationale:

Junos supports a wide range of Management, Monitoring and Automation Services, making it an extremely flexible and adaptable platform. However, as with any computer system, the more services that are offered and the more hosts to which they are available, the wider attack surface is offered to a potential attacker.

An attacker, or a misconfigured or failing management server, might flood a service on the Junos device with excessive traffic in a *Denial of Service* (or *DoS*) attack; resulting in increased load and potentially even a failure of the service or targeted device.

To prevent this *Rate-limiting* can be applied to the Firewall Filter Terms already configured for Management Services in Recommendation 2.1 - Ensure "Protect RE" Firewall Filter includes explicit terms for all Management Services by configuring a `policer` as appropriate for the service.

In some environments, it may also be appropriate to configure policers for Routing Protocols or other Services, although this is less common practice and can lead to unstable network conditions without careful design and testing.

A full discussion of how Rate-limiting is configured and implemented in Junos, and across different specific chipsets and platforms, is beyond the scope of this Benchmark. The Junos DayOne books Deploying Basic QoS and Hardening Junos Devices, 2nd Edition are available for Free from the Juniper website and provide excellent coverage of QoS/CoS techniques and the application of Rate-limiting to Firewall Filters respectively.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

Due to the range of options available for Management Service selection, management subnets and filter design, it is not possible to automatically score this recommendation. "Protect RE" Firewall Filters should be set for ingress traffic on all Loopback interfaces as discussed in Recommendation 2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine for IPv4 (inet) and IPv6 (inet6) as necessary.
You can confirm what filters are applied to all your Loopback interfaces issuing the following command from the `[edit]` hierarchy:

```
[edit]
show interfaces lo0 | display set | match filter
```

You can view the details of the configured filter/s using the following command:

```
[edit]
show firewall family <inet/inet6> filter <filter-name>
```

In the example below, the filter `CIS-Example-IPv4` is configured as the input filter for the `inet` address family (IPv4) used in Recommendation 2.2 Ensure "Protect RE" Firewall Filter includes explicit terms for all Management Services has been updated to apply a Rate Limit of 10Mb/s to SSH and HTTPS traffic, leaving sufficient capacity to allow Junos images or other files to be transferred but protecting from DoS attacks. A separate 1Mb/s limit has been applied to SNMP Polling.

```
[edit]
mwhite@SRX1# show interfaces lo0 | display set | match filter
set interfaces lo0 unit 0 family inet filter input CIS-Example-IPv4

[edit]
mwhite@SRX1#show firewall family inet filter CIS-Example-IPv4
term AcceptSSH {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port ssh;
    }
    then {
       policer limit-10m;
        count SSH-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptHTTPS {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port https;
    }
    then {
        policer limit-10m;
        count HTTPS-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptSNMP {
    from {
        source-prefix-list {
            snmp-servers;
        }
        destination-port snmp;
    }
    then {
        policer limit-1m;
        count SNMP-Poll-Allowed;
        accept;
    }
}
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*

Those Policers can be viewed using the following command from the `[edit]` hierarchy:

```
[edit]
mwhite@SRX1# show firewall policer limit-10m
if-exceeding {
    bandwidth-limit 10m;
    burst-size-limit 625k;
}
then discard;

[edit]
mwhite@aSRX1# show firewall policer limit-1m
if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 15k;
}
then discard;
```

Remediation:

A full discussion of Firewall Filters is beyond the scope of this Benchmark.

It is important to ensure that Firewall Filters include terms to match and accept all of your required Routing Protocols, Management Services and any other services used on your Junos Device. As noted elsewhere, it is strongly recommended that changes to Firewall Filters applied to the Loopback interface always be applied using `commit confirmed` so that the change will be automatically rolled back should the administrator lose connection after committing the change.

In this example we will add Rate-Limiting to the Management Services terms configured in Recommendation 2.2 Ensure "Protect RE" Firewall Filter includes explicit terms for all Management Services Draft using the following commands from the `[edit firewall]` hierarchy:

First we need to create the two 'policer' definitions, which can be re-used in multiple terms of filters.

```
[edit firewall]
mwhite@SRX1# set policer limit-10m if-exceeding bandwidth-limit 10m
mwhite@SRX1# set policer limit-10m if-exceeding burst-size-limit 625k
mwhite@SRX1# set policer limit-10m then discard
mwhite@SRX1# set policer limit-1m if-exceeding bandwidth-limit 1m
mwhite@SRX1# set policer limit-1m if-exceeding burst-size-limit 15k
mwhite@SRX1# set policer limit-1m then discard
```

These policers set a `bandwidth-limit` of 10Mb/s and 1Mb/s respectively, with an appropriate `burst-size` set on each proportional to the configured limit to allow bursts to briefly exceed the limit and smooth the impact of the policer on the service.

The `limit-10m` policer is then applied to both the `AcceptSSH` and `AcceptHTTPS` terms in the `CIS-Example-IPv4` configured previously. The policer applies separately for each term, so SSH and HTTPS can receive 10Mb/s of traffic *each*, not a combined 10Mb/s between them.

```
[edit firewall]
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSSH then
policer limit-10m
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptHTTPS then
policer limit-10m
```

Finally, we apply the lower 'limit-1m' 1Mb/s policer to the existing `AcceptSNMP` term:

```
[edit firewall]
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptSNMP then
policer limit-1m
```

If it is not already, the filter can now be applied to the Loopback interface, using the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
mwhite@SRX1# set unit 0 family inet filter input CIS-Example-IPv4
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*
Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.

Default Value:

No firewall filters are configured by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/concept/policer-overview.html
2. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](https://www.juniper.net/documentation/partners/ibm/junos11.4-oemlitedocs/config-guide-firewall-policer.pdf)
3. [Hardening Junos Devices 2nd Edition, Juniper DayOne](https://www.juniper.net/documentation/en_US/day-one-books/TW_HardeningJunosDevices_2ndEd.zip)
4. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)

Additional Information:

For SRX Firewalls, it is often desirable to configure more in-depth protection for Exception Traffic to and from the SRX device itself by using the additional security features included in the SRX such as Stateful Firewall, AppFW and IPS.

This additional protection is configured on the SRX using the special `junos-host` zone as the To Zone in one or more Security Policies. Discussion of these features is beyond the scope of this Benchmark, but more details can be found on the Juniper Tech Library Configuring Security Policies.

Where the Junos Device is an SRX Firewall and a security policies are configured for the `junos-host` zone, an inbound Firewall Filter may still be applied to the Loopback interface if desired, but is not required.

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.4 Apply Host-based Firewalls or Port Filtering
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.4 Ensure "Protect RE" Firewall Filter includes explicit terms for all Protocols (Manual)

Profile Applicability:

- Level 2

Description:

Routing and Switching Protocol traffic should be filtered

Rationale:

Junos devices support a vast range of Routing Protocols to enable flexible services to be deployed. However, as with any computer system, the more services that are offered and the more hosts to which they are available, the wider attack surface is offered to a potential attacker.

In addition, an attacker may seek to connect to Routing Protocols in an attempt to gain knowledge of the network, re-route traffic to perform *Man in the Middle* (*MITM*) attacks or disrupt the network to perform a *Denial of Service* (*DoS*) attack.

Limiting the devices able to connect to these sensitive protocols, on a per protocol basis, greatly enhances the security of the device. These protocols might include (but are not limited to):

- OSPF
- IS-IS
- BGP
- RIP

A full discussion of Firewall Filter design and evaluation is beyond the scope of this Benchmark, but is covered in more detail in Chapter 4 of the Juniper DayOne book *Hardening Junos Devices 2nd Edition*, available for free from the Juniper DayOne Tech Libary.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

Due to the range of options available for Management Service selection, management subnets and filter design, it is not possible to automatically score this recommendation. "Protect RE" Firewall Filters should be set for ingress traffic on all Loopback interfaces as discussed in Recommendation 2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine for IPv4 (inet) and IPv6 (inet6) as necessary.
You can confirm what filters are applied to all your Loopback interfaces issuing the following command from the `[edit]` hierarchy:

```
[edit]
show interfaces lo0 | display set | match filter
```

You can view the details of the configured filter/s using the following command:

```
[edit]
show firewall family <inet/inet6> filter <filter-name>
```

In the example below, the filter `CIS-Example-IPv4` is configured as the input filter for the `inet` address family (IPv4).

```
[edit]
mwhite@SRX1# show interfaces lo0 | display set | match filter
set interfaces lo0 unit 0 family inet filter input CIS-Example-IPv4

[edit]
mwhite@SRX1#show firewall family inet filter CIS-Example-IPv4
term AcceptSSH {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port ssh;
    }
    then {
        count SSH-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptHTTPS {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port https;
    }
    then {
        count HTTPS-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptSNMP {
    from {
        source-prefix-list {
            snmp-servers;
        }
        destination-port snmp;
    }
    then {
        count SNMP-Poll-Allowed;
        accept;
    }
}
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*
Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.
The use of `prefix-list' entries for the source addresses is not required, but is highly recommended as it makes filters clearer and ongoing management much simpler.
The lists used in the example can be viewed by issuing the following command from the `[edit]` hierarchy:

```
[edit]
mwhite@SRX1# show policy-options | find prefix-list
prefix-list management-hosts {
    172.16.10.0/24;
    192.168.17.0/24;
}
prefix-list snmp-servers {
    apply-path "snmp community <*> clients <*>";
}
```

Remediation:

A full discussion of Firewall Filters is beyond the scope of this Benchmark.
It is important to ensure that Firewall Filters include terms to match and accept all of your required Routing Protocols, Management Services and any other services used on your Junos Device. As noted elsewhere, it is strongly recommended that changes to Firewall Filters applied to the Loopback interface always be applied using *commit confirmed* so that

the change will be automatically rolled back should the administrator lose connection after committing the change.

To create a IPv4 firewall filter enter the following command from the [`edit firewall`] hierarchy.

```
[edit firewall]
user@host#edit family inet
[edit firewall family inet]
user@host#edit filter <filter name>
[edit firewall family inet filter <filter name>]
user@host#edit term <term name>
[edit firewall family inet filter <filter name> term <term name>]
user@host#set from <match conditions>
user@host#set then <action>
```

An IPv6 firewall filter, if required, can be configured under the family *inet6* from the same hierarchy.

Once a suitable filter has been configured, it must be applied to the Loopback interface, using the following command from the `[edit]` hierarchy:

```
[edit]
user@host#set interface lo0 unit 0 family inet filter input <filter name>
```

If additional Loopback Interface Units are configured (in other Routing Instances), the filter should also be applied to these.

If IPv6 filters are also required, the same command is used but applying to *family inet6*.

In the example below, we add a new term `AcceptBGP` to the `CIS-Example-IPv4` shown previously in the *Audit Procedure*. We opted to first configure a `prefix-list` each for our `bgp-neighbors` using the following command from the `[edit policy-options]` hierarchy:

```
[edit policy-options]
mwhite@SRX1# set prefix-list bgp-neighbors apply-path "protocols bgp group
<*> neighbor <*>"
```

The `bgp-neighbors` prefix-list used an `apply-path` to return all configured BGP Neighbors configured for any `group` under the `[edit protocols bgp]` configuration. The same technique can be used to create a list of all configured NTP Servers, SNMP Servers and so on. Lists created using an `apply-path` will automatically update when the source configuration does, so if we add a new BGP Neighbor, the prefix-list is updated automatically.

NOTE - *If you are running protocols in multiple Routing Instances, Logical Systems or similar features, you may need to adjust your prefix-list and apply-path to reflect these additional locations.*

We can then add a new term to the existing `CIS-Example-IPv4` firewall filter with the following commands from the `[edit firewall]` hierarchy:

```
[edit firewall]
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetBGPfrom
source-prefix-list bgp-neighbors
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetBGP from
protocol tcp
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetBGP from
destination-port bgp
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AccpetBGP then
count BGP-Allowed
mwhite@SRX1# set family inet filter CIS-Example-IPv4 term AcceptBGP then
accept
```

This filter matches traffic coming from any configured BGP Neighbor to TCP Port 179 and accepts it, incrementing a named `counter BGP-Allowed`, which helps us with troubleshooting and monitoring.
If it is not already, the filter can now be applied to the Loopback interface, using the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
mwhite@SRX1# set unit 0 family inet filter input CIS-Example-IPv4
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*
Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.

Default Value:

No firewall filters are configured by default.

References:

1. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](https://www.juniper.net/documentation/partners/ibm/junos11.4-oemlitedocs/config-guide-firewall-policer.pdf)
2. [Hardening Junos Devices 2nd Edition, Juniper DayOne](https://www.juniper.net/documentation/en_US/day-one-books/TW_HardeningJunosDevices_2ndEd.zip)
3. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)

Additional Information:

For SRX Firewalls, it is often desirable to configure more in-depth protection for Exception Traffic to and from the SRX device itself by using the additional security features included in the SRX such as Stateful Firewall, AppFW and IPS.

This additional protection is configured on the SRX using the special junos-host zone as the To Zone in one or more Security Policies. Discussion of these features is beyond the scope of this Benchmark, but more details can be found on the Juniper Tech Library Configuring Security Policies.

Where the Junos Device is an SRX Firewall and a security policies are configured for the junos-host zone, an inbound Firewall Filter may still be applied to the Loopback interface if desired, but is not required.

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

9.4 Apply Host-based Firewalls or Port Filtering
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.5 Ensure "Protect RE" Firewall Filter includes Flood Attack Protection terms (Manual)

Profile Applicability:

- Level 2

Description:

Flood Attack protection should be included in the "Protect RE" Filter

Rationale:

As with any computer system connected to a network, an attacker may attempt to overwhelm the resources of a Junos device by flooding it with unwanted traffic, consuming resources and potentially resulting in a *Denial of Service* (or *DoS*) Attack.

Filtering traffic sources and the available services using a "Protect RE" filter as discussed elsewhere in this section helps to limit the scope for an attack, but flood attacks using TCP SYN packets, ICMP or other protocols may still be possible.

To prevent this *Rate-limiting* can be applied to the Firewall Filter by configuring a `policer` to new terms matching the potential attack traffic.

A full discussion of how Rate-limiting is configured and implemented in Junos, and across different specific chipsets and platforms, is beyond the scope of this Benchmark. The Junos DayOne books Deploying Basic QoS and Hardening Junos Devices, 2nd Edition are available for Free from the Juniper website and provide excellent coverage of QoS/CoS techniques and the application of Rate-limiting to Firewall Filters respectively.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

Due to the range of options available for Management Service selection, management subnets and filter design, it is not possible to automatically score this recommendation. "Protect RE" Firewall Filters should be set for ingress traffic on all Loopback interfaces as

discussed in Recommendation 2.1 Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine for IPv4 (inet) and IPv6 (inet6) as necessary.
You can confirm what filters are applied to all your Loopback interfaces issuing the following command from the `[edit]` hierarchy:

```
[edit]
show interfaces lo0 | display set | match filter
```

You can view the details of the configured filter/s using the following command:

```
[edit]
show firewall family <inet/inet6> filter <filter-name>
```

In the example below, the filter `CIS-Example-IPv4` is configured as the input filter for the `inet` address family (IPv4), this has already been configured with rate limiting for SSH, HTTPS and SNMP services as shown in Recommendations 2.3 Ensure "Protect RE" Firewall filter includes Rate-Limiting for Management Services terms, to this we have added a number of Flood Protection terms:

```
[edit]
mwhite@SRX1# show interfaces lo0 | display set | match filter
set interfaces lo0 unit 0 family inet filter input CIS-Example-IPv4

[edit]
mwhite@SRX1#show firewall family inet filter CIS-Example-IPv4

term Limit-SYNFlood {
    from {
        source-prefix-list {
            management-hosts;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
    }
    then policer limit-100k;
}
term AcceptSSH {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port ssh;
    }
    then {
        policer limit-10m;
        count SSH-Allowed;
        log;
        syslog;
        accept;
    }
}
```

```
term AcceptHTTPS {
    from {
        source-prefix-list {
            management-hosts;
        }
        destination-port https;
    }
    then {
        policer limit-10m;
        count HTTPS-Allowed;
        log;
        syslog;
        accept;
    }
}
term AcceptSNMP {
    from {
        source-prefix-list {
            snmp-servers;
        }
        destination-port snmp;
    }
    then {
        policer limit-1m;
        count SNMP-Poll-Allowed;
        accept;
    }
}
term AcceptICMP {
    from {
        protocol icmp;
        icmp-type [ echo-request echo-reply unreachable time-exceeded ];
    }
    then {
        policer limit-1m;
        accept;
    }
}
term AcceptTCP-Established {
    from {
        source-port ssh;
        tcp-established;
    }
    then {
        policer limit-10m;
        accept;
    }
}
term AcceptTraceroute {
    from {
        protocol udp;
        destination-port 33434-33523;
    }
    then {
        policer limit-1m;
        accept;
    }
}
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*

The term `Limit-SYNFlood` has been added ahead of any TCP based services (in this example SSH and HTTPS for JWeb, but this could also include TCP based services such as NETCONF, DMI or BGP; in which case additional `source-prefix-list` match conditions will be needed for BGP Neighbors, Management/Automation Servers, etc). We match TCP packets from the `management-hosts` prefix-list (configured previously), which have the TCP SYN Flag, but not the ACK Flag set. Although less common than SYN Floods, an attacker may also attempt to abuse RST and FIN flags, so we also match on these. A Rate-limit of 100kb/s is applied using the `policer limit-100k`.

The `AcceptICMP` term is added to allow services like Ping (Echo) and ICMP Unreachable messages, but applies a 1kb/s policer as these services are often abused by attackers.

`AcceptTCP-Established` allows for reply traffic to outbound TCP based sessions from the Junos device. Firewall Filters are Stateless, so this is needed to allow the reply and matches based on TCP packets with the ACK or RST flags set. If other TCP based services such as BGP are used, additional `destination-port` entries will be required to allow replies to existing sessions. A 10Mb/s policer is applied to matching traffic.

Finally `AcceptTraceroute` allows for traceroute traffic through the device while applying a 1Mb/s policer to limit the scope for abuse by an attacker.

Those Policers can be viewed using the following command from the `[edit]` hierarchy:

```
[edit]
mwhite@SRX1# show firewall policer limit-10m
if-exceeding {
    bandwidth-limit 10m;
    burst-size-limit 625k;
}
then discard;

[edit]
mwhite@aSRX1# show firewall policer limit-1m
if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 15k;
}
then discard;

[edit]
mwhite@SRX1# show firewall policer limit-100k
if-exceeding {
    bandwidth-limit 100k;
    burst-size-limit 15k;
}
then discard;
```

Remediation:

A full discussion of Firewall Filters is beyond the scope of this Benchmark.
It is important to ensure that Firewall Filters include terms to match and accept all of your required Routing Protocols, Management Services and any other services used on your Junos Device. As noted elsewhere, it is strongly recommended that changes to Firewall Filters applied to the Loopback interface always be applied using `commit confirmed` so that the change will be automatically rolled back should the administrator lose connection after committing the change.
In this example, we will add the new Flood Protection terms seen in the audit procedure to our existing Firewall Filter from Recommendation 2.3 Ensure "Protect RE" Firewall filter includes Rate-Limiting for Management Services terms using the following commands from the `[edit firewall]` hierachy:
First we need to create an additional 'policer' definition, which can be re-used in multiple terms of filters.

```
 [edit firewall]
mwhite@SRX1# set if-exceeding bandwidth-limit 100k
mwhite@SRX1# set if-exceeding burst-size-limit 15k
mwhite@SRX1# set then discard
```

This new policer enforces a `bandwidth-limit` of 100kb/s, with a `burst-size` proportional to the configured limit to allow bursts to briefly exceed the limit and smooth the impact of the policer on the service.
The new `limit-100k` policer is used in the new `Limit-SYNFlood` term, while the other new terms re-use the `limit-1m` and limit-`10m` configured previously. A policer applies separately for each term, so SSH, HTTPS and new terms re-using these policers can receive 10Mb/s of traffic *each*, not a combined 10Mb/s between them.

```
 [edit firewall]
mwhite@SRX1# set term Limit-SYNFlood from source-prefix-list management-hosts
mwhite@SRX1# set term Limit-SYNFlood from protocol tcp
mwhite@SRX1# set term Limit-SYNFlood from tcp-flags "(syn & !ack) | fin |
rst"
mwhite@SRX1# set term Limit-SYNFlood then policer limit-100k
mwhite@SRX1# set term AcceptICMP from icmp-type echo-request
mwhite@SRX1# set term AcceptICMP from icmp-type echo-reply
mwhite@SRX1# set term AcceptICMP from icmp-type unreachable
mwhite@SRX1# set term AcceptICMP from icmp-type time-exceeded
mwhite@SRX1# set term AcceptICMP then policer limit-1m
mwhite@SRX1# set term AcceptICMP then accept
mwhite@SRX1# set term AcceptTCP-Established from source-port ssh
mwhite@SRX1# set term AcceptTCP-Established from tcp-established
mwhite@SRX1# set term AcceptTCP-Established then policer limit-10m
mwhite@SRX1# set term AcceptTCP-Established then accept
mwhite@SRX1# set term AcceptTraceroute from protocol udp
mwhite@SRX1# set term AcceptTraceroute from destination-port 33434-33523
```

```
mwhite@SRX1# set term AcceptTraceroute then policer limit-1m
mwhite@SRX1# set term AcceptTraceroute then accept
```

Because the `Limit-SYNFlood` term needs to be executed *before* any TCP Services like SSH, HTTPS or BGP, we will move the term ahead of the `AcceptSSH` term configured previously:

```
[edit firewall]
mwhite@SRX1# insert family inet filter CIS-Example-IPv4 term Limit-SYNFlood
before term AcceptSSH
```

If it is not already, the filter can now be applied to the Loopback interface, using the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
mwhite@SRX1# set unit 0 family inet filter input CIS-Example-IPv4
```

Note - *The example filter above not complete and may not be suitable for all environments - all other traffic to the Junos Device will be discarded.*
Your filters should include terms for all of the Management, Monitoring and Automation services, as well as any Routing Protocols or other services such as IPSEC or BFD in use in your network.

Default Value:

No firewall filters are configured by default.

References:

1. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)
2. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](https://www.juniper.net/documentation/partners/ibm/junos11.4-oemlitedocs/config-guide-firewall-policer.pdf)
3. [Hardening Junos Devices 2nd Edition, Juniper DayOne](https://www.juniper.net/documentation/en_US/day-one-books/TW_HardeningJunosDevices_2ndEd.zip)

Additional Information:

For SRX Firewalls, it is often desirable to configure more in-depth protection for Exception Traffic to and from the SRX device itself by using the additional security features included in the SRX such as Stateful Firewall, AppFW and IPS.

This additional protection is configured on the SRX using the special junos-host zone as the To Zone in one or more Security Policies. Discussion of these features is beyond the scope of this Benchmark, but more details can be found on the Juniper Tech Library Configuring Security Policies.

Where the Junos Device is an SRX Firewall and a security policies are configured for the junos-host zone, an inbound Firewall Filter may still be applied to the Loopback interface if desired, but is not required.

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.6 Ensure firewall filters contain explicit deny and log term (Manual)

Profile Applicability:

- Level 2

Description:

Filters should include a final Deny and Log term.

Rationale:

Firewall filters are built up of one or more *terms*, which are evaluated in order until either one is matched (at which point the terms *then* action is taken) or the final term has been evaluated, at which point the default action is to discard the packet.

It is important to log packets which are denied by the firewall filter, these may indicate an attempted attack or could suggest a problem in the network or with the firewall filter itself.

A term should be added to the end of the each firewall filter which logs the packet header information and blocks the packet. The `discard` method is used to block the packet silently, with no message sent back to the source, denying the attacker information and limiting resource usage on the router.

Impact:

Firewall Filters should be carefully tested before implementation on production systems as incorrect configuration may prevent normal services functioning.

It is strongly recommended that changes to Firewall Filters are applied using `commit confirmed` so that changes will be automatically rolled back should they prevent the administrator from connecting to the Junos Device.

Audit:

Due to the range of options available as to Filter Name, Term Name, terms and the use of the filter; it is not possible to score this recommendation.
Firewall filters may be viewed by issuing the following command:

```
[edit]
user@host#show firewall
```

Note *- In Junos, Firewall Filters may be used for a wide range of purposes in addition to actually filtering traffic in or out of interfaces. This could include Quality of Service (QoS)*

Classifiers, Packet Capture & Analysis or Filter Based Forwarding/Policy Based Routing. When a Firewall Filter is used for a non-Firewall purpose such as these, an explicit deny all term may not be appropriate and traffic not matching the filter may actually require an explicit accept all term instead to ensure normal network operations.

Remediation:

To create a firewall filter term enter the following command from the `[edit firewall family <family> filter <filter name>]` hierarchy.

```
[edit firewall family inet filter <filter name>]
user@host#set term <term name> then discard
user@host#set term <term name> then syslog
user@host#set term <term name> then log
```

Default Value:

No firewall filters are configured by default.

References:

1. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](http://www.juniper.net/techpubs/software/junos/junos94/swconfig-policy/firewall-filter-overview.html)
2. *Recipe 15: Low-Risk Methodology for Deploying Firewall Filters* in the [Day One: Juniper Ambassadors' Cookbook 2019](https://www.juniper.net/documentation/en_US/day-one-books/DO_Ambassadors2019.pdf)

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.7 Ensure internal sources are blocked on external networks (Manual)

Profile Applicability:

- Level 2

Description:

Deny traffic with an internal source or reserved IP address from external source.

Rationale:

An attacker may attempt to bypass security controls and Intrusion Detection Systems (IDS) by using the source address of a trusted (generally internal) host, a technique known as *spoofing*. Packets arriving on external networks should *never* have a source address from your internal network ranges, especially where the internal networks use RFC1918 private address space or invalid addresses.

Any traffic with an internal source arriving on an external interface is certain to be an attack and should be blocked.

A Firewall Filter should be applied to all external network interfaces and include a term to deny internal address ranges.

The `discard` method is used to block the packet silently, with no message sent back to the source. This traffic should also be logged to the local routing engine and SYSLOG, allowing attacks to be detected and record kept.

Audit:

Due to the range of options available as to Filter Name, Term Name and terms; it is not possible to score this recommendation. Firewall filters may be viewed by issuing the following command:

```
[edit]
user@host#show firewall
```

NOTE *- In Junos, Firewall Filters may be used for a wide range of purposes in addition to actually filtering traffic in or out of interfaces. This could include Quality of Service (QoS) Classifiers, Packet Capture & Analysis or Filter Based Forwarding/Policy Based Routing. When a Firewall Filter is used for a non-Firewall purpose such as these, a term blocking internal addresses may not be appropriate and traffic not matching the filter may actually require an explicit accept all term instead to ensure normal network operations.*

Remediation:

To create a firewall filter term enter the following command from the `[edit firewall family <family> filter <filter name>]` hierarchy.

```
[edit firewall family inet filter <filter name>]
user@host#edit term <term name>

[edit firewall family inet filter <filter name> term <term name>]
user@host#set from source-address 127.0.0.0/8
user@host#set from source-address 10.0.0.0/8
user@host#set from source-address 0.0.0.0/32
user@host#set from source-address 172.16.0.0/12
user@host#set from source-address 192.168.0.0/16
user@host#set from source-address 192.0.2.0/24
user@host#set from source-address 169.254.0.0/16
user@host#set from source-address 198.18.0.0/15
user@host#set from source-address 198.51.100.0/24
user@host#set from source-address 203.0.113.0/24
user@host#set from source-address 224.0.0.0/8
user@host#set from source-address 255.255.255.255/32
user@host#set from source-address
user@host#set then discard
user@host#set then syslog
user@host#set then log
```

NOTE - At least one further term must be included in this firewall filter to allow legitimate traffic.

Default Value:

No firewall filters are configured by default.

References:

1. Cisco IOS Benchmark Version 2.2, Requirement 2.3.1.1, Center for Internet Security
2. [Firewall Filter Overview, JUNOS Software Policy Framework Configuration Guide, Juniper Networks](http://www.juniper.net/techpubs/software/junos/junos94/swconfig-policy/firewall-filter-overview.html)

CIS Controls:

Version 7

12.2 Scan for Unauthorized Connections across Trusted Network Boundaries
Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

12.3 Deny Communications with Known Malicious IP Addresses

Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.

3 Interfaces

This section provides guidance on the secure configuration of Interface specific parameters and options which are contained under the `[edit interfaces <interface name>]` hierarchy.

3.1 DLn – Dialer Interfaces

Dialer interfaces are used to access modem connections on Juniper routers. These settings are accessed under the `[edit interfaces dln]` hierarchy (where `n` is the interface number).

Only apply the recommendations in this section where a dialer interfaces is configured on the device for Dial In Services. You can confirm the number of configured dialer interfaces by issuing the following command from the `[edit]` *hierarchy:*

```
[edit]

user@host# show interfaces | match "dl.*" | count
```

If a positive integer is returned then you should apply all of the recommendations in this section.

Some JUNOS Devices, such as many Branch SRX models, may also use the Dialer Interface for initializing a 3G or LTE Backup Connection to provide resilience for a Branch Office with only a single WAN link. The settings in this section are *not* intended for Dialer Interfaces used for this purpose *and should not be applied*.

You can confirm whether your Dialer Interface is being used for a 3G/LTE Backup with the following command issued from the `[edit]` hierarchy:

```
[edit]

user@host# show interfaces | match "backup-options interface dl0" | count
```

If a line count of 1 or higher is returned, you should *not* apply the Recommendations in this section for the Dialer Interfaces.

3.1.1 Ensure Caller ID is set (Automated)

Profile Applicability:

- Level 1

Description:

Caller restrictions MUST be used when Incoming calls are permitted.

Rationale:

Some JUNOS routers support the use of a dial in modem connection for Telnet/SSH administration of the router from a remote connection over the telephone network.

This can provide a useful out of band management channel, allowing access to a customer router at a remote site when the primary circuit has failed for example, but also creates a new route for attack, allowing a malicious user to bypass firewalls and other defenses.

Even when the phone number for the modem is kept secret, attackers may still discover it through war dialing, possibly narrowing targets by researching the number ranges used by your organization.

To limit the scope for such an attack, the dialer interface should be configured to check the incoming Caller ID for connection attempts, only allowing the connection to proceed when the caller is on a pre-configured list of approved numbers.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | match "incoming-map" | count
```

If an interface is set to accept incoming calls and use Caller ID this should be a positive integer. A value of 0 does may indicate that Caller ID is not used or may simply indicate that incoming calls are not configured at all.

Remediation:

If you have configured a dialer interface to accept incoming calls, you should restrict the allowable Caller ID by entering the following command under the [edit interfaces dln unit 0 dialer-options] hierarchy (where n is the dialer interface number);

```
[edit interfaces dln unit 0 dialer-options]
user@host#set incoming-map caller <Approved CallerID Number>
```

Up to 15 caller numbers may be configured on a dialer interface, repeat the command above for each number you wish to add.

References:

1. [Setting Up USB Modems for Remote Management, JUNOS 9.5 Security Configuration Guide, Juniper Networks](http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/config-usb-modem-chapter.html#config-usb-modem-chapter)

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3.1.2 Ensure access profile is set to use CHAP (Automated)

Profile Applicability:

- Level 1

Description:

CHAP Authentication MUST be used when Incoming calls are permitted.

Rationale:

Some JUNOS routers support the use of a dial in modem connection for Telnet/SSH administration of the router from a remote connection over the telephone network.

This can provide a useful out of band management channel, allowing access to a customer router at a remote site when the primary circuit has failed for example, but also creates a new route for attack, allowing a malicious user to bypass firewalls and other defenses.

Even when the phone number for the modem is kept secret, attackers may still discover it through war dialing, possibly narrowing targets by researching the number ranges used by your organization.

To limit the scope for such an attack, the dialer interface should be configured to use Challenge Handshake Authentication Protocol (CHAP) before allowing calls to connect. Using CHAP, a username and password can be configured for each user that needs to connect to the router via the modem. *The password should not be the same as that used by to login to the routers CLI itself.*

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | find "chap" | match "access-profile" | count
```

If an interface is set to accept incoming calls and use CHAP Authentication this should be a positive integer. A value of 0 does may indicate that CHAP is not used or may simply indicate that incoming calls are not configured at all.

Remediation:

If you have configured a dialer interface to accept incoming calls, you should configure CHAPS authentication using the following commands from the indicated hierarchy (where *n* is the interface number);

```
[edit access]
user@host#set profile <profile name> client <username> chap-secret <password>

user@host#top
user@host#edit interface dl <n> unit 0

[edit interfaces dl <n> unit 0]
user@host#set ppp-options chap access-profile <profile name>
```

Repeat the first command for each user that is required.

References:

1. Setting Up USB Modems for Remote Management, JUNOS 9.5 Security Configuration Guide, Juniper Networks

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3.1.3 Forbid Dial in Access (Automated)

Profile Applicability:

- Level 2

Description:

Dial in access should not be used on sensitive routers.

Rationale:

Some JUNOS routers support the use of a dial in modem connection for Telnet/SSH administration of the router from a remote connection over the telephone network.

This can provide a useful out of band management channel, allowing access to a customer router at a remote site when the primary circuit has failed for example, but also creates a new route for attack, allowing a malicious user to bypass firewalls and other defenses.

Even when the phone number for the modem is kept secret, attackers may still discover it through war dialing, possibly narrowing targets by researching the number ranges used by your organization.

For sensitive routers, such as those in a PCI DSS Cardholder Data Environment, the protective measures available for dial in access are insufficient and no dial in access should be used. If not required for other services the modem should be physically removed from the router.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host# show interfaces | match "incoming-map" | count
```

Remediation:

If you have configured a dialer interface to accept incoming calls, you should disable it using the following commands from the `[edit interfaces]` hierarchy (where *n* indicates the interface number);

```
[edit interfaces]
user@host#delete interface dl <n>
```

References:

1. Setting Up USB Modems for Remote Management, JUNOS 9.5 Security Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/config-usb-modem-chapter.html#config-usb-modem-chapter)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.3

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

3.2 Family Inet VRRP-Group (Interface Redundancy)

Virtual Router Redundancy Protocol (VRRP) allows administrators to create Virtual IP Addresses (VIPs) for an interface.

The VIP is shared between two routers, with only one handling traffic while other acts as a backup.

VRRP settings are accessed under the `[edit interfaces <interface name> unit <unit number> family inet vrrp-group]` hierarchy.

Authentication for VRRP Groups is only supported for IPv4 VIPs and not for IPv6 (family inet6), so recommendations are only given for family inet VRRP Groups. This is because VRRP v2 (RFC3768) and VRRPv3 (RFC5798 -which introduced support for IPv6 alongside IPv4 VIPs) removed support for authentication. The protocol developers felt that the protections too often resulted in operational or configuration issues, while not protecting against various ARP poisoning and VRRP Multi Master type attacks.

Please see **Section 9 - Security Considerations** of RFC5798 for a more complete discussion of these changes and suggested work arounds.

JUNOS devices running VRRPv2 (the default) for IPv4 VIPs *do* implement authentication through backward compatibility extensions to support RFC2338 authentication mechanisms. Because of the move away from authentication in the protocol, settings in this section are given as Level 2 Recommendations to provide information on these security options and for consideration by administrators with specific security concerns.

Only apply the recommendations in this section where one or more interfaces are configured to use VRRP. You can confirm the number of configured VRRP groups by issuing the following command from the `[edit]` *hierarchy:*

```
show | display set | match "family inet.*vrrp-group.*virtual-address" | count
```

If a positive integer is returned then you should consider applying all of the recommendations in this section for every configured VRRP Group.

3.2.1 Ensure VRRP authentication-key is set (Automated)

Profile Applicability:

- Level 2

Description:

VRRP authentication should be used where other security mechanisms are not in place.

Rationale:

VRRP provides resilience for a routers interfaces, allowing another router to act as backup in the event of a partial or complete failure of the primary router and increasing the availability network resources as well as resilience to DoS attack.

Routers configured to share a Virtual IP Address using VRRP communicate their status to their peer on a regular basis using a multicast packet, allowing a Master for the VIP to be elected. It is the Master that deals with packets destined for the VIP address.

If no authentication is used an attacker could potentially disrupt the VRRP Master Election process, causing neither router to handle packets destined for the VIP and resulting a DoS.

An authentication key can be configured for all VRRP Groups used on the device to help protect against this.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show | find "vrrp-group" | match "authentication-key" | count
```

The above command should return an integer equal to the number of VRRP Groups configured, which can be obtained by executing the following command:

```
[edit]
user@host#show | match "vrrp-group" | count
```

Remediation:

If you have configured VRRP on one or more interfaces you should configure authentication using the following commands from the `[edit interfaces <interface name> unit <unit number> family inet address <ip address>]` hierarchy;

```
[edit interfaces `<interface name> unit <unit number> family inet address <ip
address>`]
user@host#set vrrp-group <group number> authentication-key <key>
```

Default Value:

VRRP is not configured by default

References:

1. Configuring VRRP Authentication (IPv4 Only), JUNOS 9.5 High Availability Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-system-basics/archival.html%23id-11141986)

Additional Information:

Authentication for VRRP Groups is only supported for IPv4 VIPs and not for IPv6 (family inet6), so recommendations are only given for family inet VRRP Groups. This is because VRRP v2 (RFC3768) and VRRPv3 (RFC5798 -which introduced support for IPv6 alongside IPv4 VIPs) removed support for authentication. The protocol developers felt that the protections too often resulted in operational or configuration issues, while not protecting against various ARP poisoning and VRRP Multi Master type attacks.

It is recommended that other protections be used as the primary mechanism to protect VRRP from mis-use, with authentication only used as an (optional) additional layer of protection. Specifically, Layer 2 access switches should implement DHCP Snooping for IPv4 and ND Inspection for IPv6 networks or equivilent protections from other vendors.

Please see Section 9 - Security Considerations of RFC5798 for a more complete discussion of these changes and suggested workarounds.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.2.2 Ensure authentication-type is set to MD5 (Automated)

Profile Applicability:

- Level 2

Description:

Any VRRP authentication should use MD5 HMAC

Rationale:

VRRP provides resilience for a routers interfaces, allowing another router to act as backup in the event of a partial or complete failure of the primary router and increasing the availability network resources as well as resilience to DoS attack.

Routers configured to share a Virtual IP Address using VRRP communicate their status to their peer on a regular basis using a multicast packet, allowing a Master for the VIP to be elected. It is the Master that deals with packets destined for the VIP address.

If no authentication is used an attacker could potentially disrupt the VRRP Master Election process, causing neither router to handle packets destined for the VIP and resulting a DoS.

VRRP supports simple authentication and MD5. Simple authentication transmits the password in plain text so should *not* be used. MD5 authentication uses a Keyed Hash Authentication Message Code (HMAC), a techniques which uses a key combined with a cryptographic hash algorithm to verify the authenticity and integrity of the received packet.

Audit:

From the command prompt, execute the following command:

```
user@host>show vrrp detail | match "Authentication type: md5" | count
```

Remediation:

If you have configured VRRP on one or more interfaces you can configure authentication using MD5-HMAC with the following commands from the `[edit interfaces <interface name> unit <unit number> family inet address <ip address>]` hierarchy;

```
[edit interfaces <interface name> unit  <unit number> family inet address <ip
address>]
user@host#set vrrp-group <group number> authentication-type md5
```

Default Value:

VRRP authentication is not enabled by default

References:

1. Configuring VRRP Authentication (IPv4 Only), JUNOS 9.5 High Availability Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-system-basics/archival.html%23id-11141986)

Additional Information:

Authentication for VRRP Groups is only supported for IPv4 VIPs and not for IPv6 (family inet6), so recommendations are only given for family inet VRRP Groups. This is because VRRP v2 (RFC3768) and VRRPv3 (RFC5798 -which introduced support for IPv6 alongside IPv4 VIPs) removed support for authentication. The protocol developers felt that the protections too often resulted in operational or configuration issues, while not protecting against various ARP poisoning and VRRP Multi Master type attacks.

It is recommended that other protections be used as the primary mechanism to protect VRRP from mis-use, with authentication only used as an (optional) additional layer of protection. Specifically, Layer 2 access switches should implement DHCP Snooping for IPv4 and ND Inspection for IPv6 networks or equivilent protections from other vendors.

Please see Section 9 - Security Considerations of RFC5798 for a more complete discussion of these changes and suggested workarounds.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

3.3 Ensure unused interfaces are set to disable (Manual)

Profile Applicability:

- Level 1

Description:

Unused interfaces should be explicitly disabled.

Rationale:

JUNOS routers can be installed with tens or even hundreds of physical interfaces of different types. To ensure that unused interfaces are not connected to networks, either accidently or by a malicious user seeking to bypass security measures, all unused interfaces should be explicitly disabled.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces <interface name>
```

The following output should be returned

```
<interface name> {
      disable;
}
```

Please note that other configuration items related to the interface may also appear between the curly braces.

Remediation:

To disable an interface enter the following command from the `[edit interfaces <interface name>]` hierarchy.

```
[edit interfaces <interface name>]
user@host#set disable
```

Default Value:

Installed physical interfaces are enabled by default on most platforms.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.4 Ensure interface description is set (Automated)

Profile Applicability:

- Level 1

Description:

All interfaces should have a description.

Rationale:

JUNOS routers can be installed with tens or even hundreds of physical and logical interfaces of different types. To allow effective planning, troubleshooting and to avoid confusion & mistakes which may compromise your networks security, all interface units should have a description configured.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | match "description" | count
```

The returned value should be a positive integer equal to the number of configured interface units.

Remediation:

To configure an interface description enter the following command from the[edit interfaces unit] hierarchy.

```
[edit interfaces <interface name> unit <unit number>]
user@host#set description <description>
```

Default Value:

Descriptions are not set by default.

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

3.5 Ensure proxy-arp is disabled (Automated)

Profile Applicability:

- Level 2

Description:

Do not use Proxy ARP.

Rationale:

Address Resolution Protocol (ARP) provides resolution between IP and MAC Addresses (or other Network and Link Layer addresses on none IP networks) within a Layer 2 network.

Proxy ARP is a service where a device connected to one network (in this case the JUNOS router) answers ARP Requests which are addressed to a host on another network, replying with its own MAC Address and forwarding the traffic on to the intended host.

Sometimes used for extending broadcast domains across WAN links, in most cases Proxy ARP on enterprise networks is used to enable communication for hosts with mis-configured subnet masks, a situation which should no longer be a common problem.

Proxy ARP effectively breaks the LAN Security Perimeter, extending a network across multiple Layer 2 segments. Using Proxy ARP can also allow other security controls such as PVLAN to be bypassed.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | match "proxy-arp" | count
```

The returned value should return 0 or null.

Remediation:

To disable Proxy ARP enter the following command from the `[edit interfaces <interface name> unit <unit number>]` hierarchy:

```
[edit interfaces <interface name> unit <unit number>]
user@host#delete proxy-arp
```

Default Value:

Proxy ARP is disabled by default on most JUNOS routers.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.2 (page 75), National Security Agency (NSA)

Additional Information:

Proxy ARP is required in certain circumstances on some devices. The most common instance of this will be on a Firewall device which is performing NAT using an address in the same subnet as the ingress/egress interface but different to the interface address.

This scenario is described in Juniper KB21785

If Proxy ARP is required to support NAT or similar functions it should be configured *only* on those interfaces where it is explicitly required.

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

3.6 Ensure ICMP Redirects are set to disabled (on all untrusted IPv4 networks) (Manual)

Profile Applicability:

- Level 1

Description:

The Routing Engine should not send ICMP Redirect Messages.

Rationale:

ICMP Redirect Messages provide a method for a router to communicate routing information with a host and is intended for use when a router receives packets to forward to a destination to which the host should have a direct route. In a well designed, modern, network ICMP Redirects should not be needed or add any useful functionality.

An attacker may abuse this feature to obtain topology information about a target network and potentially identify weaknesses for later exploitation or to target the router and hosts with Denial of Service (DoS) or Man in the Middle (MITM) attacks.

To prevent this abuse, ICMP Redirect message generation should be disabled globally where it is not required as discussed in Recommendation 6.15.10 Ensure ICMP Redirects are Disabled for IPv4. Where this is not possible, ICMP Redirects can be disabled on a per Interface basis and should be disabled for all Untrusted networks, such as the Internet, or subnets where this functionality is not required.

Impact:

In some networks, for instances where subnets populated by hosts include multiple non-redundant gateways, removing redirects may result in traffic being doubled on some gateways interfaces as traffic is received and then forwarded on the same port.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | match "no-redirects" | count
```

The above command should return an integer value equal to the number of untrusted interfaces on the device. Because this is a subjective value, this recommendation is not scored.

Remediation:

To disable ICMP Redirect message generation on an untrusted network interface, issue the following command from the `[edit interfaces]` hierarchy;

```
[edit interfaces]
user@host#set <interface name> unit <unit number> family <address family> no-
redirects
```

Default Value:

By default the ICMP Redirect messages are generated.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-redirects-edit-system.html
2. http://www.cymru.com/gillsr/documents/icmp-redirects-are-bad.pdf

Additional Information:

Ensure that your hosts are not reliant on ICMP Redirect messages for routing before disabling this feature.

It is prefered to disable ICMP Redirects globally, as covered in Recommendation 6.15.10 Ensure ICMP Redirects are Disabled for IPv4 . This Recommendation is non-scorable and is given only as an alternative method for networks where this is not possible.

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

3.7 Ensure ICMP Redirects are set to disabled (on all untrusted IPv6 networks) (Manual)

Profile Applicability:

- Level 1

Description:

The Routing Engine should not send ICMP Redirect Messages.

Rationale:

ICMP Redirect Messages provide a method for a router to communicate routing information with a host and is intended for use when a router receives packets to forward to a destination to which the host should have a direct route. In a well-designed, modern, network ICMP Redirects should not be needed or add any useful functionality.

An attacker may abuse this feature to obtain topology information about a target network and potentially identify weaknesses for later exploitation or to target the router and hosts with Denial of Service (DoS) or Man in the Middle (MITM) attacks.

To prevent this abuse, ICMP Redirect message generation should be disabled globally where it is not required as discussed in Recommendation 6.15.11 Ensure ICMP Redirects are Disabled for IPv6. Where this is not possible, ICMP Redirects can be disabled on a per Interface basis and should be disabled for all untrusted networks, such as the Internet, or subnets where this functionality is not required.

Impact:

In some networks, for instances where subnets populated by hosts include multiple non-redundant gateways, removing redirects may result in traffic being doubled on some gateways interfaces as traffic is received and then forwarded on the same port.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces | match "no-redirects-ipv6;" | count
```

The above command should return an integer value equal to the number of untrusted interfaces on the device where IPv6 is configured. Because this is a subjective value, this recommendation is not scored.

Remediation:

To disable ICMP Redirect message generation on an untrusted network interface, issue the following command from the `[edit interfaces]` hierarchy;

```
[edit interfaces]
user@host#set <interface name> unit <unit number> family <address family> no-
redirects
```

Default Value:

By default the ICMP Redirect messages are generated.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-redirects-ipv6-edit-system-interfaces-ex-series.html
2. http://www.cymru.com/gillsr/documents/icmp-redirects-are-bad.pdf

Additional Information:

Ensure that your hosts are not reliant on ICMP Redirect messages for routing before disabling this feature.

It is prefered to disable ICMP Redirects globally, as covered in Recommendation 6.15.11 Ensure ICMP Redirects are Disabled for IPv6 . This Recommendation is non-scorable and is given only as an alternative method for networks where this is not possible.

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

3.8 Ensure Loopback interface address is set (Automated)

Profile Applicability:

- Level 2

Description:

Configure a Loopback address.

Rationale:

When a router needs to initiate connections to remote hosts, for example for SYSLOG or NTP, it will use the nearest interface for the packets source address. This can cause issues due to the possible variation in source, potentially causing packets to be denied by intervening firewalls or handled incorrectly by the receiving host.

To prevent these problems the router should be configured with a Loopback interface and any services should be bound to this address.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces lo0
```

The following should be returned:

```
unit 0 {
      family inet {
            address <ip address/mask>;
      }
}
```

Additional configuration items for the Loopback interface may also be present between the curly braces.

Remediation:

To create a loopback interface enter the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
user@host#set lo0 unit 0 family inet address <ip address>
```

Default Value:

No Loopback Address is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.1.4 (page 58), National Security Agency (NSA)

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.9 Ensure only one loopback address is set (Automated)

Profile Applicability:

- Level 1

Description:

Configure only one Loopback address per Routing Instance

Rationale:

Multiple Loopback addresses create potential for abuse, mis-configuration and confusion. A maximum of one address per address family should be set on the system's loopback address in each Routing Instance.

Alternative Loopback addresses should be configured with caution and, where they must be used, should be clearly documented.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show interfaces lo0 | family | count

[edit]
user@host#show interfaces lo0 | address | count
```

The first command should return the number of address families configured on the Loopback interface. The second command returns the number of addresses configured on the Loopback interfaces.
Both commands should return the same number.

Remediation:

To remove an additional loopback addresses enter the following command from the `[edit interfaces]` hierarchy for each address to be removed:

```
[edit interfaces]
user@host#delete lo0 unit <unit number> family <address family> address
<address to be removed>
```

Default Value:

No Loopback Address is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.1.4 (page 58), National Security Agency (NSA)

Additional Information:

For systems with multiple configured Routing Instances a separate loopback interface unit *may* be used per instance. Where this is the case one address per family may be configured per routing instance.

For systems configured with multiple Logical Systems, additional Loopbacks may be configured per LSYS. The remediation and audit procedures given here do not include instructions for these systems, which should be audited on a per LSYS basis.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.10 Ensure inbound firewall filter is set for Loopback interface (Automated)

Profile Applicability:

- Level 2

Description:

A Firewall Filter should be applied to lo0.

Rationale:

JUNOS routers can provide a wide range of services to the network and, as with any computer system, the more services that are offered and the more hosts they are available to, the wider attack surface is offered to a potential attacker.

To protect the router from attack a Firewall Filter should be applied to all inbound traffic to the Routing Engine which limits the hosts able to connect to the router and the services on which they are permitted to connect.

If applied to the `lo0` interface the filter will apply to all traffic sent to the Routing Engine rather than to traffic traversing the router. Where IPv6 traffic is also handled by the router a firewall filter will also need to be applied for `family inet 6`.

See the Firewall section for details of how to configure Firewall Filters.

NOTE : The Firewall Filter applies to ALL traffic sent to the Routing Engine, including traffic sent to the routers interface addresses. Ensure your firewall filter allows all of the Routing, Management and other protocols which are required for normal operation prior to applying the filter.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show interfaces lo0 unit 0 family <address family> filter input
```

The name of the configured firewall filter should be returned.

Remediation:

To apply a firewall filter to the loopback interface enter the following command from the `[edit interfaces]` hierarchy:

```
[edit interfaces]
user@host#set lo0 unit 0 family inet filter input <filter name>
```

Default Value:

No firewall filters are configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.1 (page 55), National Security Agency (NSA)

CIS Controls:

Version 7

9.1 Associate Active Ports, Services and Protocols to Asset Inventory
Associate active ports, services and protocols to the hardware assets in the asset inventory.

4 Protocols

A wide range of protocols are configured at this hierarchy, including Routing protocols, MPLS and PIM. Routing protocols in particular, are a fundamental part of what makes a router tick. JUNOS supports a wide range of routing protocols, the parameters for which are contained under the `[edit protocols]` hierarchy.

Because JUNOS allows the creation of Logical Routers and multiple Routing Instances on some platforms, routing may also be configured at other hierarchies.

For instance IS-IS may be configured at the `[edit protocols isis]` level, the `[edit logical-routers <logical router name> protocols isis]`, `[edit logical-routers <logical router name> routing-instances <routing instance name> protocols isis]` and the `[edit routing-instances <routing instance name> protocols isis]`.

These latter hierarchies are essentially copies of the `[edit protocols isis]` configuration options. Any recommendations that apply to the protocol at this level, equally apply the protocol when it is configured at other levels.

4.1 BGP

Border Gateway Protocol (BGP) is the core routing protocol of the Internet and is also commonly used on the internal core networks of larger Enterprises and Service Providers. Exterior Gateway Routing Protocols in general and BGP in particular are complex systems; it is beyond the scope of this benchmark to give even an overview of how BGP operates on Juniper routers.

BGP parameters for JUNOS routers are configured under the `[edit protocols bgp]` hierarchy.

Only apply the recommendations in this section where one or more instances of BGP are configured on the device. You can confirm the number of configured BGP instances by issuing the following command from the `[edit]` hierarchy:

```
[edit]

user@host#show | match "logical-system|routing-instance|protocols|bgp {"
```

If the term `bgp {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.1.1 Ensure peer authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

BGP Peers should be authenticated.

Rationale:

Where it is deployed, BGP routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers BGP neighbors may inject incorrect information into the route table resulting in DOS attack or loss of confidential data through a Man in the Middle attack.

On Juniper routers (as well as routers from other manufacturers such as Cisco or Brocade) it is possible to authenticate neighbors using an MD5 digest of elements of the TCP segment, creating a signature which can be verified without ever needing to transmit the password. This method is described in RFC 2385.

Audit:

Enter the following command from operational mode:

```
user@host>show bgp neighbor | match "Authentication key is configured" |
count
```

The above command should return a positive integer equal to the number of configured BGP Neighbors.

Remediation:

If you have deployed BGP in your network you should authenticate all neighbors. Authentication can be configured at the Global, Group or Neighbor level, with more specific settings overriding less specific. For eBGP a different MD5 password should be configured for each neighbor or peer. For iBGP neighbors the same key may be used globally or different keys may be used by group or neighbor as appropriate to your infrastructure. To configure BGP Authentication at the globally enter the following command at the `[edit protocols bgp]` hierarchy:

```
[edit protocols bgp]
user@host#set authentication-key <md5 key>
```

To configure BGP Authentication at the group level enter the following command at the `[edit protocols bgp]` hierarchy:

```
[edit protocols bgp]
user@host#set group <group name> authentication-key <md5 key>
```

Finally, to configure BGP Authentication at the neighbor level enter the following command at the `[edit protocols bgp group <group name>]` hierarchy:

```
[edit protocols bgp group <group name>]
user@host#set neighbor <neighbor IP> authentication-key <md5 key>
```

Remember that more specific settings override less specific settings, so a key set at the neighbor level will be used even if keys are also set at the group and global levels.

Default Value:

No BGP routing is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.5 (page 123), National Security Agency (NSA)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on both neighbors which may require coordination with your external peers. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.1.2 Ensure peer authentication is set to IPSEC SA (Manual)

Profile Applicability:

- Level 2

Description:

BGP Neighbors should be strongly authenticated.

Rationale:

Where it is deployed, BGP routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network.

An attacker posing as one of the target routers BGP neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack. As well as MD5 hash based authentication, JUNOS routers can also authenticate BGP neighbors using IPSEC Security Associations. This allows more robust authentication mechanisms to be used and is recommended as an alternative to MD5 HMAC in high security environments.

Although M, T and MX series devices normally require a Services PIC or DPC installed to use IPSEC tunnels, no additional hardware is required for IPSEC SA based authentication of BGP neighbors. As with MD5 HMAC, IPSEC SA based Authentication can be configured Globally, at the Group Level or at the Neighbor Level, with more specific settings overriding less specific settings.

Because IPSEC SA Authentication is intended for use in high security environments, it is recommended that different parameters are configured for each neighbor, particularly where eBGP is used.

Audit:

Due to the range of options for configuring IPSEC SA based Authentication with BGP, this recommendation is not scorable.

Remediation:

To setup IPSEC SA based authentication, first configure a Security Association at the `[edit security ipsec]` hierarchy;

```
[edit security ipsec]
edit security-association <SA name>
set description <description>
set mode transport
set manual direction bidirectional protocol ah
set manual direction bidirectional authentication algorithm <authentication
method>
set manual direction bidirectional authentication key <key>
```

The SA must be bi-directional and must be configured with the same parameters on all neighbors reachable on the intended interface. Note that only Authenticated Header is configured in this example which provides mutual authentication but *does not encrypt BGP protocol messages in transit*.
To configure IPSEC SA based authentication globally for BGP, issue the following command from the `[edit protocols bgp]` hierarchy;

```
[edit protocols bgp]
user@host#set ipsec-sa
```

To configure IPSEC SA based authentication for a group, issue the following command from the `[edit protocols bgp group <group name>]` hierarchy;

```
[edit protocols bgp group <group name>]
user@host#set ipsec-sa <SA name>
```

To configure IPSEC SA based authentication for a neighbor, issue the following command from the `[edit protocols bgp group <group name> neighbor <neighbor ip address>]` hierarchy;

```
[edit protocols bgp group <group name> neighbor <neighbor ip address>]
user@host#set ipsec-sa <SA name>
```

Default Value:

No BGP routing is configured by default.

References:

1. Applying IPSEC Security Association, JUNOS Software Routing Configuration Guide, Juniper Networks

Additional Information:

Security Associations must be configured correctly on all neighbors reached through interfaces where IPSEC based authentication is configured for BGP to continue to function.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.1.3 Ensure EBGP peers are set to use GTSM (Automated)

Profile Applicability:

- Level 1

Description:

GTSM should be used with all EBGP peers.

Rationale:

Where it is deployed, External BGP routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic destined for external networks. An attacker may attempt to exhaust the routers CPU and memory resources by flooding a target router with fake routing updates, resulting in a DoS condition. Potentially an attack may also inject fake routing information into the route table.

General TTL Security Mechanism (GTSM) is defined in RFC5082 and takes advantage of the fact that routers normally peer with adjacent neighbors, i.e. with routers only 1 hop away. GTSM uses the Time to Live (TTL) field of routing update packets to determine whether or not the packet originated from an adjacent router, denying those which do not.

Juniper routers effectively implement GTSM by default. Administrators can use the `multihop` command hierarchy to increase the maximum acceptable TTL for route updates, allowing updates from non adjacent peers. When peering with adjacent routers then multihop should not be configured, using the default to effectively configure GTSM with a TTL limit of 254 (or 1 hop). If your network requires peering with routers more than 1 hop away (non adjacent peers), multihop should be configured on a per peer or per group basis with the minimum possible value so as to limit the distance, in terms of networks, from which an attack can be launched.

Audit:

Enter the following command from operational mode:

```
[edit]
user@host#show protocols bgp | match "multihop" | count
```

The above command should return an integer indicating the number of occasions that multihop is defined. In most cases, where adjacent peers are used, the returned value should be 0 (or 1 if peering with the Team Cymru Bogon Route Server).

Remediation:

If you have deployed multihop in your network but do not have any peers more then 1 hop away, disable multihop with the following command from the `[edit protocols bgp]`, `[edit protocols bgp group <group name>]` or `[edit protocols bgp group <group name> neighbor <neighbor address>]` depending at which level you have configured multihop;

```
[edit protocols bgp]
user@host#delete multihop
```

To change the number of hops distance from which a route update can originate, enter the following command from the `[edit protocols bgp group <group name>]` to apply multihop to a group or `[edit protocols bgp group <group name> neighbor <neighbor address>]` to apply multihop to a single neighbor;

```
[edit protocols bgp group <group name>]
user@host#set multihop ttl <number of hops>
```

Remember that, in both cases, more specific settings override less specific ones. So if multihop is set to 5 at the neighbor level, but the default of 1 at the global level, the neighbor level setting will apply for communications with that peer.

Default Value:

A TTL of 1 is used by default on eBGP sessions and a default TTL of 64 is used for iBGP.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.5 (page 123), National Security Agency (NSA)

CIS Controls:

Version 7

11 <u>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</u>
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

4.1.4 Ensure Bogon Filtering is set (where EBGP is used) (Manual)

Profile Applicability:

- Level 2

Description:

Bogon prefixes should be filtered when using eBGP.

Rationale:

Bogon Networks are those IP Address blocks which should never appear on the Internet. Examples include loopback addresses, RFC1918 private addresses and IP blocks which have not yet been assigned by the IANA (Internet Assigned Numbers Authority) to one of the RIRs (Regional Internet Registries). If traffic arrives at your network edge from a Bogon network, the traffic is almost certainly malicious and should be filtered. Studies have shown instances where as much as 60% of DoS attack traffic is being sourced from Bogon or Martian (a subset which includes RFC1918 and RFC3330 networks) addresses.

As a rule Bogon traffic should also be filtered from leaving the network as it may be malicious or represent a possible information leak. Either way, return traffic would not get back. Bogon information can be obtained from a number of sources such as:

- IANA - Obtain the current IPv4 assignments list, anything that is shown as *Unallocated* or *Reserved* is a Bogon.
- *Team Cymru* provides, what is effectively, the definitive Bogon list in a range of formats and through a BGP Route Server project.
- *RIPE NCC* also provides lists of Unallocated, Martian and combined Bogon space.

An important point to remember about Bogon filtering is that the addresses that make up Bogon space *change*. Unallocated addresses get allocated, reserved networks may be re-purposed, etc. If you keep your Bogon filters static, you may accidently block valid traffic from these addresses. *Ensure you have a procedure to keep your Bogon lists up to date!*

Audit:

Not scored or auditable.

Remediation:

JUNOS offers a variety of options for filtering Bogons and Martians, which is why this item is not scored. Some of the more common options are discussed below.
1 - The Martian Table Most Martian space (but not all, else you would not be able to use

your router on private networks) is blocked using the Martian Routing Table, which is discussed elsewhere in this Benchmark and configured under the `[edit routing-options martians]` hierarchy. Route updates for prefixes in this special table are ignored, so adding Bogons here will prevent them being learned through *any* routing protocol.

2 - Ingress Prefix Filtering Ingress Filtering should be used on eBGP sessions to prevent your own prefixes being advertised back to your network or, in the case of ISP networks, customer networks advertising prefixes other than those allocated to them.

The other filtering types are covered previously. Prefix lists are configured under the `[edit policy-options]` hierarchy, but are discussed here as they are applied under the `[edit protocols bgp <group name>]` hierarchy. First configure a policy:

```
[edit policy-options]
user@host#edit policy-statement <policy name> term <term name>
[edit policy-options policy-statement <policy name> <term name>]
user@host#set from route-filter <network>/<mask> <exact | orlonger | prefix-
length-range <start>-<end>> reject
```

The last stage should be repeated for each prefix required, but as several options are shown, a couple of examples are given below:

```
[edit policy-options <policy name> <term name>]
user@host#set from route-filter 0.0.0.0/0 exact reject
user@host#set from route-filter 10.0.0.0/8 orlonger reject
user@host#set from route-filter 0.0.0.0/0 prefix-length-range /29-/32 reject
```

The first line in the example rejects a default route advertised to the router and only that route. The second line will filter any route from the 10.0.0.0/8 range, for instance 10.1.1.0/24 or 10.2.0.0/16. The final line is a little more complex, this will reject any route with a mask length of /29, /30, /31 or /32 (generally eBGP routes should be summarized into larger prefixes than this). Having defined a policy, we need to apply it.

As with most other BGP configuration options, you can apply the policy at Global, Group or Neighbor levels as suites your needs. In this example we will apply the policy to a group containing all our eBGP peers:

```

[edit protocols bgp group <group name>]
user@host#set import <policy name/s>
```

3 - Peering with a Bogon Route Server As far as I am aware, the idea of using a BGP Peering session to a Route Server for updates on Bogon networks was hatched by Team Cymru and they offer a free, public Bogon Route Server, which you can peer with to keep you Bogon list up to date. The theory works equally well by peering to a route server of your own, allowing a greater degree of control over your Bogon list updates for your organization if desired. First a static route is created and configured to discard traffic. An address that is reserved for Test or Example networks is used, you may need to allow this /32 prefix in the Martian Table:

```
[edit routing-options]
user@host#set static route 192.0.2.1/32 discard no-readvertise retain
```

An import policy should be set to match prefixes from the route servers AS and the Community (if used) for Bogon updates, setting the next hop to 192.0.2.1 and accepting the route.

```
[edit policy-options]
user@host#edit policy-statement <policy name> term <term name>
[edit policy-options policy-statement <policy name> term <term name>]
user@host#set from protocol bgp as-path <peer AS> community <community>
user@host#set then next-hop 192.0.2.1
```

Finally the BGP Peering and Group is configured with the import policy above and not to export. In addition security options covered in other recommendations should be used:

```
[edit protocols bgp <group name>]
user@host#set type external description "bogon route servers"
user@host#set import <policy name>
user@host#set peer-as <AS of Route Server>
user@host#set neighbor <neighbors IP>
user@host#set local-address <local IP to use for peering>
```

Default Value:

Most Martians are filtered by default, most Bogons are not.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.5 (page 123), National Security Agency (NSA)
2. The Bogon Reference, Team Cymru (http://www.team-cymru.org/Services/Bogons/)
3. IPv4 Address Space Registry, Internet Assigned Numbers Authority (IANA) (http://www.iana.org/assignments/ipv4-address-space/)

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

4.1.5 Ensure Ingress Filtering is set for EBGP peers (Manual)

Profile Applicability:

- Level 1

Description:

Filter prefixes advertised to the router through eBGP.

Rationale:

In addition to filtering Bogon and Maritan routes JUNOS routers peering with eBGP neighbors should also apply Ingress Filtering to prevent the router processing bad updates sent from the neighbor router, either maliciously or by accident. At a minimum prefix filters should deny any prefix which belong to your own AS. Depending on your type of deployment you may also wish to block prefixes which are more specific than those issues by RIR's or limit ISP customers to advertising those prefixes which you have assigned to them.

Audit:

Because a policy may be applied at one or more different levels depending on the requirements of a specific organization, it is not possible to score this recommendation.

Remediation:

From the `[edit policy-options]` hierarchy, define a new policy by issuing the following commands:

```
[edit policy-options]
user@host#edit policy-statement <policy name> term <term name>
[edit policy-options policy-statement <policy name> term <term name>]
user@host# set from route-filter <network>/<mask> <exact | orlonger | prefix-
length-range <start>-<end>> reject
```

Now apply the policy, either globally, to a group or to an individual peer as required by your environment.

```
[edit protocols bgp <group name>]
user@host#set import <policy name>
```

Default Value:

No Ingress Filtering is applies by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.5 (page 123), National Security Agency (NSA)

Additional Information:

As a rule, you should not apply strict ingress filters on Transit peers, as for these providers you should expect to receive advertisements for prefixes which originate outside of the peer network.

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

4.1.6 Ensure RPKI is set for Origin Validation of EBGP peers (Manual)

Profile Applicability:

- Level 2

Description:

Use RPKI for Origin Validation on Public BGP Peering

Rationale:

In addition to filtering Bogon and Maritan routes JUNOS routers peering with eBGP neighbors should also apply Ingress Filtering to prevent the router processing bad updates sent from the neighbor router, either maliciously or by accident.

Traditional Ingress Filtering, outlined in Recommendation 4.1.5 Ensure Ingress Filtering is set for EBGP peers, uses manually administrated Routing Policy configured on individual routers to validate prefixes being received from BGP Neighbours in Peer *Autonomous Systems (ASs)* based on *Internet Routing Registry (IRR)* entries.

This technique is maintenance intensive and prone to errors, although semi automated tools do exist to help. It is also not readily enforceable on *Transit* Connections, where the router does not connect directly to the *Origin AS*, but instead receives their routes via a *Transit Service Provider*. The receiving AS has no option but to trust that their upstream provider/s are correctly implementing filtering, with no way to validate the routing information they receive independently.

This leaves BGP Routing prone to *Hijack Attacks*, with numerous incidents in recent years causing issues both with reachability for some prefixes/ASs and with theft of information, after traffic is re-routed to fake destinations.

To combat this the *Resource Public Key Infrastructure (RPKI)* framework was created to allow Public ASs to sign their *Resources* (IPv4 and IPv6 Prefixes they will originate) by creating a *Route Origination Authorizations (ROA)* Certificate, through their *Regional Internet Registry (RIR)* (AFRINIC, ARIN, APNIC, LACNIC or RIPE NCC).

Public ASs can perform *Origin Validation* on the routes received through BGP, whether from direct Peer networks or through a Transit Provider. The Junos Router does this by checking the route information it receives through BGP with a *RPKI Validator Server* (sometimes called an *RPKI Cache Server*) through the *RPKI-RTR* Protocol defined in RFC 8210. The RPKI Validator maintains a cache of ROAs distributed by the RIRs and returns a verdict to the Router, which may be either:

- *Valid* - The AS, Prefix and Prefix Length all match a valid ROA
- *Invalid* - A matching ROA exists for the Prefix, but either the Origin AS or the Prefix Length does not match
- *Unknown* or *Not Found* - No matching ROA exists, most likely the Resource Owner has not created an RPKI with their RIR

Routing Policy on the Junos device is configured to determine whether routes should be accepted based on results returned by the RPKI Validator. Most commonly Valid and Unknown/Not Found routes will be accepted and Invalid rejected, but this should be determined by the policy of each individual AS.

A full discussion of RPKI is beyond the scope of this Benchmark, but is covered in detail in the Juniper TechLibary BGP Origin Validation Using Resource Public Key Infrastructure, available for free from the Juniper website.

RIPE NCC, one of the RIRs, provide detailed instructions for installing several common RPKI Validators (including their own) in How to Install an RPKI Validator.

Impact:

Incorrect configuration of any Route Filtering may impact on reachability

Audit:

Because a policy may be applied at one or more different levels depending on the requirements of a specific organization, it is not possible to automatically score this recommendation.
You can confirm a RPKI Validator Server is configured by issuing the following command from the `[edit routing-options]` configuration hierachy:

```
[edit routing-options]
user@host# show validation
```

If a RPKI Validator is configured, details will be returned.
In the example below, the RPKI Validator Server's IP Address is 10.10.0.100, the RPKI-RTR protocol is running on TCP Port 8323 (the standard port for the RIPE NCC RPKI Validator, this may vary for other servers) and the local IP used to by the Junos Router for the session is 10.10.0.200:

```
[edit routing-options]
user@host# show validation
validation {
        group rpki-validator {
                session 10.10.0.100 {.
                        port 8323;
                        local-address 10.10.0.200;
                }
        }
}
```

Multiple RPKI Validators can be configured and additional options may also be present.
If multiple Logical Systems are in use, RPKI Origin Validation may need to be configured separately for all which are performing Public BGP peering.
Junos Routers use a Routing Policy to determine what action to take for a route based on the response from the RPKI Validator. This should be applied to all Group's or Neighbours which will be performing Public BGP Peering and can be checked by issuing the following command from the `[edit protocols]` configuration hierarchy:

```
[edit protocols]
user@host# show bgp group <group-name>
```

Where `<group-name>` is the group or groups used for Public BGP Peering (this will often be several groups). In the example below the `rpki-validation` policy is applied to routes received by the `transit1` group:

```
[edit protocols]
user@host# show bgp group transit1
type external;
import rpki-validation;
export export-direct;
peer-as 64510
neighbor 203.0.113.10
neighbor 203.0.113.11
```

To confirm the configured RPKI Policy, issue the following command from the `[edit policy-options]` configuration hierarchy:

```
[edit policy-options]
user@host# show policy-statement <policy name>
```

Where `<policy name>` is the policy configured for the Group or Neighbour in the previous command (in our example `rpki-validation`) :

```
[edit policy-options]
user@host# show policy-statement rpki-validation
term valid {
        from {
                protocol bgp;
                validation-database valid;
        }
        then {
                validation-state valid;
                accept;
        }
}
```

```
term invalid {
        from {
                protocol bgp;
                validation-database invalid;
        }
        then {
                validation-state invalid;
                reject;
        }
}
term unknown {
        from protocol bgp;
        then {
                validation-state unknown;
                accept;
        }
}
```

In this case the Policy will `accept` routes for which the RPKI Validator returns Valid or Unknown and will `reject` routes which are Invalid.

Remediation:

Configuration and deployment of an RPKI Validator and a full discussion of all configuration options is beyond the scope of this Benchmark.
To configure an RPKI Validator Server, issue following commands from the `[edit routing-options]` configuration hierarchy:

```
[edit routing-options]
user@host# set validation group <group-name> session <RPKI Server IP> port
<RPKI Server Port> local-address <Local IP>
```

Where:

- `<group-name>` is a descriptive name chosen for the RPKI Server
- `<RPKI Server IP>` is the IP address used on the RPKI Validator for the RPKI-RTR protocol
- `<RPKI Server Port>` is the port configured on RPKI Validator for the RPKI-RTR protocol
- `<Local IP>` is a Local Interface address that the Router should use as the source for RPKI-RTR sessions

**Note ** - If multiple Logical Systems are configured, RPKI Validation will need to be configured separately for all LSYS being used for Public BGP Peering.

Next create a Routing Policy to `accept` or `reject` routes based on the RPKI Validation Database, using the following commands for each term from the `[edit policy-options]` heirachy:

```
[edit policy-options]
user@host# set policy-statement <policy-name> term <term-name> from protocol
bgp
user@host# set policy-statement <policy-name> term <term-name> from
validation-database <RPKI Database Result>
user@host# set policy-statement <policy-name> term <term-name> then
validation-state <RPKI State>
user@host# set policy-statement <policy-name> term <term-name> then <action>
```

Where:

- `<policy-name>` is a descriptive name for the Routing Policy
- `<term-name>` is a descriptive name for the Term
- `<RPKI Database Result>` is the result returned by the RPKI Validator
- `<RPKI State>` is the RPKI State to be recorded locally for the route (normally the same as the RPKI Validator result)
- `<action>` is a Routing Policy action such as to `accept` or `reject` the route

These steps can be repeated until all of your required terms and actions are configured. Here we create the `rpki-validation` Routing Policy given in the Audit Procedure example:

```
[edit policy-options]
user@host# set policy-statement rpki-validation term valid from protocol bgp
user@host# set policy-statement rpki-validation term valid from validation-
database valid
user@host# set policy-statement rpki-validation term valid then validation-
state valid
user@host# set policy-statement rpki-validation term valid then accept
user@host# set policy-statement rpki-validation term invalid from protocol
bgp
user@host# set policy-statement rpki-validation term invalid from validation-
database invalid
user@host# set policy-statement rpki-validation term invalid then validation-
state invalid
user@host# set policy-statement rpki-validation term invalid then reject
user@host# set policy-statement rpki-validation term unknown from protocol
bgp
user@host# set policy-statement rpki-validation term unknown then validation-
state unknown
user@host# set policy-statement rpki-validation term unknown then accept
```

The final term matches on all BGP Routes which do not return either `valid` or `invalid` from the RPKI Server, so does not require the additional match condition on the `validation-database` result.
The RPKI Routing Policy should now be applied to all BGP Neighbours or Groups used for Public BGP peering using the following commands from the `[edit protocols bgp]` configuration heirachy:

```
[edit protocols bgp]
user@host# set group <group-name> import <policy-name>
```

OR

```
[edit protocols bgp]
user@host# set neighbor <Neighbor IP> import <policy-name>
```

Where:

- is the name of the BGP Group
- is the Routing Policy configured in the previous step
- is the IP Address of the individual neighbor to which policy will be applied

Note - *Other BGP Import policies may already be applied, it is important to ensure all policy is applied correctly and in the correct order to prevent disruption to the network.*

Default Value:

BGP Origin Validation is not configured by default

References:

1. Juniper TechLibary [BGP Origin Validation Using Resource Public Key Infrastructure](https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-187-bgp-rpki-tn.html),available for free from the Juniper website.
2. RIPE NCC [How to Install an RPKI Validator](https://labs.ripe.net/Members/tashi_phuntsho_3/how-to-install-an-rpki-validator)
3. RPKI Adoption - https://rpki-monitor.antd.nist.gov/#rpki_adopters
4. https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

4.2 ISIS

Intermediate System to Intermediate System (IS-IS) is a Link State Interior Gateway Routing Protocol similar in operation to OSPF. It is less popular on Enterprise networks than on Service Provider networks where it scales more effectively than OSPF.

IS-IS is a complex protocol, with many configuration options which may have effects which are not immediately obvious. Administrators should be familiar with the IS-IS protocol and their routing environment before applying recommendations in this section.

IS-IS parameters for JUNOS routers are configured under the `[edit protocols isis]` hierarchy.

Only apply the recommendations in this section where one or more instances of IS-IS are configured on the device. You can confirm the number and type of configured IS-IS instances by issuing the following command from the ''[edit]'' hierarchy:

```
[edit]

user@host#show | match "logical-system|routing-instance|isis {"
```

If the term `isis {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.2.1 Ensure IS-IS neighbor authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On Juniper routers (as well as routers from other manufacturers such as Cisco or Brocade) it is possible to authenticate neighbors using either Simple authentication or a Keyed Hash Based Message Authentication Check using an MD5 digest of elements in PDU combined with a sequence number to protect against Replay attacks and confirm authenticity.

Simple authentication sends the configured password as clear-text and should *never* be used. MD5 HMAC based authentication sends only a one way hash in the packets, providing authentication without exposing sensitive date, so should be used instead.

Authentication is configured for each IS-IS Level. More fine grained authentication for Hello packets may also be set at the interface level.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "authentication-" | except "-auth" | count
```

The above command should return '2' when both required statements are configured.

Remediation:

If you have deployed IS-IS in your network you should use MD5 authentication for all neighbors at each IS-IS Level configured.

To configure MD5 authentication and the secret key to be used, issue the following commands from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#set level <level> authentication-type md5
user@host#set level <level> authentication-key <key>
```

Default Value:

No IS-IS routing is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.3 (page 113), National Security Agency (NSA)
2. Configuring IS-IS Authentication, JUNOS Software Routing Protocols Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-routing/configuring-is-is-authentication.html#id-11133728)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on all routers in the IS-IS Area at the given level. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.2 Ensure IS-IS neighbor authentication is set to SHA1 (Automated)

Profile Applicability:

- Level 2

Description:

IS-IS Neighbors should be authenticated with stronger SHA1 HMAC mechanism, where supported.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On Juniper routers (as well as routers from *some* other manufacturers such as Cisco or Brocade) it is possible to authenticate neighbors using an SHA1 digest of elements in PDU combined with a sequence number to protect against Replay attacks.

SHA1 provides a stronger algorithm than the older MD5 standard, but is not so widely supported on none Juniper platforms so should only be deployed once you are certain that all of the devices with which IS-IS Adjacencies will be formed support SHA1-HMAC authentication.

SHA1 authentication is configured differently than either Simple (which sends the password cleartext and should *never* be used) or MD5 authentication methods. Instead of configuring the key directly at the IS-IS protocol, area or interface level, support for SHA1 authentication is added via the *Hitless Key Rollover* extensions. This provides the added benefit of introducing mechanisms to coordinate regular changes to authentication keys and make changes to authentication settings without the need to reset IS-IS adjacencies.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "authentication-key-chain" | exclude "hello-"| count
```

The above command should return a positive integer equal to the number of levels configured for this router.

Then confirm that all keys in the named key-chain are configured to use the SHA1. First getting the name/s of any configured key-chains:

```
[edit protocols isis]
user@host#show | match "authentication-key-chain" | exclude "hello-"
```

And then checking each key-chain does not contain any non-SHA1 algorithms with the following command issued from the `[edit security authentication-key-chains]` hierarchy for each key-chain found:

```
[edit security authentication-key-chains]
user@host#show key-chain <name> | match "algorithm" | exclude "hmac-sha-1" |
count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network you should consider configuring Hitless Key Rollover with SHA1 authentication for all neighbors at each IS-IS Level configured.
First a key-chain must be configured. The same key-chain may be used for multiple levels or separate key-chains used for each level (or even for individual interfaces where required). From the `[edit security authentication-key-chains]` hierarchy issue the following commands:

```
[edit security authentication-key-chains]
user@host#set key-chain <name> key <key number> secret "<secret key>"
user@host#set key-chain <name> key <key number> start-time "<yyyy-mm-
dd.hh:mm:ss>"
user@host#set key-chain <name> key <key number> algorithm hmac-sha-1
user@host#set key-chain <name> key <key number> options isis-enhanced
```

The `start-time` must be provided for all keys and provides the mechanism for controlled key rollover. Keys with a start time in the future can be configured across all of the devices in advance, when the time is reached all of the devices will hitlessly rollover to the new keys without disruption to IS-IS Adjacencies.
Next the key should be set for all Levels at which SHA1 HMAC authentication will be used. From the `[edit protocols isis]` hierarchy, issue the following command:

```
[edit protocols isis]
user@host#set level <level> authentication-key-chain <name>
```

Where a different key is required for a specific area or interface, the key-chain used at the Level can be overridden on a per interface per level basis using the following command from the `[edit protocols isis]' hierarchy:

```
[edit protocols isis]
user@host#set interface <interface name> level <level> hello-authentication-
key-chain <name>
```

Note - Only the setting of the authentication-key-chain on a per level basis is included in the audit procedure for scoring this recommendation, the per interface override is included as additional information only.

Default Value:

No IS-IS routing is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.3 (page 113), National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/concept/authentication-hitless-keychain-isis.html

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on all routers in the IS-IS Area at the given level. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.3 Ensure authentication check is not suppressed (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On JUNOS routers it is possible to suppress some authentication features to aid integration with other vendors IS-IS implementations. One of these interoperability features allows you to configure the router to generate authenticated packets, but not check the authentication of received packets. This leaves the router as vulnerable as it would be with no authentication enabled at all and should not be used in a production environment.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "no-authentication-check" | count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network and have disabled authentication checking, re-enable it by issuing the following command from the `[edit protocols isis]` hierarchy for each level at which it had been set:

```
[edit protocols isis]
user@host#delete level <level> no-authentication-check
```

Default Value:

No IS-IS routing is configured by default.

References:

1. Configuring IS-IS Authentication, JUNOS Software Routing Protocols Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-routing/configuring-is-is-authentication.html#id-11133728)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details and supported on all routers in the IS-IS Area at the given level. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.4 Ensure loose authentication check is not configured (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On JUNOS routers it is possible to suppress some authentication features to aid integration with other vendors IS-IS implementations. One of these interoperability features allows you to configure the router to accept both authenticated and unauthenticated IS-IS packets. This is to allow for transition period, where authentication is not yet configured across all devices in a network, but leaves the protocol open to exploitation and should not be left in place once the migration to an authentication method is complete.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "loose-authentication-check" | count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network and have enabled loose authentication checking, re-enable it by issuing the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#delete loose-authentication-check
```

Default Value:

No IS-IS routing is configured by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/usage-guidelines/routing-enabling-authentication-for-is-is-without-network-wide-deployment.html
2. https://www.juniper.net/documentation/en_US/junos/topics/usage-guidelines/routing-configuring-is-is-authentication.html

Additional Information:

Ensure that Neighbor Authentication is configured with the same details and supported on all routers in the IS-IS Area at the given level. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.5 Ensure IS-IS Hello authentication check is not suppressed (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack. On JUNOS routers it is possible to suppress some authentication features to aid integration with other vendors IS-IS implementations.

One of these interoperability features allows you to configure the router to ignore authentication for *Hello* messages from other routers. This potentially leaves the router open to attack through *Hello* messages to the same extent as it would be were authentication not configured at all.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "no-hello-authentication " | count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network and have disabled hello authentication checking, re-enable it by issuing the following command from the `[edit protocols isis]` hierarchy for each level at which it was configured:

```
[edit protocols isis]
user@host#delete level <level> no-hello-authentication
```

Default Value:

No IS-IS routing is configured by default.

Hello Authentication is not suppressed by default when IS-IS is configured.

References:

1. Configuring IS-IS Authentication, JUNOS Software Routing Protocols Configuration Guide, Juniper Networks

Additional Information:

Ensure that all routers with which the JUNOS router must communicate with through IS-IS support authentication of Hello messages prior to re-enabling it.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.6 Ensure PSNP authentication check is not set to suppressed (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On JUNOS routers it is possible to suppress some authentication features to aid integration with other vendors IS-IS implementations. One of these interoperability features allows you to configure the router to ignore authentication for *Partial Sequence Number PDU (PSNP)* messages from other routers. This potentially leaves the router open to attack through *PSNP* messages to the same extent as it would be were authentication not configured at all.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "no-psnp-authentication " | count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network and have disabled PSNP authentication checking, re-enable it by issuing the following command from the `[edit protocols isis]` hierarchy for each level at which it was set:

```
[edit protocols isis]
user@host#delete level <level> no-psnp-authentication
```

Default Value:

No IS-IS routing is configured by default.

PSNP Authentication is not suppressed by default when IS-IS is configured

References:

1. Configuring IS-IS Authentication, JUNOS Software Routing Protocols Configuration Guide, Juniper Networks

Additional Information:

Ensure that all routers with which the JUNOS router must communicate with through IS-IS support authentication of PSNP messages prior to re-enabling it.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.2.7 Ensure CSNP authentication check is not set to suppressed (Automated)

Profile Applicability:

- Level 1

Description:

IS-IS Neighbors should be authenticated.

Rationale:

Where it is deployed, IS-IS routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers IS-IS neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On JUNOS routers it is possible to suppress some authentication features to aid integration with other vendors IS-IS implementations. One of these interoperability features allows you to configure the router to ignore authentication for *Complete Sequence Number PDU (CSNP)* messages from other routers. This potentially leaves the router open to attack through *CSNP* messages to the same extent as it would be were authentication not configured at all.

Audit:

Enter the following command from the `[edit protocols isis]` hierarchy:

```
[edit protocols isis]
user@host#show | match "no-csnp-authentication " | count
```

The above command should return null or 0.

Remediation:

If you have deployed IS-IS in your network and have disabled CSNP authentication checking, re-enable it by issuing the following command from the `[edit protocols isis]` hierarchy for each level at which it was set:

```
[edit protocols isis]
user@host#delete level <level> no-csnp-authentication
```

Default Value:

No IS-IS routing is configured by default.

CSNP Authentication is not suppressed by default when IS-IS is configured.

References:

1. Configuring IS-IS Authentication, JUNOS Software Routing Protocols Configuration Guide, Juniper Networks

Additional Information:

Ensure that all routers with which the JUNOS router must communicate with through IS-IS support authentication of CSNP messages prior to re-enabling it.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.3 OSPF

Open Shortest Path First (OSPF) is common Interior Gateway Routing Protocol widely deployed in Enterprise and Service Provider networks. OSPF is a complex protocol, with many configuration options which may have effects which are not immediately obvious. Administrators should be familiar with the OSPF protocol and their routing environment before applying recommendations in this section.

OSPF parameters for JUNOS routers are configured under the `[edit protocols ospf]` hierarchy.

Only apply the recommendations in this section where one or more instances of OSPF are configured on the device. You can confirm the number and type of configured OSPF instances by issuing the following command from the `[edit]` hierarchy:

```
[edit]

user@host#show | match "logical-system|routing-instance|ospf {"
```

If the term `ospf {` is returned, all recommendations from this section should be considered at each routing-instance (including the default) or logical-system for which OSPF is configured.

4.3.1 Ensure OSPF authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

OSPF Neighbors should be authenticated.

Rationale:

Where it is deployed, OSPF routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers OSPF neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On Juniper routers (as well as routers from other manufacturers such as Cisco or Brocade) it is possible to authenticate neighbors using an MD5 digest of elements in the update combined with a sequence number to protect against Replay attacks.

Authentication is configured on a per Interface basis when an interfaces is assigned to an OSPF area.

Audit:

Enter the following command from operational mode:

```
user@host>show ospf interface detail | match "Auth type MD5" | count
```

The above command should return a positive integer equal to the number of interfaces on which OSPF is configured.

Remediation:

To configure MD5 based authentication, first configure the authentication type at the `[edit protocols ospf area <area number>]` hierarchy (this step is not required on all versions of JUNOS):

```
[edit protocols ospf area <area number>]
user@host#set authentication-type md5
```

The key must then be configured for any interfaces in the area

```
[edit protocols ospf area <area number>]
user@host#set interface <interface number> authentication md5 <key number>
<key>
```

The parameter needs to be the same across all routers in the area and is there to provide a method for transitioning from old to new keys.

Default Value:

No OSPF routing is configured by default.

References:

1. Cisco IOS Benchmark Version 2.2, Requirement 2.3.2.3, Center for Internet Security
2. Router Security Configuration Guide, Version 1.1b, Section 4.4.3 (page 106), National Security Agency (NSA)

Additional Information:

Ensure that Neighbor Authentication is configured with the same method and details on all routers in the network segment or OSPF area. Failure to do so will prevent route updates from being accepted. Changing authentication methods will result in existing adjacencies being reset.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.3.2 Ensure OSPF authentication is set to IPSEC SA with SHA (Automated)

Profile Applicability:

- Level 2

Description:

OSPF Neighbors should be strongly authenticated.

Rationale:

Where it is deployed, OSPF routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network.

An attacker posing as one of the target routers OSPF neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

In addition to MD5 hash based authentication, JUNOS routers can also authenticate OSPF neighbors using IPSEC Security Associations. This allows more robust authentication mechanisms to be used and is recommended as an alternative to MD5 HMAC in high security environments. Support for IPSEC based authentication with other vendors is not universal, so ensure all of your devices are able to support this method before proceeding.

A Manual IPSEC Security Association is formed between neighbors, using Authenticated Header (IP Protocol 51) with the stronger HMAC-SHA1 or HMAC-SHA2 (SHA2 is not available on all platforms) methods to ensure that the updates were sent by trusted neighbors and were not changed in transit. Only AH is used to avoid the added overhead required to encrypt and decrypt the packets contents which ESP would entail. It is possible to use ESP in place of AH if encryption of routing information across an untrusted segment is required, but this can have a significant performance cost.

In "dual stack" IPv4/IPv6 environments running both OSPFv2 for IPv4 routing and OSPFv3 for IPv6, it is common to use a single SA on a segment to provide authentication both protocols.

NOTE - Although M, T and MX series devices normally require a Services PIC or DPC installed to provide IPSEC VPNs, no additional hardware is required for IPSEC SA based authentication of OSPF neighbors.

Audit:

Enter the following command from the `[edit protocols ospf]` hierarchy;

```
[edit protocols ospf]
user@host#show | match "ipsec-sa" | count
```

The above command should return a positive integer equal to the number of interfaces configured for OSPF which can be checked with the following command:

```
[edit protocols ospf]
user@host#show | match "interface" | count
```

As the use of IPSEC SA based authentication is to avoid weak each Security Association configured should be checked to confirm MD5 is not used. First find each `<sa name>` used for OSPF:

```
[edit protocols ospf]
user@host#show | match "ipsec-sa"
```

Then check each SA does not include MD5:

```
[edit protocols ospf]
user@host#top show security ipsec security-association <sa name> | match
"md5" | count
```

This command should return null or 0 if no insecure hashing methods are used.

Remediation:

To setup IPSEC SA based authentication, first configure a Security Association at the `[edit security ipsec]` hierarchy;

```
[edit security ipsec]
edit security-association <SA name>
set description <description>
set mode transport
set manual direction bidirectional protocol ah
set manual direction bidirectional algorithm hmac-sha1-96
set manual direction bidirectional authentication key <key>
```

The SA must be bi-directional and must be configured with the same parameters on all neighbors reachable on the intended interface.
Note that only Authenticated Header is configured in this example which provides mutual authentication but **does not encrypt OSPF protocol messages in transit.**
Next configure IPSEC SA based authentication for one or more interfaces which OSPF will be run over from the `[edit protocols ospf]` hierarchy;

```
[edit protocols ospf]
user@host#set area <area number> interface <interface number> ipsec-sa <SA
name>
```

Default Value:

No OSPF routing is configured by default.

References:

1. Configuring Authentication for OSPFv2, JUNOS Software Routing Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos95/swconfig-routing/frameset.html)

Additional Information:

NOTE: Security Associations must be configured correctly on all neighbors reached through interfaces where IPSEC based authentication is configured for OSPF to continue to function. Changing authentication methods will result in existing adjacencies being reset.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.4 OSPF3

Open Shortest Path First (OSPF) Version 3 is an Interior Gateway Routing Protocol widely deployed in Enterprise and Service Provider networks which expands OSPF to support IPv6.

OSPF is a complex protocol, with many configuration options which may have effects which are not immediately obvious. Administrators should be familiar with the OSPFv3 protocol and their routing environment before applying recommendations in this section.

OSPFv3 parameters for JUNOS routers are configured under the `[edit protocols ospf3]` hierarchy.

Only apply the recommendations in this section where one or more instances of OSPFv3 are configured on the device. You can confirm the number and type of configured OSPFv3 instances by issuing the following command from the `[edit]` hierarchy:

```
[edit]

user@host#show | match "logical-system|routing-instance|ospf3 {"
```

If the term `ospf3 {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.4.1 Ensure OSPFv3 authentication is set to IPSEC SA (Automated)

Profile Applicability:

- Level 1

Description:

OSPFv3 Neighbors should be strongly authenticated.

Rationale:

Where it is deployed, OSPFv3 routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network.

An attacker posing as one of the target routers OSPFv3 neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

OSPFv3 does not support MD5 HMAC based authentication, instead relying on IPSEC Security Associations to authenticate neighbors. This provides more robust authentication mechanisms and for, optional, encryption of routing data in transit.

A Manual IPSEC Security Association is formed between neighbors, using Authenticated Header (IP Protocol 51) with the strong SHA1-HMAC method to ensure that the updates were sent by trusted neighbors and were not changed in transit. Only AH is used to avoid the added overhead required to encrypt and decrypt the packets contents which ESP would entail. It is possible to use ESP in place of AH if encryption of routing information across an untrusted segment is required, but this can have a significant performance cost.

In "dual stack" IPv4/IPv6 environments running both OSPFv2 for IPv4 routing and OSPFv3 for IPv6, it is common to use a single SA on a segment to provide authentication both protocols.

NOTE - Although M, T and MX series devices normally require a Services PIC or DPC installed to provide IPSEC VPNs, no additional hardware is required for IPSEC SA based authentication of OSPF neighbors.

Audit:

Enter the following command from the `[edit protocols ospf3]` hierarchy;

```
[edit protocols ospf3]
user@host#show | match "ipsec-sa" | count
```

The above command should return a positive integer equal to the number of interfaces on which IPSEC SA based authentication is required.

```
[edit protocols ospf3]
user@host#show | match "interface" | count
```

As the use of IPSEC SA based authentication is to avoid weak each Security Association configured should be checked to confirm MD5 is not used. First find each `<sa name>` used for OSPFv3:

```
[edit protocols ospf3]
user@host#show | match "ipsec-sa"
```

Then check each SA does not include MD5:

```
[edit protocols ospf]
user@host#top show security ipsec security-association <sa name> | match
"md5" | count
```

This command should return null or 0 if no insecure hashing methods are used.

Remediation:

To setup IPSEC SA based authentication, first configure a Security Association at the `[edit security ipsec]` hierarchy;

```
[edit security ipsec]
edit security-association <SA name>
set description <description>
set mode transport
set manual direction bidirectional protocol ah
set manual direction bidirectional algorithm hmac-sha1-96
set manual direction bidirectional authentication key <key>
```

The SA must be bi-directional and must be configured with the same parameters on all neighbors reachable on the intended interface.
Note that only Authenticated Header is configured in this example which provides mutual authentication but **does not encrypt OSPFv3 protocol messages in transit**.
Next configure IPSEC SA based authentication for one or more interfaces which OSPF will be run over from the `[edit protocols ospfv3]` hierarchy;

```
[edit protocols ospfv3]
user@host#set area <area number> interface <interface number> ipsec-sa <SA
name>
```

Default Value:

No OSPFv3 routing is configured by default

References:

1. Configuring Authentication for OSPFv3, JUNOS Software Routing Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos95/swconfig-routing/frameset.html)

Additional Information:

Security Associations must be configured correctly on all neighbors reached through interfaces where IPSEC based authentication is configured for OSPFv3 to continue to function. Changing authentication methods will result in existing adjacencies being reset.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.5 RIP

Routing Information Protocol is a distance vector protocol used for interior gateway routing on some networks. RIP is a complex protocol, with many configuration options which may have effects which are not immediately obvious. Administrators should be familiar with the RIP protocol and their routing environment before applying recommendations in this section.

RIP parameters for JUNOS routers are configured under the `[edit protocols rip]` hierarchy and in JUNOS RIPv2 is used by default (though communication with legacy v1 neighbors can be configured).

Only apply the recommendations in this section where one or more instances of RIP are configured on the device. You can confirm the number and type of configured RIP instances by issuing the following command from the `[edit]` hierarchy:

```
[edit]

user@host#show | match "logical-system|routing-instance|protocols|rip {"
```

If the term `rip {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.5.1 Ensure RIP authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

RIP Neighbors should be authenticated.

Rationale:

Where it is deployed, RIP routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network. An attacker posing as one of the target routers RIP neighbors may inject incorrect information into the route table resulting in DoS attack or loss of confidential data through a Man in the Middle attack.

On Juniper routers (as well as routers from other manufacturers such as Cisco or Brocade) it is possible to authenticate neighbors using an MD5 digest of elements in the update. RIP Authentication is defined in RFC2082.

Audit:

Enter the following command from the `[edit protocols rip]` hierarchy:

```
[edit protocols rip]
user@host#show | match "authentication-" | count
```

The above command should return '2' when both required statements are configured.

Remediation:

If you have deployed RIP in your network you should use MD5 authentication for all neighbors. To configure authentication enter the following command from the `[edit protocols rip]` hierarchy:

```
[edit protocols rip]
user@host#set authentication-type md5
user@host#set authentication-key <key>
```

Default Value:

No RIP routing is configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.4.3 (page 109), National Security Agency (NSA)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on all routers in the AS. Failure to do so will prevent route updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.5.2 Ensure RIP is set to check for zero values in reserved fields (Automated)

Profile Applicability:

- Level 1

Description:

The router should check that fields that the RFC requires must be 0 are, in fact, 0.

Rationale:

Where it is deployed, RIP routing is vital for normal operation of an organization's network infrastructure. Correct route information is required for routers to correctly direct traffic through the network.

The RFCs relating to RIP define a number of reserved fields in the packet format for future use. Those fields not used in the protocol version used should be set to 0.

If a packet is received with reserved fields set to a value other than 0 then it is breaking the RFC standards and may be an attempt to attack the router. In almost all network environments there is no reason for such a packet to exist, so JUNOS's default behavior of ignoring them should be used.

Audit:

Enter the following command from the `[edit protocols rip]` hierarchy:

```
[edit protocols rip]
user@host#show | match "check-zero" | count
```

The above command should return '1' when checking is enabled.

Remediation:

If you have deployed RIP in your network and disabled zero value checking of reserved fields, you should re-enable it by issuing the following command from the `[edit protocols rip]` hierarchy:

```
[edit protocols rip]
user@host#set check-zero
```

Default Value:

When RIP is used, check-zero is the default setting.

References:

1. Accepting Packets Whose Reserved Fields Are Nonzero, JUNOS Software Protocols Configuration Guide, Juniper Networks

Additional Information:

If the check-zero option has been disabled in your environment, confirm that there are no misconfigured or noncompliant routers which rely on sending malformed RIP updated prior to re-enabling the option otherwise routing information from some neighbours may be ignored.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

4.6 bfd

Some security settings are configured in exactly the same way across all routing protocols on a JUNOS device.

One of these is Bidirectional Forwarding Detection (BFD), which may configured under the `[edit protocols <protocol> bfd-liveness-detection]` hierarchy where `<protocol>` is one of `isis`, `bgp`, `ospf`, `static`, `rip`, `pim` or another protocol with BFD support.

To confirm whether BFG Liveness Detection is configured on the device, enter the following command from the root `[edit]` configuration hierarchy:

```
[edit]

user@host# show | display set | match "bfd-live"
```

If any lines are returned, all Recommendations in this Section should be applied to all instances of BFD.

If BFD is not used but is configured, it should be removed from each interface or neighbor for which it is currently configured.

4.6.1 Ensure BFD Authentication is Set (Automated)

Profile Applicability:

- Level 2

Description:

BFD Peers should be authenticated.

Rationale:

Bidirectional Forwarding Detection (BFD) is a Forwarding Plane feature which allows more rapid detection of a failed neighbor then can be achieved through a routing protocols' normal detection mechanisms, providing faster reconvergence.

If no authentication was used an attacker may replay or spoof BFD messages to destabilize a network and/or prevent proper reconvergence resulting in a Denial of Service. Several authentication mechanisms are supported for BFD ranging from plain text password, which should not be used, to meticulously keyed SHA1.

The latter provides the strongest hashing algorithm and best replay protection, with the sequence number being updated on each packet, and it is this mechanism that should be used in most cases.

However, if None Stop Routing (NSR) features are required; meticulously keyed SHA1 or MD5 should not be used as the BFD Sessions using these algorithms may fail when switching to the Backup Routing Engine.

Both BFD peers must be configured with the same keys and method, otherwise the BFD link may be declared down resulting in a reconvergence. Because it is not possible to configure both ends of an existing BFD link simultaneously you may need to use Loose Authentication Checking as a transitional step by configuring the `loose-check` option.

Impact:

BFD Authentication must be configured to use the same Key and Algorithm on all neighbors/peers with which the session will be used. A mismatch will result in the BFD session failing and related routes being declared unreachable.

BFD Authentication with meticulous-keyed-sha-1 and meticulous-keyed-md5 algorithms should not be used in conjunction with NSR and GRES. Fail over between Routing Engines will cause Authentication to fail.

Audit:

To confirm whether BFD Authentication is configured, issued the following command from the root `[edit]` hierarchy:

```
[edit]
user@host#show | display set | match "bfd-live.*authentication" | except
loose | count
```

Now issue the following command to count the total number of BFD sessions configured:

```
[edit]
user@host#show | match "bfd-live.{" | count
```

The line count returned by the first command should be double that returned by the second, indicating that every BFD session has been configured with an Authentication Algorithm and Key Chain (requiring two commands).
If the Audit Procedure shows that Authentication is missing, enter the following command and apply the Remediation Procedure at each hierarchy where BFD is configured, but Authentication is not.

```
[edit]
user@host#show | display set | match "bfd-live"
```

Remediation:

If you have deployed BFD, authentication can be configured by issuing the following commands.
First set the authentication algorithm and keychain from the appropriate `[.* bfd-liveness-detection]` hierarchy, in this example we are configuring BFD Authentication for OSPF Neighbors on Interface Ge-0/0/0.0:

```
[edit protocols ospf interface ge-0/0/0.0 bfd-liveness-detection]
user@host#set authentication algorithm <algorithm>
user@host#set authentication key-chain <key-chain>
```

Where:

- <algorithm> is either `keyed-md5`, `keyed-sha-1`, `meticulous-keyed-md5` or `meticulous-keyed-sha-1`, which is preferred but is not compatible with NSR and other failover options.
- <key-chain> is the name of a configured key-chain (see below).

If a Key Chain is not already defined, you should create one by issuing the following command at the `[edit security authentication-key-chains]` hierarchy:

```
[edit security authentication-key-chains]
user@host#set key-chain <key-chain> key <key number> secret <key>
```

Where:

- <key-chain> is the name of the key-chain already configured for the BFD session
- <key number> is the number to identify this key, used for key rollover
- <key> is the Shared Secret Key

The <algorithm> and <key> **must** be the same on all devices which will use the BFD session being configured.
If the BFD Session is already in use, setting Authentication on one side before the other will cause the BFD Session (and the associated routes or adjacencies) to be declared down resulting in loss of traffic. To aide in rollout of BFD Authentication, JUNOS Devices can operate in a "Loos Authentication Check" mode, whereby they will send Authentication information, but will not reject unauthenticated messages.
This should be used in transition *only* and can be configured with the following command from the same `[.* bfd-liveness-detection]` hierarchy:

```
[edit protocols ospf interface ge-0/0/0.0 bfd-liveness-detection]
user@host#set authentication loose-check
```

BFD may be configured at a wide variety of configuration hierarchies, for different Protocols, Routing Instances or even for Static Routes. The `bfd-liveness-detection` hierarchy is the same at each level it is used, so the Remediation Process is the same and should be applied at each hierarchy indicated in the Audit Procedure.

Default Value:

No BFD is configured by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-bfd-static-routes-understanding.html
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/bfd-liveness-detection-edit-routing-options.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

4.6.2 Ensure BFD Authentication is Not Set to Loose-Check (Automated)

Profile Applicability:

- Level 2

Description:

BFD Peers should be authenticated.

Rationale:

Bidirectional Forwarding Detection (BFD) is a Forwarding Plane feature which allows more rapid detection of a failed neighbor then can be achieved through a routing protocols' normal detection mechanisms, providing faster reconvergence.

If no authentication was used an attacker may replay or spoof BFD messages to destabilize a network and/or prevent proper reconvergence resulting in a Denial of Service.

JUNOS supports a Loose Authentication Check mechanism, which is intended for use when transitioning from unauthenticated BFD to authenticated BFD implementations or when changing Shared Secret Keys.

When Loose Authentication Checking is enabled, the JUNOS Device will produce authenticated BFD packets, but will not check the authentication of packets it receives from its peer. When enabled the JUNOS Device is effectively as unprotected as when authentication is not configured at all.

BFD Sessions should never be configured with the `authentication loose-check` option in a production network, with the exception of short transition periods while updating/replacing keys.

Impact:

BFD Authentication must be configured to use the same Key and Algorithm on all neighbors/peers with which the session will be used. A mismatch will result in the BFD session failing and related routes being declared unreachable.

BFD Authentication with meticulous-keyed-sha-1 and meticulous-keyed-md5 algorithms should not be used in conjunction with NSR and GRES. Fail over between Routing Engines will cause Authentication to fail.

Audit:

To confirm whether BFD Authentication Loose Check is configured, issued the following command from the root `[edit]` hierarchy:

```
[edit]
user@host#show | display set | match "bfd-live.*authentication loose" | count
```

A line count of 0 should be returned. If a line count of 1 or greater is returned, re-issue the command without the `count` option and apply the Remediation Procedure at each hierarchy indicated.

Remediation:

If you have deployed BFD with Loose Authentication Checking, it can be disabled by issuing the appropriate `[.* bfd-liveness-detection]` hierarchy, in this example we are configuring BFD Authentication for BGP:

```
[edit protocols bgp bfd-liveness-detection]
user@host# delete authentication loose-check
```

BFD may be configured at a wide variety of configuration hierarchies, for different Protocols, Routing Instances or even for Static Routes. The `bfd-liveness-detection` hierarchy is the same at each level it is used, so the Remediation Process is the same and should be applied at each hierarchy indicated in the Audit Procedure.

Default Value:

No BFD is configured by default

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-bfd-static-routes-understanding.html
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/bfd-liveness-detection-edit-routing-options.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

4.7 LDP

Label Distribution Protocol (LDP) is used in many Multi Protocol Label Switched (MPLS) networks to exchange Label information between Label Switch Router (LSR) peers and is defined in RFC5036.

MPLS networks are complex, with many configuration options which may have effects which are not immediately obvious; it is beyond the scope of this benchmark to give even an overview of how LDP and MPLS operate on Juniper routers. It is strongly recommended that administrators be familiar both with MPLS protocols and their network prior to implementing these recommendations.

LDP parameters for JUNOS routers are configured under the `[edit protocols ldp]` hierarchy.

Only apply the recommendations in this section where one or more instances of LDP are configured on the device. You can confirm the number of configured LDP instances by issuing the following command from the `[edit]` *hierarchy:*

```
[edit]

user@host#show | match "logical-system|routing-instance|protocols|ldp {"
```

If the term `ldp {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.7.1 Ensure authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

LDP peers should be authenticated.

Rationale:

Where it is deployed, LDP is vital for normal operation of an MPLS network. LDP is used to determine Label mapping and populate the routers Forwarding Information Base (FIB). An attacker posing as one of the target routers LDP peers may attempt to inject incorrect label information or exploit a vulnerability in the routers LDP implementation to cause an information disclosure or denial of service.

On Juniper routers (as well as routers from other manufacturers such as Cisco or Brocade) it is possible to authenticate LDP sessions using an MD5 digest of elements in LDP messages.

LDP Session Authentication may be configured on a per session or per session-group basis. The Audit Procedure checks for both, however, the remediation procedure is only given for a session-group; as configuration at the session level is deprecated in current versions of JUNOS.

Audit:

Enter the following command from the `[edit protocols ldp]` hierarchy:

```
[edit protocols ldp]
user@host#show | match "authentication-key" | count
```

The above command should return an integer value equal to the number of LDP Sessions found with the following command:

```
[edit protocols ldp]
user@host#show | match "session |session-group" | count
```

Remediation:

If you have deployed LDP in your network you should use MD5 authentication for all neighbors.

To configure authentication for a session-group enter the following command from the `[edit protocols ldp]` hierarchy:

```
[edit protocols ldp]
user@host#set session-group <Destination IP Address or IP/Mask>
authentication-key <key>
```

Default Value:

LDP is not configured by default.

When LDP sessions are configured, MD5 is the default authentication method when an `authentication-key` is specified.

References:

1. Configuring Miscellaneous LDP Properties, Juniper Software MPLS Applications Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/config-guide-mpls-applications/mpls-configuring-miscellaneous-ldp-properties.html)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on all neighbours in a session-group. Failure to do so will prevent label updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.7.2 Ensure authentication is set to AES-CMAC (Automated)

Profile Applicability:

- Level 2

Description:

LDP peers should be strongly authenticated.

Rationale:

Where it is deployed, LDP is vital for normal operation of an MPLS network. LDP is used to determine Label mapping and populate the routers Forwarding Information Base (FIB). An attacker posing as one of the target routers LDP peers may attempt to inject incorrect label information or exploit a vulnerability in the routers LDP implementation to cause an information disclosure or denial of service.

On Juniper routers (as well as routers from some other vendors) it is possible to authenticate LDP sessions using a Cipher-based Message Authentication Code method with the AES encryption algorithm.

AES-128-CMAC-96 is significantly more robust than the MD5-HMAC method, which has traditionally been used for LDP session authentication, and should be used wherever both LSRs support it (such as in an all Juniper deployment).

Where support for AES-128-CMAC-96 is not available; SHA1-HMAC, while not as strong as the AES method, should be strongly preferred over MD5-HMAC which is considerably weaker.

Strong LDP Session Authentication is configured on a per session-group basis, allowing you to easily support different algorithms with different groups if necessary.

Audit:

Enter the following command from the `[edit protocols ldp]` hierarchy:

```
[edit protocols ldp]
user@host#show | match "aes-128-cmac-96" | count
```

The above command should return an integer value equal to the number of LDP Sessions found with the following command:

```
[edit protocols ldp]
user@host#show | match "session |session-group" | count
```

Remediation:

If you have deployed LDP in your network you should use strong authentication for all neighbors.
Both AES-CMAC and SHA1-HMAC authentication require a keychain to be configured on the device under the `[edit security authentication-key-chains]` hierarchy with at least one key which has a start time in the past.

```
[edit security authentication-key-chains]
user@host#set key-chain <name> key <key number> start-time <YYYY-MM-DD.HH:MM>
user@host#set key-chain <name> key <key number> secret <secret key>
```

The chosen algorithm and keychain should then be configured for all session groups from the `[edit protocols ldp]` hierarchy:

```
[edit protocols ldp]
user@host#set session-group <Destination IP Address or IP/Mask>
authentication-algorithm aes-128-cmac-96
user@host#set session-group <Destination IP Address or IP/Mask>
authentication-key-chain <name>
```

or for SHA1 :

```
[edit protocols ldp]
user@host#set session-group <Destination IP Address or IP/Mask>
authentication-algorithm hmac-sha-1-96
user@host#set session-group <Destination IP Address or IP/Mask>
authentication-key-chain <name>
```

Default Value:

LDP is not configured by default.

When LDP is configured with an `authentication-key`, MD5 is the default `authentication-algorithm`.

References:

1. Configuring Miscellaneous LDP Properties, Juniper Software MPLS Applications Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/config-guide-mpls-applications/mpls-configuring-miscellaneous-ldp-properties.html)

Additional Information:

Ensure that Neighbor Authentication is configured with the same details on all neighbours in a session-group. Failure to do so will prevent label updates from being accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.8 MSDP

Multicast Source Discovery Protocol (MSDP) provides a method for linking multiple PIM-SM domains (Protocol Independent Multicast - Sparse Mode) and is defined in RFC3681.

PIM-SM and MSDP are complex protocols, with many configuration options which may have effects which are not immediately obvious; it is beyond the scope of this benchmark to give even an overview of how MSDP, PIM and Multicast operate on Juniper routers. It is strongly recommended that administrators be familiar both Multicast protocols and their network prior to implementing these recommendations.

MSDP parameters for JUNOS routers are configured under the `[edit protocols msdp]` hierarchy.

Only apply the recommendations in this section where one or more instances of MSDP are configured on the device. You can confirm the number of configured MSDP instances by issuing the following command from the `[edit]` *hierarchy:*

```
[edit]

user@host#show | match "logical-system|routing-instance|protocols|msdp {"
```

If the term `msdp {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.8.1 Ensure authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

MSDP Peers should be authenticated.

Rationale:

When deployed MSDP it provides PIM-SM with information for routing Multicast traffic and is critical to operation of Multicast services on the network. If no authentication is used, an attacker may inject false information into the PIM-SM distribution tree, resulting in potential Denial of Service or Integrity compromise.

MSDP packets can be authenticated using a Keyed Hash-based Message Authentication Code (HMAC) generated by hashing elements of the of the update packet combined with a shared secret using MD5.

Audit:

Enter the following command from the `[edit protocols msdp]` hierarchy:

```
[edit protocols msdp]
user@host#show | match "authentication-key" | count
```

This should return an integer value equal to the number of configured MSDP Peers obtained with the following command:

```
[edit protocols msdp]
user@host#show | match "peer .* {" | count
```

Remediation:

If you have deployed MSDP, authentication can be configured on a peer by peer basis, by issuing the following command from the `[edit protocols msdp]` hierarchy:

```
[edit protocols msdp]
user@host#set peer <peer address> authentication-key <key>
```

Default Value:

No MSDP is configured by default.

References:

1. Configuring the MSDP Authentication Key, JUNOS Software Multicast Protocols Configuration Guide, Juniper Networks

Additional Information:

MSDP Peers must both be configured to use the same key and algorithm otherwise MSDP updates will not be accepted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.9 Neighbor-discovery

Neighbor Discovery Protocol (NDP), defined in RFC2461, is an important component of IPv6, effectively replacing the combined functions provided by ICMP Router Discovery (RDISC), Address Resolution Protocol (ARP) and ICMP Redirect in IPv4.

Neighbor Discovery Protocol parameters for JUNOS routers are configured under the `[edit protocols neighbor-discovery]` hierarchy.

Only apply the recommendations in this section where IPv6 is configured on the device. You can confirm the number of configured whether any IPv6 is configured by issuing the following command from the `[edit]` hierarchy:

```
[edit]

user@host#show | match "family inet6" | count
```

If a positive integer is returned, you should consider applying the recommendations in this section. If IPv6 configuration is found and you do not intend to support IPv6, all IPv6 related configuration should be deactivated or removed.

4.9.1 Ensure Secure Neighbor Discovery is configured (Automated)

Profile Applicability:

- Level 2

Description:

NDP should be protected.

Rationale:

One of the primary functions of NDP is to resolve Network Layer (IP) addresses to Link Layer (eg Ethernet) addresses, a function performed in IPv4 by ARP. An attacker who has access to the broadcast segment may abuse NDP or ARP to trick hosts into sending the attacker traffic destined for someone else, a technique known as ARP Poisoning.

To protect IPv6 networks against this, and other attacks against NDP functions, Secure Neighbor Discovery (SEND) should be deployed where preventing access to the broadcast segment may not be possible or in sensitive environments with a requirement for increased protection.

Support for SEND was added to JUNOS in version 9.3. SEND utilizes public/private RSA key pairs to produce Cryptographically Generated Addresses (as defined in RFC3972), which ensures that the claimed source of an NDP message is the owner of the claimed address.

Audit:

Enter the following command from the `[edit protocols]` hierarchy:

```
[edit]
user@host#show neighbor-discovery secure | match cryptographic-address |
count
```

The above command should return a value of 2.

Remediation:

If you have deployed IPv6 you can configure SEND by issuing the following commands from the `[edit protocols neighbor-discovery]` hierarchy: If you have not already done so, you will need to generate or install an RSA key pair, to generate a new pair enter the following command:

```
user@host>request pki generate-key-pair <name> <ca-profile>
```

Next, set the security level to define how unsecure NDP messages should be handled. If only a subset of devices will be configured to use SEND, then use the default option. If all nodes on the segment require protection, which is recommended, use the secure-messages-only option:

```
[edit protocols neighbor-discovery]
user@host#set secure security-level secure-messages-only
```

Finally, specify the key pair and details you generated/installed earlier:

```
[edit protocols neighbor-discovery]
user@host#set secure cryptographic-address key-pair <name>
user@host#set secure cryptographic-address key-length <length>
```

For more details on configuring Public/Private Key Pairs in JUNOS please refer to: Generating a Public-Private Key Pair, JUNOS Software Security Configuration Guide, Juniper Networks

Default Value:

SEND is not configured by default.

References:

1. Secure Neighbor Discovery Configuration Guidelines, JUNOS Software Routing Protocol Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos95/swconfig-routing/jd0e84357.html)

Additional Information:

All nodes on the segment will need to be configured with SEND if the `secure-messages-only` option is selected, which is recommended unless only a small subset of devices require increased protection. Failure to configure SEND for all nodes may result in loss of connectivity.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.10 Router-discovery

ICMP Router Discovery, defined in RFC1256, provides a method for hosts on a multicast or broadcast segment to discover routers attached to the network segment.

ICMP Router Discovery parameters for JUNOS routers are configured under the `[edit protocols router-discovery]` hierarchy.

4.10.1 Ensure ICMP Router Discovery is disabled (Automated)

Profile Applicability:

- Level 1

Description:

ICMP Router Discovery should not be used.

Rationale:

ICMP Router Discovery provides details of routers attached to a broadcast or multicast segment in response to Router Solicitation messages from hosts or in the form of a period Router Advertisement.

These messages may provide an attacker attached to the segment with a clearer picture of network environment and also increases the attack surface of the JUNOS device. As the feature is rarely used, ICMP Router Discovery should only be configured on networks where a specific requirement exists for its use.

Audit:

Enter the following command from the `[edit]` hierarchy:

```
[edit]
user@host#show protocols router-discovery
```

The above command should return the following output:

```
disable;
```

Additional configuration items may be present between the inner curly braces, but will have no effect because the protocol is disabled.

Remediation:

If you have configured ICMP Router Discovery and do not require it, you can disable it by issuing the following command from the `[edit protocols router-discovery]` hierarchy:

```
[edit protocols router-discovery]
user@host#set disable
```

Default Value:

ICMP Router Discovery is disabled by default.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.11 RSVP

Resource Reservation Protocol (RSVP) is commonly used in Quality of Service (QoS) and MLPS Traffic Engineering (through the RSVP-TE variation) solutions, in simple terms it allows node to 'reserve' bandwidth throughout the path that a session will take.

RSVP parameters for JUNOS routers are configured under the `[edit protocols rsvp]` hierarchy.

Only apply the recommendations in this section where one or more instances of RSVP are configured on the device. You can confirm the number of configured RSVP instances by issuing the following command from the `[edit]` *hierarchy:*

```
[edit]

user@host#show | match "logical-system|routing-instance|protocols|rsvp {"
```

If the term `rsvp {` is returned, all recommendations from this section should be considered at each hierarchy indicated.

4.11.1 Ensure authentication is set to MD5 (Automated)

Profile Applicability:

- Level 1

Description:

RSVP Peers should be authenticated.

Rationale:

RSVP messages may be abused by an attacker to interfere with QoS and Traffic Engineering services, resulting in poor performance or Denial of Service, or seek to attack the target router directly using weaknesses in the RSVP implementation.

To protect against these types of attacks RSVP messages may be Authenticated using an MD5 hash of certain packet elements combined with a secret key (MD5 HMAC). RSVP authentication is supported in the two major variants described in the IETF Draft "RSVP Cryptographic Authentication draft-ietf-rsvp-md5-03" and in RFC 2747. JUNOS automatically detects which variant to use on a neighbor by neighbor basis and not interaction is required from the administrator for multi-vendor support.

RSVP Authentication is set on an interface by interface basis and should be configured for all interfaces where RSVP is used.

Audit:

Enter the following command from the `[edit]` hierarchy:

```
[edit]
user@host#show protocols rsvp | match authentication-key | count
```

The above command should return an integer value equal to the number of interfaces for which RSVP is configured.

Remediation:

If you have configured RSVP you can add authentication by issuing the following command from the `[edit protocols rsvp]` hierarchy:

```
[edit protocols rsvp]
user@host#set interface <interface name> authentication-key <key>
```

Default Value:

RSVP is not configured by default

References:

1. Configuring RSVP Interfaces, JUNOS Software MPLS Applications Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/config-guide-mpls-applications/mpls-configuring-rsvp-interfaces.html#id-39542)

Additional Information:

All RSVP neighbors reachable through each interface will need to be configured with the same key and authentication method for continued operation.

In addition, all interfaces participating in a single LSP should be configured to use the same authentication details, otherwise the LSP will be marked Down.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.12 LLDP and LLDP-MED

The *Link Layer Discovery Protocol (LLDP)* is a vendor-neutral and widely supported standard used for network devices to advertise information about their capabilities, identity, software and management details to other network devices on the LAN. LLDP is specified in the IEEE 802.1AB-2005 standard.

LLDP is configured under the `[edit protocols lldp]` configuration hierarchy and supported on all Junos devices with Ethernet interfaces.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP published by the *Telecommunications Industry Association (TIA)* in the ANSI/TIA-1057 standard. LLDP-MED is primarily used to enable *Voice over IP (VoIP)* services by allowing connected devices to acquire information such as VLAN & DiffServ markings for Voice traffic, device location for emergency call requirements and extended *Power over Ethernet (PoE)* management.

LLDP-MED is configured under the `[edit protocols lldp-med]` configuration hierarchy on a wide range of Juniper devices including SRX Firewalls and EX series Switches.

Because the two protocols are closely related, recommendations relating to both are grouped together in the same section of this Benchmark.

As with many other protocols on Junos devices, LLDP and LLDP-MED may be configured separately under different *Logical Systems* or *Routing Instances*, these recommendations apply to all instances where LLDP and LLDP-MED are used.

4.12.1 Ensure LLDP is Disabled if not Required (Manual)

Profile Applicability:

- Level 2

Description:

LLDP should be disabled when not required

Rationale:

The *Link Layer Discovery Protocol (LLDP)* is a vendor-neutral and widely supported standard used for network devices to advertise information about their capabilities, identity, software and management details to other network devices on the LAN. LLDP is specified in the IEEE 802.1AB-2005 standard.

It is broadly similar in purpose and application to the older, proprietary *Cisco Discovery Protocol (CDP)* which is still widely used in Cisco networks, but less widely in multivendor environments (and is not supported on Junos).

Devices configured for LLDP advertise information on all chosen Ethernet interfaces by sending an Ethernet Frame containing an *LLDPDU* to a Multicast Address (several address options existing, including Unicast) which 802.1D compliant switches should not forward further. This information is specified in a sequence of *Type-Length-Value (TLV)* data structures, which may include:

- System hostname and description (`system-name` and `system-description` TLVs)
- Port details and description for the sending interface (`mac-phy-config-status`, `port-description`)
- VLAN name and description for the sending interface (`vlan-name`, `port-vid`)
- Management IP address for the Junos device (`management-address`)
- Device capabilities (such as Switch or Router) (`system-capabilities`, preformatted based on model)
- LAGP Link Aggregation information (`link-aggregation`)
- Device Serial Number (`jnpr-chassis-serial`)
- Further information and additional TLVs

This information can be extremely useful when documenting or troubleshooting a network, but is also extremely useful to a potential attacker, either directly connected to the device or having compromised a neighbouring device.

To reduce the information given to a potential attacker, in high security environments LLDP should be disabled where it is not absolutely required for normal operation. LLDP can either be disabled globally, or on a per interface basis (for example, leaving LLDP enabled on access ports where it may be used for PoE or VoIP applications, but disabling it on infrastructure links or connections to untrusted networks).

Impact:

LLDP is commonly used to support VoIP and devices such as Wireless APs or Access Control systems which make use of PoE for power - disabling LLDP or LLDP-MED for these interfaces may result in service disruption.

Audit:

Due to the range of options as to the type of device, deployment scenario and where LLDP will be used in the network, it is not possible to provide Automated Scoring of this recommendation.
To check whether LLDP is enabled, use the following command from the `[edit protocols]` configuration hierarchy:

```
[edit protocols]
user@host#show lldp | display set | match "interface|disable"
```

The command should return all Routing Instances or Logical Systems where LLDP has been enabled globally for all interfaces by returning one or more lines ending `interface all`.
If LLDP is configured for only selected interfaces, one or more lines should be returned ending with the interface name/s, for example `set protocols lldp interface ge-0/0/0`.
Review the returned list of interfaces to determine if LLDP is required on these ports, disabling it where it is not required.
LLDP may be disabled globally (in which case `set protocols lldp disable` will be returned in one line), or on one or more interfaces (returning `set protocols lldp interface <interface name> disable`).

Remediation:

To turn off LLDP globally for all interfaces, issue the following command from the `[edit protocols]` configuration hierarchy:

```
[edit protocols]
user@host# set lldp disable
```

Sending of LLDPDUs will be disabled, while any LLDP related configuration will be retained (but ignored).
Alternatively, you may wish to disable LLDP on a per-interface basis by issuing the

following command from the `[edit protocols]` configuration hierarchy:
To disable LLDP for a specific interface, leaving LLDP enabled for all others:

```
[edit protocols]
user@host# set lldp interface <interface name> disable
```

Or to disable LLDP for all interfaces and allow only for specific ports:

```
[edit protocols]
user@host# delete lldp interface all
user@host# set lldp interface <interface name>
```

This procedure should be repeated for all Routing Instances/Logical Systems where LLDP is configured but not required.

Default Value:

LLDP is disabled by default

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/device-discovery-using-lldp-lldp-med.html
2. https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-lldp-configuring.html

Additional Information:

For organizations which require LLDP or LLDP-MED, but wish to limit the information sent Junos allows administrators to control which TLVs will be sent.

- `tlv-filter` allows specific *non-mandatory* TLVs to be blocked, while sending all others
- `tlv-select` allows all *non-mandatory* TLVs to be blocked, with the exception of those specified by the administrator

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

4.12.2 Ensure LLDP-MED is Disabled if not Required (Manual)

Profile Applicability:

- Level 2

Description:

LLDP-MED should be disabled when not required

Rationale:

The *Link Layer Discovery Protocol (LLDP)* is a vendor-neutral and widely supported standard used for network devices to advertise information about their capabilities, identity, software and management details to other network devices on the LAN. LLDP is specified in the IEEE 802.1AB-2005 standard.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP published by the Telecommunications Industry Association (TIA) in the ANSI/TIA-1057 standard. LLDP-MED is primarily used to enable Voice over IP (VoIP) services by adding additional *Type-Length-Value (TLV)* data structures to the existing *LLDPDU* Ethernet Frames sent by LLDP. This information may include:

- Detailed information about Power Supply Type, Source and Priority (in the `ext-power-via-mdi` TLV)
- The physical location of the endpoint (configured via *Emergency Location Identification Number (ELIN)* or Geographic Location, in the `location-id` TLV)
- The Network Policy (VLAN configuration, DiffServ code points, in the `network-policy` TLV).

This information may be vital to provision of VoIP or other Media services, or when documenting/troubleshooting the network; but is also extremely useful to a potential attacker, either directly connected to the device or having compromised a neighbouring device.

To reduce the information given to a potential attacker, in high security environments LLDP-MED should be disabled where it is not absolutely required for normal operation. Like LLDP, LLDP-MED can either be disabled globally, or on a per interface basis (for example, leaving LLDP-MED enabled on access ports where it may be used for PoE or VoIP applications, but disabling it on infrastructure links or connections to untrusted networks).

LLDP-MED is not supported on all Junos device types, as it is primarily concerned with communication with VoIP Phones at the Access Layer. At present LLDP-MED is supported on:

- EX Series Access Switches (2200, 2300, 3300, 3400, 4200, 4300) (LLDP-MED enabled for all ports by default)
- Branch/Mid-Range and Virtual SRX Firewalls (SRX100-650, SRX1500, vSRX) (LLDP-MED disabled by default)
- NFX150 Network Services Platform (Virtual CPE) (defaults not clear)

Impact:

LLDP-MED is commonly used to support VoIP devices - disabling LLDP or LLDP-MED for these interfaces may result in service disruption.

Audit:

Due to the range of options as to the type of device, deployment scenario and where LLDP will be used in the network, it is not possible to provide Automated Scoring of this recommendation.
To check whether LLDP is enabled, use the following command from the `[edit protocols]` configuration hierarchy:

```
[edit protocols]
user@host#show lldp-med | display set | match "interface|disable"
```

LLDP-MED is enabled by default on EX series platforms, so will be enabled for all Interfaces if `set protocols lldp-med interface all disable` is *not* returned.
For other supported platforms LLDP-MED is disabled by default.
It may be enabled for all interfaces, in which case `set protocols lldp-med interface all` will be returned.
LLDP-MED may also be enabled (`set protocols lldp-med interface <interface name>`) or disabled (`set protocols lldp-med interface <interface name> disable`) on a per-interface basis.

Remediation:

To turn off LLDP-MED globally for all interfaces, issue the following command from the `[edit protocols]` configuration hierarchy:

```
[edit protocols]
user@host# set lldp-med interface all disable
```

Sending of LLDPDUs will be disabled, while any other LLDP-MED related configuration will be retained (but ignored).
Alternatively, you may wish to disable LLDP on a per-interface basis by issuing the following command from the `[edit protocols]` configuration hierarchy:
To disable LLDP-MED for a specific interface, leaving LLDP-MED enabled for all others:

```
[edit protocols]
user@host# set lldp-med interface <interface name> disable
```

Or to disable LLDP-MED for all interfaces and allow only for specific ports:

```
[edit protocols]
user@host# set lldp-med interface all disable
user@host# set lldp-med interface <interface name>
```

This procedure should be repeated for all Routing Instances/Logical Systems where LLDP-MED is configured but not required.

Default Value:

LLDP-MED is enabled by default on EX Series switches and disabled by default on other supported platforms

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/device-discovery-using-lldp-lldp-med.html
2. https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-lldp-configuring.html

Additional Information:

For organizations which require LLDP or LLDP-MED, but wish to limit the information sent Junos allows administrators to control which TLVs will be sent.

- `tlv-filter` allows specific *non-mandatory* TLVs to be blocked, while sending all others
- `tlv-select` allows all *non-mandatory* TLVs to be blocked, with the exception of those specified by the administrator

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

5 SNMP

Simple Network Management Protocol (SNMP) provides a standards based interface to manage and monitor network devices.

This section provides guidance on the secure configuration of SNMP parameters which are contained under the `[edit snmp]` hierarchy.

To confirm if your device is using SNMP, enter the following command:

```
[edit]
user@host# show snmp | count
```

If a line count of 1 or great is returned, your device is managed with SNMP and you should consider applying all recommendations in this section.

If you do not intend your device to be manageable with SNMP then you should delete any configuration at the `[edit snmp]` hierarchy with the command below:

```
[edit]
user@host# delete snmp
```

5.1 Ensure Common SNMP Community Strings are NOT used (Automated)

Profile Applicability:

- Level 1

Description:

Do not use common / default community strings.

Rationale:

SNMP can be used to read, and sometime write, sensitive information about your router and network environment.

When using SNMP Versions 1 and 2C (SNMPv2c) a community string is used to identify and, to a limited degree, authenticate Management Stations. If an attacker knows or guesses the community string that is used they may be able gain access to the SNMP interface as if they were a valid administrator.

To reduce the risk of an attacker guessing your community strings you should not use the following well known, common strings which are used as defaults on many brands of router:

- "Public"
- "Private"
- "Admin"
- "Monitor"
- "Security"

Any community used should be complex and should not match any of the passwords used elsewhere on the device or in your organization.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp | match community | match
"public|private|admin|monitor|security" | count
```

The above command should return 0 or an error.

Remediation:

If you have deployed SNMPv1 or SNMPv2c on your router using one of these strings, rename the community using the following command under the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#rename community <old community> to community <new community>
```

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.2.1 (page 77), National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.2.1 and 8.5

Additional Information:

SNMP communities are sent in clear text and should not match any passwords used elsewhere on the router or in your organization.

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

5.2 Ensure SNMPv1/2 are set to Read Only (Automated)

Profile Applicability:

- Level 1

Description:

Do not allow Read-Write SNMP access for versions below SNMPv3.

Rationale:

SNMP can be used to read and write configuration information from a router using your Network Management Systems; however the inherently insecure design of the older SNMP V1, V2 and V2C standards, which do not use encryption to protect community strings, make their use for setting configuration an open invitation to an attacker.

While, by default, a JUNOS router configured for SNMP Write access provides access only to Ping or Traceroute from the router, these still provide a potential source of information about your network or avenue for further attack so should not be permitted. Additional SNMP Management Information Base (MIB) views might be configured which, were Write access permitted, would allow an attacker to disable interfaces, change routing configuration or change anything else that you might do from the command line.

If an NMS is being used to configure routers via SNMP write access it should only do so via SNMPv3, which is significantly more secure.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp | match "authorization read-write" | count
```

The above command should return 0 or an error.

Remediation:

If you have deployed SNMP below Version 3 on your router with Read-Write access, delete the associated community using the following command under the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#delete community <community>
```

Alternatively you can set the communities authorization level to Read Only with the following command from the `[edit snmp <community>]` hierarchy;

```
[edit snmp]
user@host#set community <community> authorization read-only
```

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.2.1 (page 77), National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.2.1 and 8.5

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

5.3 Ensure a client list is set for SNMPv1/v2 communities (Automated)

Profile Applicability:

- Level 1

Description:

Limit clients to access SNMP.

Rationale:

Even when limited to read only access, SNMP can provide an attacker with a wealth of information about your router and network topology.

To limit the potential for attacks against your routers SNMP service you should limit the IP addresses that are permitted to connect using a client-list. This ensure that individual community strings are used to authenticate *only* by the systems in the list, providing granular access control that should be applied in addition to any firewall filter.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp | match "client-list-name" | count
```

The above command should return a positive integer equal to the number of communities configured on the router.

Remediation:

To configure a client list issue the following command under the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#edit client-list <client list name>

[edit snmp client-list <client list name>]
user@host#set default restrict
user@host#set <ip address/range>
user@host#set <ip address> restrict #optionally add exceptions
user@host#up 1

[edit snmp]
user@host#edit community <community name>

[edit snmp community <community name>]
user@host#set client-list-name <community name>
```

The `set default restrict` is covered in detail in the next recommendation.
Additional IP Addresses may be permitted by repeating the `set <ip address/range>` command as needed.
Optionally, addresses that you wish to deny from within a permitted range previously set can be configured with the `set <ip address> restrict` command.
Note - Client-lists may also be defined directly under the `[edit snmp community <community name> clients]` *hierarchy for use within the specified community with the same effect, but for ease of management and audit, the first method is preferred.*

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Configuring the SNMP Community String, JUNOS Software Management Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-net-mgmt/configuring-the-snmp-community-string.html#id-10428981)

CIS Controls:

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

5.4 Ensure “Default Restrict” is set in all client lists (Automated)

Profile Applicability:

- Level 1

Description:

Limit clients to access SNMP.

Rationale:

Even when limited to read only access, SNMP can provide an attacker with a wealth of information about your router and network topology.

To limit the potential for attacks against your routers SNMP service your client lists should be configured to deny any source address which is not explicitly permitted (by being added to the list).

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp | match "default restrict" | count
```

The above command should return a positive integer equal to the number of SNMP client lists configured on the router, which can be checked with the following command:

```
[edit]
user@host#show snmp | match "client-list" | count
```

Remediation:

To configure a client list issue the following command under the `[edit snmp client-list <client list name>]` hierarchy;

```
[edit snmp client-list <client list name>]
user@host#set default restrict
```

Note - Client-lists may also be defined directly under the `[edit snmp community <community name> clients]` *hierarchy for use within the specified community with the same effect, but for ease of management and audit, the first method is preferred.*

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Cisco IOS Benchmark Version 2.2, Requirement 1.1.5.6, Center for Internet Security
2. Configuring the SNMP Community String, JUNOS Software Management Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-net-mgmt/configuring-the-snmp-community-string.html#id-10428981)

CIS Controls:

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

5.5 Ensure SNMP Write Access is not set (Automated)

Profile Applicability:

- Level 2

Description:

Do not allow Read-Write SNMP access.

Rationale:

SNMP can be used to read and write configuration information from a router using your Network Management Systems; however the inherently insecure design of the older SNMP V1, V2 and V2C standards, which do not use encryption to protect community strings, make their use for setting configuration an open invitation to an attacker.

Even the more recent SNMPv3, which introduces encryption, authentication and message integrity checking, does not provide support for centralized authentication, account lockout or other basic security measures applied to other methods to access the router. This leaves the router vulnerable to brute force attack. The use of UDP as the transport mechanism in SNMP also makes spoofing the source of an SNMP request far simpler, easing brute force or flooding attacks.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp | match "read-write|write-view" | count
```

The above command should return 0 or an error.

Remediation:

If you have deployed SNMP below Version 3 on your router with Read-Write access, delete the associated community using the following command under the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#delete community <community>
```

Alternatively you can set the communities authorization level to Read Only with the following command from the `[edit snmp <community>]` hierarchy;

```
[edit snmp]
user@host#set community <community> authorization read-only
```

If you have deployed SNMP Version 3 on your router with Write access, delete the write view using the following command under the `[edit snmp v3 vacm access]` hierarchy;

```
[edit snmp v3 vacm access]
user@host#delete group <group name> default-context-prefix security-model
<security model> security-level <security level> write-view
```

Complete the sections in <> with the details configured for your group/s. This command will leave any read or notify views for the group in place. If only a write-view is configured, the group can be deleted instead.

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.2.1 (page 77), National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.1.6 and 8.2.1

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.6 Ensure AES128 is set for all SNMPv3 users (Automated)

Profile Applicability:

- Level 2

Description:

Do not allow plaintext SNMPv3 access.

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages.

When configuring a user for SNMPv3 you have the option of using a range of encryption schemes, or no encryption at all, to protect messages in transit. The strongest scheme available is AES128 and this should be configured for all SNMPv3 "users" on all sensitive devices.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp v3 usm local-engine | match "privacy-aes128" | count
```

The above command should return a positive integer equal to the number of configured SNMPv3 "users", which can be checked using the following command:

```
[edit]
user@host#show snmp v3 usm local-engine | match "user" | count
```

Remediation:

For each SNMPv3 user created on your router add privacy options by issuing the following command from the `[edit snmp v3 usm local-engine]` hierarchy;

```
[edit snmp v3 usm local-engine]
user@host#set user <username> privacy-aes128 privacy-password <password>
```

Default Value:

No SNMP is configured by default on most platforms.

References:

1. Creating SNMPv3 Users, JUNOS Software Network Management Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/config-guide-network-mgm/snmpv3-users-creating-junos-nm.html#id-10699507)

Additional Information:

An Authentication method and key must be configured for the user prior to configuring the Privacy method.

On some export versions of JUNOS the AES algorithm is not supported due to legal restrictions. On these platforms 3DES or DES should be utilized, with 3DES preferred if available.

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.7 Ensure SHA1 is set for SNMPv3 authentication (Automated)

Profile Applicability:

- Level 2

Description:

Do not allow unauthenticated SNMPv3 access.

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages. Authentication in SNMPv3 is performed using Keyed-Hash Message Authentication Code or HMAC. This technique uses a cryptographic hash function in combination with a secret key to authenticate and ensure the integrity of a given message.

JUNOS supports the MD5 and SHA1 hash functions for use in SNMPv3 authentication. MD5 is an older protocol which has shown significant vulnerability in recent years, so the more recent and more trusted SHA1 should be used.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp v3 usm local-engine | match "authentication-sha" | count
```

The above command should return a positive integer equal to the number of configured SNMPv3 "users".

Remediation:

For each SNMPv3 user created on your router add privacy options by issuing the following command from the `[edit snmp v3 usm local-engine]` hierarchy;

```
[edit snmp v3 usm local-engine]
user@host#set user <username> authentication-sha authentication-password
<password>
```

Default Value:

No SNMP communities are set by default on most platforms.

References:

1. Creating SNMPv3 Users, JUNOS Software Network Management Configuration Guide, Juniper Networks

Additional Information:

SHA1 is not supported on some export versions of JUNOS due to legal restrictions. In these instances MD5 should be utilized instead.

SHA1 is no longer considered as strong as it once was, but is the strongest hashing algorithm currently supported within the SNMPv3 USM standard. Weakness of this algorithm is, in part, why SNMPv3 write access should not be permitted.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

5.8 Ensure interface restrictions are set for SNMP (Automated)

Profile Applicability:

- Level 1

Description:

SNMP should only be configured on required interfaces.

Rationale:

By default the SNMP service will listen for incoming connections on all interfaces which have an IP Address configured, exposing SNMP to users on all networks through which the router is reachable.

In most cases the router should only be manageable over some of its interfaces; in particular a router providing connectivity to untrusted networks such as the Internet should only be manageable from trusted sources.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp interfaces
```

The configured Interface or Interfaces should be returned.

Remediation:

To restrict SNMP to required interfaces issue the following command from the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#set interface <interface or interface list>
```

Default Value:

By default SNMP, when configured, is accessible over all configured interfaces.

References:

1. Configuring the Interfaces on Which SNMP Request Can Be Accepted, JUNOS Software Management Configuration Guide, Juniper Networks

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

5.9 Ensure SNMP is set to OOB management only (Automated)

Profile Applicability:

- Level 2

Description:

SNMP should only be configured on Out of Band management interfaces.

Rationale:

By default the SNMP service will listen for incoming connections on all interfaces which have an IP Address configured, exposing SNMP to users on all networks through which the router is reachable.

In higher security environments management services, such as SNMPv3, should be restricted such as to only be reachable through the Out of Band management port which is available on most JUNOS platforms.

The name of the Out of Band Management port varies considerably between platforms, typically:

- `fxp[0-9]` on most routing platforms and SRX firewalls
- `me[0-9]` on most EX and some QFX switches
- `em[0-9]` on some EX and QFX switches
- `jmgmt0` on NFX platforms

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show snmp interfaces | display xml | match "<interface>" | match
"fxp[0-9]|em[0-9]|me[0-9]|jmgmt" | count
```

This should output a positive integer showing the number of Out of Band Management interfaces configured for SNMP. Compare this to the number of non Out of Band Management interfaces

```
[edit]
user@host#show snmp interfaces | display xml | match "<interface>" | except
"fxp[0-9]|em[0-9]|me[0-9]|jmgmt" | count
```

This should return 0. If a positive integer is returned, the non Out of Band Management interfaces should be removed.

Remediation:

To restrict SNMP to required interfaces issue the following command from the `[edit snmp]` hierarchy;

```
[edit snmp]
user@host#set interface <interface or interface list>
```

To delete an existing interface from the list issue the following command from the `[edit snmp]` hierachy;

```
[edit snmp]
user@host#delete interface <interface>
```

Default Value:

By default SNMP, when configured, is accessible over all configured interfaces.

References:

1. Configuring the Interfaces on Which SNMP Request Can Be Accepted, JUNOS Software Management Configuration Guide, Juniper Networks

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

6 System

This section explores settings that apply to the JUNOS System itself such as DNS Servers, Hostname, Configuration Archiving or Users.

These settings are all applied under the `[edit system]` hierarchy.

A subset of these settings may be applied on a per Logical System basis at the `[edit logical-system "LSYS Name" system]` hierarchy.

6.1 Accounting

When using External Authentication, Authorization and Accounting services, the Accounting mechanisms provide centralized record of what a router and its users are doing and when.

Keeping records of accounting information separate to the router is vital to allow administrators to spot when an attack may have occurred and to reconstruct what happened in the aftermath of an attack.

On Juniper routers, accounting services are configured under `[edit system accounting]` and should be configured whenever External AAA services like RADIUS or TACACS+ are used.

6.1.1 Ensure Accounting Destination is configured (Automated)

Profile Applicability:

- Level 1

Description:

Where external Authentication, Authorization and Accounting services using either RADIUS or TACACS+ are used, accounting data should be sent to at least one AAA server destination.

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services.

Both protocols provide services to receive and record information about what users and processes on a router are doing.

Where RADIUS or TACACS+ are configured for AAA, at least one accounting RADIUS or TACACS+ server should be configured to record accounting data for the JUNOS device. Generally, it is recommended that more than one server is used to ensure resilience of this vital service.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system accounting destination | match "server" | count
```

The above command should return an integer value greater than or equal to 1.

Remediation:

Configure one or more RADIUS or TACACS+ servers as Accounting Destinations use the following commands under the `[edit system accounting destination]` hierarchy; For RADIUS

```
[edit system accounting destination]
user@host#set radius server <server ip> secret <shared secret>
```

For TACACS+

```
[edit system accounting destination]
user@host#set tacplus server <server ip> secret <shared secret>
```

Default Value:

Accounting is not configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 166, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.2

Additional Information:

Use of External AAA services is *highly recommended* for all network devices.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

6.1.2 Ensure Accounting of Logins (Automated)

Profile Applicability:

- Level 1

Description:

When External AAA is used, Login Events should be sent to configured accounting destinations.

Rationale:

To protect any asset, including a Juniper router, you have to have a record of who logged in or attempted to login as well as who made changes to the configuration and when.

JUNOS can log these events to RADIUS and/or TACACS+ servers to allow reliable, centralized records to be kept for all of the devices in your network.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system accounting
```

The above command should return the output below:

```
accounting {
      events login;
}
```

Additional configuration items for Accounting may be present.

Remediation:

Configure Accounting of Logins and Configuration Changes by entering the following commands under the `[edit system accounting]` hierarchy;

```
[edit system accounting]
user@host#set events login
```

Default Value:

External accounting is not configured by default

References:

1. Router Security Configuration Guide, Version 1.1b, Page 166, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.2

Additional Information:

Use of External AAA services is *highly recommended* for all network devices.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.1.3 Ensure Accounting of Configuration Changes (Automated)

Profile Applicability:

- Level 1

Description:

When External AAA is used Configuration Change events should be sent to configured accounting destinations.

Rationale:

To protect any asset, including a Juniper router, an audit trail of changes made to the devices configuration, when they were made and by whom is essential.

JUNOS can log these events to RADIUS and/or TACACS+ servers to allow reliable, centralized records to be kept for all of the devices in your network.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system accounting
```

The above command should return the output below:

```
accounting {
      events change-log;
}
```

Additional configuration items for Accounting may be present.

Remediation:

Configure Accounting of Logins and Configuration Changes by entering the following commands under the `[edit system accounting]` hierarchy;

```
[edit system accounting]
user@host#set events change-log
```

Default Value:

External accounting is not configured by default

References:

1. Router Security Configuration Guide, Version 1.1b, Page 166, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.2

Additional Information:

Use of External AAA services is *highly recommended* for all network devices.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.1.4 Recommend Accounting of Interactive Commands (where External AAA is used) (Automated)

Profile Applicability:

- Level 2

Description:

Where External AAA is used, Interactive Command Accounting Events should be sent to either TACACS+ or RADIUS.

Rationale:

To protect any asset, including a Juniper router, you have to have a record of who logged in or attempted to login as well as who made changes to the configuration and when. For additional security you should also keep records of all commands issued, who issued them and when.

This is not possible in all deployments due to the additional load, network traffic and storage requirements. For most scenarios the high resource use is outweighed by the benefits that the command history provides, particularly in responding to an incident or fault.

JUNOS can log these events to RADIUS and/or TACACS+ servers to allow reliable, centralized records to be kept for all of the devices in your network.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system accounting
```

The above command should return the output below:

```
accounting {
      events interactive-commands;
}
```

Additional configuration items for Accounting may be present on the same line.

Remediation:

Configure Accounting of Logins and Configuration Changes by entering the following commands under the `[edit system accounting]` hierarchy;

```
[edit system accounting]
user@host#set events [change-log interactive-commands login]
```

The interactive-commands should be selected at a minimum, although in many cases you may also wish to add change-log and login accounting.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 166, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.2

Additional Information:

Use of External AAA services is *highly recommended* for all network devices.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.2 Archival

JUNOS can be configured to send a backup of its configuration to an external destination using the options set under the `[edit system archival]` hierarchy.

This can provide the administrator with both a significant security benefit for tracking changes or post incident investigation, and to general system availability by allowing for more rapid recovery in the event of a fault of device failure.

It is *highly recommended* that all JUNOS devices are backed up to external destinations on a regular basis or after any change. For some organizations the built-in system archival tool discussed here will be the correct solution for backup, while for others 3rd party tools such as RANCID (http://www.shrubbery.net/rancid/) or Oxidized (https://github.com/ytti/oxidized), which are not configured directly on the device, maybe more suitable.

6.2.1 Ensure Archive on Commit (Automated)

Profile Applicability:

- Level 2

Description:

The routers configuration should be archived whenever changes are committed.

Rationale:

Before changes made to a JUNOS router are applied they must be committed. Archiving the configuration to an external server on every commit creates a complete history of all changes allowing an effective 'post mortem' to be carried out following any breach and aiding recovery to security and other incidents.

The archive can also be used to alert administrators of unauthorized changes and identify what was changed by utilizing hashes or diff in scripts or systems like Tripwire.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system archival
```

The above command should yield the following output:

```
configuration {
      transfer-on-commit
}
```

Additional configuration items for the Archival service may be present between the curly braces.

Remediation:

To enable Archival on commit issue the following commands from the `[edit system]` hierarchy;

```
[edit system]
user@host#set archival configuration transfer-on-commit
```

Default Value:

Archival is not configured by default.

References:

1. Archival, JUNOS 9.2 System Basic Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-system-basics/archival.html)

CIS Controls:

Version 7

10.4 Ensure Protection of Backups

Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

6.2.2 Ensure at least one SCP Archive Site is configured (Automated)

Profile Applicability:

- Level 2

Description:

Configuration archival should use only secure transport over SCP.

Rationale:

Archiving the configuration to an external server creates a history of changes allowing an effective 'post mortem' to be carried out following any breach and aiding recovery to security and other incidents.

The archive can also be used to alert administrators of unauthorized changes and identify what was changed by utilizing hashes or diff in scripts or systems like Tripwire.

At least one Secure Copy (SCP) Archive Site should be configured on the router. No other transport methods should be used.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system archival configuration archive-sites | match "scp://" |
count
```

The command above should return a positive integer equal to or greater than 1.

Remediation:

To enable a Secure Copy Archival Site on commit issue the following commands from the `[edit system]` hierarchy;

```
[edit system]
user@host#set archival configuration archive-site <SCP URL> password
<password>
```

Default Value:

Archival is not configured by default

References:

1. Archival, JUNOS 9.2 System Basic Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-system-basics/archival.html)

CIS Controls:

Version 7

10.1 Ensure Regular Automated Back Ups
Ensure that all system data is automatically backed up on regular basis.

10.4 Ensure Protection of Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

6.2.3 Ensure NO Plain Text Archive Sites are configured (Automated)

Profile Applicability:

- Level 1

Description:

The routers configuration MUST NOT be sent in plain text to the Archive Site.

Rationale:

JUNOS routers can use a range of protocols for copying configuration files to Archive Sites including FTP, TFTP, NFS and SCP. Of these, only Secure Copy (SCP) provides encryption for the data in transit. Using FTP, FTP or NFS transfer files in plain text, allowing an attacker to copy the file from the network exposing sensitive data and possibly authentication information for both the router and the Archive Site.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system archival configuration archive-sites | match
"ftp://|file://|tftp://" | count
```

The command above should return 0 or an error.

Remediation:

Archival is not configured by default. If plain text Archive Sites have been configured, they can be removed by issuing the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#delete archival configuration archive-site <URL>
```

Archive sites should be reconfigured using SCP.

Default Value:

Archival is not configured by default.

References:

1. Archival, JUNOS 9.2 System Basic Configuration Guide, Juniper Networks

CIS Controls:

Version 7

10.4 Ensure Protection of Backups

Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

6.3 Authentication-Order

Each user of a Juniper router must have a unique username and password which allows them to be identified for Authentication, Authorization and Accounting (AAA) purposes. Centralized AAA services such as RADIUS and TACACS+ provide essential mechanisms to protect network devices.

Most critically, centralized Authentication provides network administrators with the ability to manage user accounts in a single place to affect all of the devices in their network. This is vital in situations where, for example, an employee leaves the organization or a user account is compromised by an attacker.

Juniper devices support multiple Authentication protocols, the order in which these are used can be configured under `[edit system authentication-order]`. Understanding the devices AAA settings is fundamental to securing your network.

6.3.1 Ensure external AAA is used (Automated)

Profile Applicability:

- Level 1

Description:

At least one external Authentication method should be specified.

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services. Both protocols provide services to authenticate users on routers, switches and other systems.

Juniper routers support both RADIUS and TACACS+ authentication. JUNOS will use each of the configured protocols in order set under `[edit system authentication-order]` until the password is accepted or the end of the list is reached.

It is vital to understand the impact of this behavior and its relation to security. If the order is set as RADIUS then TACACS+, the router will attempt to authenticate a user's credentials first using the RADIUS server. If the RADIUS server cannot be reach *or the login is denied* the router will attempt to authenticate against TACACS+.

Settings for RADIUS or TACACS+ servers themselves for Authentication are configured separately under the `[edit system radius-server]` or `[edit system tacplus-server]` hierarchies respectively.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system authentication-order | match "radius|tacplus" | count
```

The above command should return an integer value of 1.

Remediation:

Configure at least one external Authentication method using the following commands under the `[edit system]` hierarchy; For RADIUS

```
[edit system]
user@host#set authentication-order radius
```

For TACACS+

```
[edit system]
user@host#set authentication-order tacplus
```

For RADIUS then TACACS+

```
[edit system]
user@host#set authentication-order [radius, tacplus]
```

For TACACS+ then RADIUS

```
[edit system]
user@host#set authentication-order [tacplus, radius]
```

Default Value:

By default all Juniper routers use local password authentication with accounts set under the `[edit system login user]` hierarchy.

References:

1. Configuring the Authentication Order, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-the-authentication-order.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.3.2 Ensure Local Accounts can ONLY be used during loss of external AAA (Automated)

Profile Applicability:

- Level 1

Description:

Authentication using locally configured usernames and passwords should only be permitted when External AAA servers are down or cannot be reached.

Rationale:

Juniper routers support local user accounts in addition to RADIUS and TACACS+ based authentication. JUNOS will use each of the configured protocols in order set under `[edit system authentication-order]` until the password is either accepted or the end of the list is reached.

It is vital to understand the impact of this behavior and its relation to security.

If the order is set as RADIUS then local password, the router will attempt to authenticate a user's credentials first using the RADIUS server. If the RADIUS server cannot be reach *or the login is denied* the router will attempt to authenticate against the user accounts configured in the `[edit system login user]` hierarchy.

Because local user accounts cannot be centrally audited and controlled they present a far greater risk when, for example, and account is compromised or an employee leaves the organization.

By removing local authentication from the authentication-order you prevent these accounts being used when RADIUS or TACACS+ reject an authentication attempt; however local accounts remain usable on occasions where all other authentication services cannot be reached such as during router maintenance or AAA server outages.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system authentication-order | match "password" | count
```

The above command should return zero or an error.

Remediation:

Remove local user authentication from the authentication order by issuing the following command from the `[edit system]` hierarchy; [edit system]

```
user@host#delete authentication-order password
```

This command will leave other authentication methods (RADIUS or TACACS+) that are already configured under the authentication-order statement.

Default Value:

By default all Juniper routers use local password authentication with accounts set under the `[edit system login user]` hierarchy.

References:

1. Configuring the Authentication Order, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-the-authentication-order.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.4 Diag-Port-Authentication

Many control boards used in Juniper routers provide a Diagnostic Port, intended for use by Juniper engineers or when working with JTAC to resolve problems. Juniper routers allow authentication to be configured for these diagnostic ports under the `[edit system diag-port-authentication]` hierarchy.

6.4.1 Ensure Authentication is configured for Diagnostic Ports (Automated)

Profile Applicability:

- Level 1

Description:

An encrypted password should be set for access to the routers diagnostic ports.

Rationale:

Most high end Juniper network devices contain Diagnostic Ports on one or more of the control boards installed in the system, such as FEB (Forwarding Engine Board) in M5 or M10 routers or SSB (System Switching Board) in M20 routers. These ports allow access to a range of diagnostic functions and could provide an attacker with physical access to the system a route to bypass other controls in order to compromise the router.

Because of this risk, it is possible to set a password for all Diagnostic Ports installed in the system. As with other similar items, the password is stored by JUNOS as a hash (in this case MD5) in the configuration file. Please note, only local authentication is supported for the Diagnostic Ports, which are intended for limited use only, often when the device is experience a serious outage where external AAA services may be unavailable.

Should a system not contain any diagnostic ports, this item of configuration is ignored by the device.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system diag-port-authentication
```

The above command should return the following output:

```
diag-port-authentication encrypted-password "<MD5 Hash>";
```

Remediation:

Configure a password for the diagnostic ports using one of the following commands under the `[edit system]` hierarchy; To enter a new password in plain text:

```
[edit system]
user@host#set diag-port-authentication plain-text-password
```

You will be prompted to enter the new password, which JUNOS will then hash with MD5 before placing the command in the candidate configuration. To enter an existing password hash which you have taken from an existing configuration file, type the following :

```
[edit system]
user@host#set diag-port-authentication encrypted-password "<MD5 Hash>"
```

Default Value:

By default no password is configured for diagnostic ports

References:

1. Configuring the Password on the Diagnostics Port, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-the-password-on-the-diagnostics-port.html#id-10969646)
2. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA)
3. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.2.3

CIS Controls:

Version 7

4.2 Change Default Passwords
Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

6.4.2 Ensure Diagnostic Port Authentication uses a complex password (Manual)

Profile Applicability:

- Level 1

Description:

A complex password should be used to protect access to Diagnostic Port/s

Rationale:

Due to the sensitivity of the routers Diagnostic Port/s a complex password should be employed to help prevent attackers employing 'brute force' or 'dictionary' attacks to gain access through these ports.

Passwords are stored, automatically by JUNOS, as a MD5 hash in the configuration under the `[edit system diag-port-authentication]` hierarchy.

A complex password should be employed which meets or exceeds the following requirements:

- Does not contain Dictionary words, names, dates, phone numbers or addresses.
- Is at least 8 characters in length (longer is recommended).
- Contains at least one each of upper & lower case letters, numbers and special characters.
- Avoids more than 4 digits or same case letters in a row.

Audit:

Because Diagnostic Port passwords are automatically stored by JUNOS as a MD5 hash, which will always be 128bits long, it is not possible to confirm from the command line the complexity and length of the password used therefore this is not a scored item.

Remediation:

Configure a password for the diagnostic ports using one of the following commands under the `[edit system]` hierarchy; To enter a new password in plain text :

```
[edit system]
user@host#set diag-port-authentication plain-text-password
```

You will be prompted to enter the new password, which JUNOS will then hash with MD5 before placing the command in the candidate configuration. To enter an existing password hash which you have taken from an existing configuration file, type the following :

```
[edit system]
user@host#set diag-port-authentication encrypted-password "<MD5 Hash>"
```

References:

1. Configuring the Password on the Diagnostics Port, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks](http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-the-password-on-the-diagnostics-port.html#id-10969646)
2. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA)
3. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.2.3

CIS Controls:

Version 7

4.2 Change Default Passwords
Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.5 Internet-Options

Using options under the `[system internet-options]` hierarchy, JUNOS provides administrators with a number of tools to protect a Juniper network device from common abuse of IP protocol options.

6.5.1 Ensure ICMPv4 rate-limit is Set (Automated)

Profile Applicability:

- Level 2

Description:

ICMPv4 traffic should be rate limited to protect the devices resources.

Rationale:

Many Denial of Service attacks against network devices will attempt to overwhelm the target's processing, memory or bandwidth by barraging the router with malicious ICMP traffic which may be easily spoofed or generated in significant volumes.

Some administrators simply block all ICMP traffic; however this can cause many problems such as the inability of hosts to perform Path MTU Discovery and preventing debugging through common tools such as Ping (ICMP Echo). Loss of these important ICMP functions can adversely affect the reliability or functionality of the network. By limiting the rate at which ICMP traffic can be sent or received by the Routing Engine, it is possible to limit the impact of many DoS attacks without losing the important functionality that ICMP provides to the network.

The limits are set using two parameters. The first, `packet-rate`, defines the number of ICMPv4 (of any type) packets allowed per second. Traffic below this rate will be allowed. Traffic above this rate will also be permitted so long as tokens remain in the "token bucket" associated with the policer. Each packet above the configured packet-rate uses one token until the bucket is empty, at which point all ICMPv4 traffic will be denied. The second parameter, `bucket-size`, defines the rate at which the token bucket is refilled, controlling the amount by which burst traffic will be permitted..

By default, once configured, the packet-rate will be 1000 packets per second with a bucket-size of 5 seconds. This should be sufficient on most platforms to prevent serious DoS attacks, whilst being high enough not to interfere with normal operation.

The administrator should set the limits based on the normal level of ICMPv4 traffic that is handled by the router. Failure to do this could cause the router to become unreliable in some cases.

This requirement deals only with ICMPv4 Exception Traffic *to or from the Routing Engine* (the Control Plane of a JUNOS device) and has no effect on ICMPv4 Transit Traffic *traversing* the device.

Impact:

If all accumulated packets in the bucket are used, rate limiting will drop all further ICMPv4 traffic to/from the RE until new packets have been added to the bucket at the rate defined by <limit>

Audit:

To confirm whether an ICMPv4 Rate Limit has been configured, enter the following command from the `[edit system internet-options]` hierarchy:

```
[edit system internet-options]
user@host#show icmpv4-rate-limit | count
```

The above command should return an integer value greater than or equal to 1.

Remediation:

ICMPv4 Rate Limiting can be configured by issuing the following commands from the `[edit system internet-options]` hierarchy.

```
[edit system internet-options]
user@host#set icmpv4-rate-limit bucket-size <bucket> packet-limit <limit>
```

Where:

- <bucket> is the size of the Rate Limit Bucket, in seconds (if not specified, defaults to 5 seconds)
- <limit> is the rate at which packets are added to the bucket, in packets per second (if not specified, defaults to 1000pps)

Default Value:

By default icmpv4-rate-limit is not configured.

Once configured the bucket-size defaults to 5 seconds and the packet-limit defaults to 1000 packets per second.

References:

1. icmpv4-rate-limit, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (https://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/icmpv4-rate-limit.html#id-11178870)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/icmpv4-rate-limit-edit-system.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.5.2 Ensure ICMPv6 rate-limit is Set (Automated)

Profile Applicability:

- Level 2

Description:

ICMPv6 traffic should be rate limited to protect the devices resources.

Rationale:

Many Denial of Service attacks against network devices will attempt to overwhelm the target's processing, memory or bandwidth by barraging the router with malicious ICMP traffic which may be easily spoofed or generated in significant volumes.

Some administrators simply block all ICMP traffic; however this can cause many problems such as the inability of hosts to perform Path MTU Discovery and preventing debugging through common tools such as Ping (ICMP Echo). Loss of these important ICMP functions can adversely affect the reliability or functionality of the network. By limiting the rate at which ICMP traffic can be sent or received by the Routing Engine, it is possible to limit the impact of many DoS attacks without losing the important functionality that ICMP provides to the network.

The limits are set using two parameters. The first, `packet-rate`, defines the number of ICMPv6 (of any type) packets allowed per second. Traffic below this rate will be allowed. Traffic above this rate will also be permitted so long as tokens remain in the "token bucket" associated with the policer. Each packet above the configured packet-rate uses one token until the bucket is empty, at which point all ICMPv6 traffic will be denied. The second parameter, `bucket-size`, defines the rate at which the token bucket is refilled, controlling the amount by which burst traffic will be permitted..

By default, once configured, the packet-rate will be 1000 packets per second with a bucket-size of 5 seconds. This should be sufficient on most platforms to prevent serious DoS attacks, whilst being high enough not to interfere with normal operation.

The administrator should set the limits based on the normal level of ICMPv6 traffic that is handled by the router. Failure to do this could cause the router to become unreliable in some cases.

This requirement deals only with ICMPv6 Exception Traffic *to or from the Routing Engine* (the Control Plane of a JUNOS device) and has no effect on ICMPv6 Transit Traffic *traversing* the device.

Impact:

If all accumulated packets in the bucket are used, rate limiting will drop all further ICMPv6 traffic to/from the RE until new packets have been added to the bucket at the rate defined by

Audit:

To confirm whether ICMPv6 Rate Limiting has been configured, enter the following command from the `[edit system internet-options]` hierarchy:

```
[edit system internet-options]
user@host#show icmpv6-rate-limit | count
```

A line count of 1 should be returned, indicating that ICMPv6 Rate Limiting is set.

Remediation:

ICMPv6 Rate Limiting can be configured by issuing the following commands from the [edit system internet-options] hierarchy.

```
[edit system internet-options]
user@host#set icmpv6-rate-limit bucket <bucket> limit <limit>
```

Where:

- is the size of the Rate Limit Bucket, in seconds (if not specified, defaults to 5 seconds)
- is the rate at which packets are added to the bucket, in packets per second (if not specified, defaults to 1000pps)

Default Value:

By default icmpv6-rate-limit is not configured.

Once configured the bucket-size defaults to 5 seconds and the packet-limit defaults to 1000 packets per second

References:

1. icmpv6-rate-limit, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (https://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/icmpv6-rate-limit.html#id-11148130)

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.5.3 Ensure ICMP Source-Quench is Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

ICMP Source Quench messages should be ignored.

Rationale:

ICMP Source Quench messages are intended to allow a host to request that a peer with which it is communicating slows down the transmission of new data because the host is being overwhelmed.

Several recorded vulnerabilities have shown how Source Quench messages may be abused by an attacker to create a DoS attack, causing the router to slow down transmission of data to one, several or all destinations. Due to these vulnerabilities, and the general ineffectiveness of Source Quench for congestion control, RFC6633 deprecated its use and ICMP Source Quench should be disabled.

Impact:

ICMP Source Quench is deprecated and there is no valid reason for ICMP Source Quench to be present on a modern network.

Audit:

To confirm whether ICMP Source Quench Requests will be dropped, enter the following command from the `[edit system internet-options]` hierarchy:

```
[edit system internet-options]
user@host#show no-source-quench | count
```

A line count of 1 should be returned, indicating that the ICMP Source Quench is Set to Disabled.

Remediation:

Configure the JUNOS Device to ignore ICMP source-quench messages by issuing the following command from the `[edit system internet-options]` hierarchy.

```
[edit system internet-options]
user@host#set no-source-quench
```

Default Value:

By default the router does not ignore ICMP Source Quench messages.

References:

1. Configuring Source Quench, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (https://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-source-quench.html#id-10993765)
2. http://www.kb.cert.org/vuls/id/222750
3. https://tools.ietf.org/html/rfc6633

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.5.4 Ensure TCP SYN/FIN is Set to Drop (Automated)

Profile Applicability:

- Level 1

Description:

TCP Segments which have both the SYN and FIN flags set should be dropped.

Rationale:

TCP packets that have both SYN and FIN flags set are sometimes used by attackers to bypass Intrusion Detection Systems and Firewalls or to directly attack hosts on the target network. If patches are up-to-date then most systems are no longer vulnerable to this technique; however, there is no valid reason for a packet to contain both SYN and FIN flags, so such traffic is almost certainly malicious or the result of an error and should *never* be processed.

Impact:

There is no valid reason for a TCP Segment to have both SYN and FIN flags set.

Audit:

To confirm whether the Device is configured to drop SYN/FIN Segments, issue the following command from the `[edit system internet-options]` hierarchy:

```
[edit system internet-options]
user@host#show | match "synfin" | count
```

A line count of 1 should be returned, indicating that TCP Segments with SYN/FIN set will be dropped.

Remediation:

Configure the router to drop TCP Segments containing both SYN and FIN flags by issuing the following command from the `[edit system internet-options]` hierarchy.

```
[edit system internet-options]
user@host#set tcp-drop-synfin-set
```

Default Value:

By default JUNOS does not drop TCP packets with both TCP SYN and FIN flags set.

References:

1. Configuring the Router to Drop Packets with the SYN and FIN Bits Set, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (https://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-the-router-to-drop-packets-with-the-syn-and-fin-bits-set.html#id-10938681)
2. http://www.kb.cert.org/vuls/id/464113

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.5.5 Ensure TCP RST is Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Connection attempts to a closed / non-listening port should not return a TCP RST

Rationale:

As with most Operating Systems, by default, when a client attempts to connect to a TCP port which is not being used by a service to listen for connections JUNOS will return a TCP RST message to inform the client that there is no service available on that port.

This behavior may aide an attacker who is performing port scanning to identify open services as part of a reconnaissance of the network or may allow Denial of Service (DoS) attack to be performed by placing unnecessary processing load on the Routing Engine.

No valid use exists for attempting to connect to non-listening ports on a router or other network device, so JUNOS should be configured to silently drop all packets (with any flags) sent to closed TCP ports without sending a TCP reset (RST). The client attempting to connect will timeout rather than getting instant feedback, reducing the load on the JUNOS device and increasing the time required for any port scanning.

Impact:

Connection attempts to closed/non-listening ports on the JUNOS Device will time out rather than receiving a TCP RST.

Audit:

To confirm whether TCP RST is disabled, enter the following command from the `[edit system internet-options]` hierarchy:

```
[edit system internet-options]
user@host#show | display set | match | "no-tcp-reset drop-all-tcp" | count
```

A line count of 1 should be returned, indicating that TCP RST is set to Disabled.

Remediation:

To disable sending TCP RSTs to any connections to closed ports issue the following command from the `[edit system internet-options]` hierarchy.

```
[edit system internet-options]
user@host#set no-tcp-reset drop-all-tcp
```

Default Value:

By default JUNOS sends TCP RSTs to connections made to non-listening ports.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-tcp-reset-edit-system-internet-options.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.6 Login

A variety of options can be set to control the login process and users on a JUNOS router under the `[edit system login]` hierarchy.

6.6.1 Retry Options

Options that dictate how the router treats failed remote login attempts are configured under the `[edit system login retry-options]` hierarchy.

6.6.1.1 Ensure Max 3 Failed Login Attempts (Automated)

Profile Applicability:

- Level 1

Description:

A maximum of 3 failed login attempts should be allowed before the session is disconnected.

Rationale:

Remote administration protocols like Telnet and SSH are commonly targeted by Brute Force or Dictionary attacks where a malicious user attempts to guess a valid username/password combination in order to gain control of the router. To slow down the rate at which an attacker can attempt to guess passwords, sessions should be disconnected after no more than 3 failed login attempts (a lower value can be used if preferred).

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login retry-options tries-before-disconnect
```

The above command should return an integer value equal to or less than 3.

Remediation:

Configure the number of tried before disconnect using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login retry-options tries-before-disconnect
```

Default Value:

For most JUNOS version the default is to disconnect after 10 failed login attempts.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 229, National Security Agency (NSA)
2. Configuring Password Retry Limits for Telnet and SSH Access, JUNOS 9.5 Security Configuration Guide, Juniper Network (http://www.juniper.net/techpubs/software/junos-security/junos-

security95/junos-security-admin-guide/config-passwd-retry-telnet-ssh.html#config-passwd-retry-telnet-ssh)

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.1.2 Ensure Max Login Backoff Threshold of 2 (Automated)

Profile Applicability:

- Level 1

Description:

A *maximum* of 2 failed login should trigger a backoff.

Rationale:

Remote administration protocols like Telnet and SSH are commonly targeted by Brute Force or Dictionary attacks where a malicious user attempts to guess a valid username/password combination in order to gain control of the router. To slow down the rate at which an attacker can attempt to guess passwords Juniper routers can initiate a backoff timer when a user login fails more times than a configured threshold. Once initiated the backoff will not allow a further login attempt by the user for a configured (see next recommendation) period of time called the backoff factor. After the next failed login attempt further logins will not be allowed for the 2x the backoff factor, then 3x and so on.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login retry-options backoff-threshold
```

The above command should return an integer value equal to or less than 2.

Remediation:

Configure the backoff threshold using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login retry-options backoff-threshold <threshold>
```

Default Value:

For most JUNOS version the default is to backoff after 2 failed login attempts.

References:

1. Configuring Password Retry Limits for Telnet and SSH Access, JUNOS 9.5 Security Configuration Guide, Juniper Network (http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/config-passwd-retry-telnet-ssh.html#config-passwd-retry-telnet-ssh)

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.1.3 Ensure Minimum Backoff Factor of 5 (Automated)

Profile Applicability:

- Level 1

Description:

A *minimum* of 5 seconds should be used for the backoff factor.

Rationale:

Remote administration protocols like Telnet and SSH are commonly targeted by Brute Force or Dictionary attacks where a malicious user attempts to guess a valid username/password combination in order to gain control of the router. To slow down the rate at which an attacker can attempt to guess passwords Juniper routers can initiate a backoff timer when a user login fails more times than a configured threshold. Once initiated the backoff will not allow a further login attempt by the user for a configured (see next recommendation) period of time called the backoff factor. After the next failed login attempt further logins will not be allowed for the 2x the backoff factor, then 3x and so on.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login retry-options backoff-factor
```

The above command should return an integer value equal to or greater than 5.

Remediation:

Configure the backoff threshold using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login retry-options backoff-factor
```

Default Value:

For most JUNOS version the default is to backoff factor of 5 seconds.

References:

1. Configuring Password Retry Limits for Telnet and SSH Access, JUNOS 9.5 Security Configuration Guide, Juniper Network

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.1.4 Ensure Minimum Session Time of at least 20 seconds (Automated)

Profile Applicability:

- Level 1

Description:

A Minimum Session Time should be set to *at least* 20 seconds.

Rationale:

Remote administration protocols like Telnet and SSH are commonly targeted by Brute Force or Dictionary attacks where a malicious user attempts to guess a valid username/password combination in order to gain control of the router. To slow down the rate at which an attacker can attempt to guess passwords Juniper routers can enforce a minimum session time, preventing an attacker from attempting to circumvent the backoff timer through using multiple sessions.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login retry-options minimum-time
```

The above command should return an integer value equal to or greater than 20.

Remediation:

Configure the Minimum Session Time using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login retry-options minimum-time
```

Default Value:

For most JUNOS version the default is a Minimum Session Time of 20 seconds.

References:

1. Configuring Password Retry Limits for Telnet and SSH Access, JUNOS 9.5 Security Configuration Guide, Juniper Network

(http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/config-passwd-retry-telnet-ssh.html#config-passwd-retry-telnet-ssh)

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.1.5 Ensure Lockout-period is set to at least 30 minutes (Automated)

Profile Applicability:

- Level 1

Description:

Users who have been disconnected due to bad login attempts should be locked out for 30 minutes.

Rationale:

Remote administration protocols like Telnet and SSH are commonly targeted by Brute Force or Dictionary attacks where a malicious user attempts to guess a valid username/password combination in order to gain control of the router.

To slow down the rate at which an attacker can attempt to guess passwords accounts disconnected by the *tries-before-disconnect* option should be locked out for a period of 30 minutes.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login retry-options lockout-period
```

The above command should return an integer value equal to or greater than 30.

Remediation:

Configure the time users should be locked out using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login retry-options lockout-period 30
```

Default Value:

By default users who are disconnected for multiple failed login attempts are not locked out.

References:

1. JUNOS Administration Guide for Security Devices - lockout-period (https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/lockout-period-edit-system-login-retry-options.html)
2. JUNOS Administration Guide for Security Devices - clear locked out users - (https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/clear-system-login-lockout.html)
3. NIST SP800-123, General Server Security Guidance, Section 4.2.2 Configure OS User Authentication (https://www.nist.gov/publications/guide-general-server-security)

Additional Information:

Genuine users may be locked out when they enter their credentials incorrectly multiple times. An authenticated user may unlock a user who's account is locked out with the '''clear system lockout user ''' command.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.2 Ensure Login Class is set for all Users Accounts (Automated)

Profile Applicability:

- Level 1

Description:

All user accounts must have a class set.

Rationale:

Controlling the level of access which users are granted when logging into a router, helps protect against both malicious attacks and accidental misconfiguration of the router by less experienced staff.

Configuring user permissions on a user by user basis can quickly become unwieldy and difficult to manage, potentially leading to mistakes with a serious impact on the routers security. Instead, permissions should be assigned to classes to which individual users are linked in order to grant the appropriate level of access that corresponds with their job role.

JUNOS provides 4 built in Login Classes:

- Operator (can perform operational commands like ping but cannot view or edit the configuration or reboot the device)
- read-only (can view configuration and perform some operational commands)
- super-user (can issue any command)
- unauthorized (can login, but cannot perform any actions except for logging out)

In addition to the built in classes, JUNOS allows administrators to configure Custom Login Classes and to permit or deny additional permissions through Vendor Specific Attributes used with External AAA Servers like RADIUS or TACACS+.

Because a user account, whether being used for a local user or used as a template for logins from External AAA, will be placed in the highly privileged `super-user' class by default - it is essential that all user accounts be explicitly configured with the required login class, even when further restrictions are being applied through permit/deny commands by External AAA.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login | display set | match "login user.* class " |
count
```

The above command should return a positive integer equal to the number of configured users, which can be confirm with the following command:

```
[edit]
user@host#show system login | display set | match "login user " | count
```

Remediation:

Configure a class for a user account using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set user <username> class <class name>
```

Default Value:

By default all users are, in effect, members of the super-user class.

References:

1. JUNOS Login Classes Overview, JUNOS 9.5 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/frameset.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 7.1.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

16 Account Monitoring and Control
Account Monitoring and Control

6.6.3 Ensure Idle Timeout is set for all Login Classes (Automated)

Profile Applicability:

- Level 1

Description:

All login classes should have an idle timeout defined.

Rationale:

Controlling the level of access which users are granted when logging into a router, helps protect against both malicious attacks and accidental misconfiguration of the router by less experienced staff.

Login classes should be defined to grant permissions to user accounts, both local and remote, allowing permissions to be managed in a similar manner to User Groups on a Microsoft Windows system.

All login classes should have an Idle Timeout of no more than 15 minutes configured, so that unused sessions are automatically logged out after this time, limiting the scope for abuse of unattended sessions.

Note - *The built in Super-User Class does not have an Idle Timeout configured and, for this reason, should be used extremely sparingly if at all.*

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login | match "idle-timeout [0-9]|idle-timeout 1[0-5]"
| count
```

The above command should return a positive integer equal to the number of configured classes.

Remediation:

Configure the Idle Timeout for a class using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set class <class name> idle-timeout <timeout in minutes>
```

Default Value:

No idle timeout is defined by default.

References:

1. JUNOS Login Classes Overview, JUNOS 9.5 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/frameset.html)

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

6.6.4 Ensure Custom Login Classes have Permissions Defined (Automated)

Profile Applicability:

- Level 1

Description:

All login classes should have permissions defined.

Rationale:

Controlling the level of access which users are granted when logging into a router, helps protect against both malicious attacks and accidental misconfiguration of the router by less experienced staff. Login classes should be defined to grant permissions to user accounts, both local and remote, allowing permissions to be managed in a similar manner to User Groups on a Microsoft Windows system.

All Custom Login classes should have one more permissions defined which will be applied to all users, local and remote, linked to the class.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login | match "permissions" | count
```

The above command should return a positive integer equal to the number of configured classes.

Remediation:

Configure the Permissions for a class using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set class <class name> permissions <permission or list of
permissions>
```

Default Value:

No permissions are defined by default.

References:

1. JUNOS Login Classes Overview, JUNOS 9.5 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/frameset.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 7.1.2.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

16 Account Monitoring and Control
Account Monitoring and Control

6.6.5 Ensure all Custom Login Classes Forbid Shell Access (Automated)

Profile Applicability:

- Level 1

Description:

All login classes should deny Shell access.

Rationale:

JUNOS runs on top of a heavily modified BSD Unix based operating system and users with certain permission sets will be able to start a Shell to interact with this underlying system directly. Once within a Unix Shell a user may execute scripts or applications and perform changes outside of the normal Authentication, Authorization and Accounting (AAA) mechanisms which protect the router when a user performs commands in JUNOS.

Access to the underlying Unix Shell is not required in normal operation for almost all deployments and the default position should be for this to be denied.

In the rare instances where it is required, access to the Shell should be restricted to a very small number of users, ideally only being granted on a case by case basis and removed when the task requiring access is complete.

To ensure all interaction with the router will need to be performed through JUNOS, all Custom Login Classes should have access to the shell explicitly denied.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login | match "deny-commands.*start shell.*" | count
```

The above command should return a positive integer equal to the number of configured classes.

Remediation:

Deny Shell access for a class using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set class <class name> deny-commands "start shell"
```

You may also wish to deny other commands or groups of commands by using a list or Regular Expression as the deny-commands value, ensure that start shell is still included.

Default Value:

Shell access is not restricted by default.

References:

1. JUNOS Login Classes Overview, JUNOS 9.5 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/frameset.html)

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

16 Account Monitoring and Control
Account Monitoring and Control

6.6.6 Ensure Predefined Login Classes are not used (Automated)

Profile Applicability:

- Level 1

Description:

All user accounts must have a class set, but the Predefined JUNOS Login Classes should be avoided.

Rationale:

JUNOS routers ship with 4 Predefined Login Classes, these are:

- super-user
- read-only
- operator
- unauthorized

These classes provide basic configuration to allow organizations to get a router up and running, but do not provide fine grained control needed by all but very smallest organizations.

The built in classes also do not meet the other recommendations in this section. For example, the *super-user* class (which is the only built in class with read/write permissions) also has permission to start a Unix Shell and does not have an Idle Session Timeout.

Because of these limitations it is recommended that Custom Login Classes be defined following the principle of *least privilege*, where each class of users is granted *only* those permissions needed to complete their job role.

All of these class should meet the other requirements in this section and no users (either local or remote template users) should use the built-in accounts.

Impact:

Careful configuration of permissions following the least privilege principle is essential for secure and reliable management of the network.

For larger networks, creating and maintaining Login Classes on each individual device may become cumbersome and error prone - for these environments it is suggested you consider the Level 2 Recommendation "Ensure Remote Login Class for Authorization through External AAA".

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login | find "user .* {" | match "class" | match
"superuser|super-user|read-only|operator|unauthorized" | count
```

The above command should return zero where no Emergency Access Account has been configured or 1 where an Emergency Access Account is used.

Remediation:

To create a new class you can issue the following commands from the `[edit system login]` hierarchy. In this example, we create a new class named 'noc' and allow them permissions to run show commands like `show bgp summary`, view the configuration and access the network with ping, SSH, traceroute and Telnet.

```
[edit system login]
user@host#set class noc permissions [ view view-configuration network ]
```

(this class should also have Idle timeouts and other options set in line with other recommendations in this section).
To change the class for a user account, use the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set user <username> class <class name>
```

Default Value:

By default all users are, in effect, members of the super-user class.

References:

1. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/user-access.html
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 7.1.

Additional Information:

It is generally recommended that a local "Emergency Access" account with a locally configured login be maintained on the device. In normal operation, with External AAA working and available, this account should not be accessible due to the authentication-order (see section 6.3 Authentication-Order). It is common practice for this account to be placed in the Super-user class, as externally defined classes will not be possible when this account is used.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.7 Ensure Remote Login Class for Authorization through External AAA (Automated)

Profile Applicability:

- Level 2

Description:

External AAA servers should be utilized to provide Authorization via a single "Remote" template account.

Rationale:

JUNOS routers ship with 4 Predefined Login Classes for user Authorization, these are:

- super-user
- read-only
- operator
- unauthorized

These classes provide basic Authorization, restricting what users in each class can or cannot do, to allow organizations to get a router up and running, but do not provide fine grained control needed by all but very smallest organizations.

The built in classes also do not meet the other recommendations in this section. For example, the *super-user* class (which is the only built in class with read/write permissions) also has permission to start a Unix Shell and does not have an Idle Session Timeout.

Because of these limitations it is recommended that Custom Login Classes be defined following the principle of *least privilege*, where each class of users is granted *only* those permissions needed to complete their job role.

However, defining and maintaining Custom Login Classes locally on each router, switch, firewall or other network device can quickly become difficult and error prone in a larger environment.

For larger networks JUNOS provides for extremely fine grained access control rules to be defined on an External AAA server running either RADIUS or TACACS+ through the use of *Vendor Specific Attributes* which map to the same permissions that can be set locally for a class.

Vendor Specific Attributes (or VSAs) are standards based extensions to the RADIUS and TACACS+ protocols and are supported on most implementations by defining an appropriate dictionary.

When performing Authorization using External RADIUS or TACACS+ services, it is recommended that a single "remote" user is configured on the device and mapped to a "remote" class with minimal permissions set. The user should be named "remote" where possible, as this name is reserved by JUNOS as the account to which users are mapped when authenticated through External AAA and for whom the Juniper-Local-User-Name VSA is not set.

When a user is authenticated by RADIUS or TACACS+ the server can return a number of VSAs including:

- *Juniper-Local-User-Name* - Maps the user to a local user "template account", if this is not specified the single "remote" user account is used.
- *Juniper-User-Permissions* - Allows the server to set the same permissions as would be set in a login class locally. These permission are added to those of the remote user's configured class.
- *Juniper-Allow-Commands* - Uses an Extended Regular Expression to *grant* Operational Mode commands in addition to those allowed by the user's class.
- *Juniper-Deny-Commands* - Uses an Extended Regular Expression to *deny* Operational Mode commands which would otherwise be allowed by the user's class.
- *Juniper-Allow-Configuration* - As with the Allow Commands, but to grant Configuration Mode commands not normally allowed by the user's class.
- *Juniper-Deny-Configuration* - As with Deny Commands, but to deny Configuration Mode commands which would otherwise be allowed by the user's class.

NOTE - This is not a complete list of all attributes and uses the RADIUS VSA naming convention. Equivalent TACACS+ VSAs match the above but with slightly different naming.

By combining the use of the above VSAs from either a RADIUS or TACACS+ server, it is possible to define granular access control equivalent to that which can be set using locally configured Login Classes, but without the need to configure and maintain consistent, granular AAA policy across all devices.

Where devices are primarily managed via Software Defined Networking or other centralized management and/or automation platforms rather than through the CLI or other local interfaces, then this may be sufficient to meet requirements for centralized AAA and/or allow for effective management of local template accounts without using external AAA.

Impact:

Careful configuration of permissions following the least privilege principle is essential for secure and reliable management of the network.

When configuring remote AAA, it is recommended that a local Emergency Access Account also be configured to allow management of the device in the event that AAA services are unavailable.

Audit:

From the command prompt, execute the following commands:
Firstly, confirm that no users (apart from any Emergency Access Account) use any of the predefined login classes.

```
[edit]
user@host#show system login | find "user .* {" | match "class" | match
"superuser|super-user|read-only|operator|unauthorized" | count
```

The above command should return zero where no Emergency Access Account has been configured or 1 where an Emergency Access Account is used.
Then confirm that the `remote` user account is defined:

```
[edit]
user@host#show system login user remote
```

The above command should return the configured class, UID and other options for the remote user.

Remediation:

To create a new class you can issue the following commands from the `[edit system login]` hierarchy. In this example, we create a new class named 'remote', granting only `view` permissions, and assign the `remote` user to the new class. More detailed permissions will be added to these permissions

```
[edit system login]
user@host#set class remote permissions [ view ]
```

(this class should also have Idle timeouts and other options set in line with other recommendations in this section).
To change the class for a user account, use the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set user remote class remote
```

A full discussion of RADIUS or TACACS+ configuration and options is beyond the scope of this guide, but a simple example of using a TACACS.net server running on Windows with AD integration for a `remote` user is shown below.

This example is taken from an anonymized real world deployment, so also includes sections to allow access to different groups of TACACS+ Clients and permissions for Cisco IOS and Netscreen devices. The most relevant section is the `<Service>` for `service=junos-exec`, where the VSAs for TACACS+ Clients running JUNOS are defined, but the entire Authorization for this Class is given for context.

```
<Authorization>
<!--CIS Example remote user Authorization from TACACS.net Authorization.xml--
>
        <UserGroups>
        <!-- The UserGroup is defined elsewhere - in this case it maps to an
Active Directory Group call GRP-NETOPS -->
                <UserGroup>GRP-NETOPS</UserGroup>
        </UserGroups>
        <ClientGroups>
        <!--Defines the Groups of devices this usergroup can login to -->
                <ClientGroup>CORE-NET</ClientGroup>
                <ClientGroup>ACCESS-NET</ClientGroup>
                <ClientGroup>FIREWALLS</ClientGroup>
        </ClientGroups>
        <Shell>
        <!--note that the login and exit commands are always permitted.  (used
for Cisco and Netscreen devices) -->
                <Permit>show.*</Permit>
                <Permit>terminal.*</Permit>
                <Permit>get.*</Permit>
                <Deny>.*</Deny>
        </Shell>
        <Services>
                <Service>
                <!-- JUNOS VSAs to set additional user permissions -->
                        <Set>service=junos-exec</Set>
                        <Set>local-user-name=remote</Set> <!--This will be
mapped to a template user on JUNOS devices with "remote" class permissions --
>
                        <Set>allow-commands=show.*</Set> <!-- Additional
permission (above remote class set above) to allow all "show" operational
commands -->
                        <Set>user-permissions=view-configuration</Set> <!--
Grants additional permission to view the full config (no secrets)-->
                        <Set>user-permissions=network</Set> <!-- Grants access
to the network for SSH, Ping, etc -->
                </Service>
        </Services>
        <AutoExec>
        <!--Set the Priv lvl to 15 for Cisco devices, ignored by JUNOS
devices -->
                <Set>priv-lvl=15</Set>
        </AutoExec>
</Authorization>
```

Default Value:

By default all users are, in effect, members of the super-user class.

References:

1. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/user-access.html
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 7.1.
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/general/tacacs-vendor-specific-attributes-juniper-networks.html
4. https://www.juniper.net/documentation/en_US/junos/topics/reference/general/radius-vendor-specific-attributes-juniper-networks.html

Additional Information:

There are a few exceptions which should be considered:

1 - It is generally recommended that a local "Emergency Access" account with a locally configured login be maintained on the device. In normal operation, with External AAA working and available, this account should not be accessible due to the authentication-order (see section 6.3 Authentication-Order). It is common practice for this account to be placed in the Super-user class, as externally defined classes will not be possible when this account is used.

2 - Where an account does require Shell access with `su` privileges and membership of the Unix Wheel group, a locally defined user or template *must* be used in order for these permissions to be granted via the `Maintenance` or `all` permissions attributes. While these permissions can be set for remote users via VSAs, the underlying Unix OS changes can only be made for locally configured users. One example where this may be needed is when configuring the user account for the JUNOS Puppet agent, which operates at the Unix Shell rather than at the JUNOS level.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.6.8 Ensure login message is set (Automated)

Profile Applicability:

- Level 1

Description:

A login message should be displayed before a user logs into the router.

Rationale:

Prior to a user logging into the router a legal notice should be displayed warning that they are connecting to a private system.

This legal notice may be necessary to protect your organizations rights to pursue legal action or to monitor users of the system. It might, in general:

- Warn that this is a private system
- Tell unauthorized users that they should disconnect immediately
- Inform users that activity is monitored/recorded and may be shared with 3rd parties or used in a criminal investigation
- May reference applicable legislation
- May specify that continuing to login constitutes agreement to an Acceptable Use policy or similar
- May provide contact details for any queries

NOTE *The wording of the legal notice is normally defined as part of an organization's security policy. You should consult your organizations legal department or counsel to ensure the legality of the banner message and suitability for the country/s in which you operate.*

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login message
```

The above command should return the following output:

```
message "<LEGAL NOTICE>";
```

Remediation:

Configure a login message using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login message "<LEGAL NOTICE>"
```

Default Value:

By default no login message is set.

References:

1. Configuring a System Login Message, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (https://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-a-system-login-message.html#id-10963857)
2. Router Security Configuration Guide, Version 1.1b, Page 171, National Security Agency (NSA)

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.6.9 Ensure local passwords require multiple character sets (Automated)

Profile Applicability:

- Level 1

Description:

Passwords for local user accounts must be configured to require character set changes.

Rationale:

Weak passwords on local user accounts present a serious threat to the security of any device, allowing malicious user access through simple dictionary or brute force attacks.

Fortunately JUNOS provides a mechanism for enforcing complexity requirements when new passwords are initially set in plain-text.

Secure passwords should contain characters from number of different character sets (Upper case letters, Lower case letters, Numbers, Punctuation and Special Characters) and JUNOS should be configured to force passwords for local users to meet this requirement.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login password change-type
```

The above command should return the following output:

```
change-type character-sets;
```

Remediation:

Configure a password character set changes using the following command under the `[edit system]` hierarchy:

```
[edit system]
user@host#set login password change-type character-set
```

Default Value:

For routers running JUNOS the default is change-type is character-set. For routers running JUNOS FIPS the default is set-transitions.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA) Payment Card Industry Data Security Standard (PCI DSS), Version 1.2, Requirement 8.5.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.6.10 Ensure at least 4 set changes in local passwords (Automated)

Profile Applicability:

- Level 1

Description:

Passwords for local user accounts must be configured to require at least 4 character set changes.

Rationale:

Weak passwords on local user accounts present a serious threat to the security of any device, allowing malicious user access through simple dictionary or brute force attacks.

Fortunately JUNOS provides a mechanism for enforcing complexity requirements when new passwords are initially set in plain-text.

Secure passwords should contain characters from at least 4 different character sets (Upper case letters, Lower case letters, Numbers, Punctuation and Special Characters) and JUNOS should be configured to force users' passwords to meet this requirement.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login passwords minimum-changes
```

The above command should return the following output:

```
login password minimum-changes 4;
```

A value greater than 4 is also acceptable.

Remediation:

Configure the minimum character set changes using the following command under the [edit system] hierarchy:

```
[edit system]
user@host#set login passwords minimum-changes 4
```

Default Value:

For routers running JUNOS the default is minimum changes is 1. For routers running JUNOS FIPS the default is 3.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.1.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.6.11 Ensure local passwords are at least 10 characters (Automated)

Profile Applicability:

- Level 1

Description:

Passwords for local user accounts must be configured to require at least 10 characters.

Rationale:

Weak passwords on local user accounts present a serious threat to the security of the device, allowing malicious user access through simple dictionary or brute force attacks.

Fortunately JUNOS provides a mechanism for enforcing complexity requirements when new passwords are initially set in plain-text.

Secure passwords should be required to contain at least 10 characters in line with the minimum enforced by JUNOS FIPS compliant versions.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login password minimum-length
```

The above command should return the following output:

```
minimum-length <n>;
```

Where is a number equal to or greater than 10.

Remediation:

Configure the minimum characters for passwords using the following command under the [edit system] hierarchy:

```
[edit system]
user@host#set login passwords minimum-length 8
```

Default Value:

For routers running JUNOS the default minimum-length is 6. For routers running JUNOS FIPS the default is 10.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.1.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.6.12 Ensure SHA512 is used to hash local passwords (Automated)

Profile Applicability:

- Level 1

Description:

Passwords should be hashed with a strong hashing algorithm.

Rationale:

Passwords for locally configured users are stored in the JUNOS configuration file.

By applying a hashing algorithm to the password before storing it, JUNOS limits an attacker's ability to gain passwords from configuration backups or to escalate privileges when using a different account through the CLI.

JUNOS hashes local passwords using MD5, or SHA1 for FIPS mode devices, by default. However, both are older algorithms and are widely considered to be weak for this type of usage.

The newer SHA-2 algorithm should be used with a 512bit digest wherever possible, however, some older but still supported JUNOS devices do not support this (see notes for more details).

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system login password format
```

The above command should return the following output:

```
login password format sha512;
```

Remediation:

Confirm that your device supports SHA-2 with 512bit hashes by issuing the following command from the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set password format ?
```

The system should provide a range of options, such as in the example below which is for a system which does support SHA512:

```
[edit system login]
user@host# set password format ?
Possible completions:
  md5                  Message Digest 5
  sha1                 Secure Hash Algorithm 1
  sha256               Secure Hash Algorithm 256 ($5$)
  sha512               Secure Hash Algorithm 512 ($6$)
[edit system login]
```

Configure password hashing using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set login password format sha512
```

For systems which *do not* support SHA-2 with 512bit hashes, configure SHA-1 using the following command under the `[edit system login]` hierarchy:

```
[edit system login]
user@host#set login password format sha1
```

NOTE - *SHA1 hashing should only be configured on systems which do not support SHA512.*

Default Value:

For routers running JUNOS the default format is MD5. For routers running JUNOS FIPS the default is SHA1.

Additional Information:

Some currently supported platforms running the JTAC recommended release, such as some older SRX Branch devices (SRX100, 200, etc), do not support the SHA256 or SHA512 options.

If your JUNOS device does not support SHA512 or SHA256, the older SHA1 format should be used *as a minimum*.

For organizations with particular security concerns or where SHA1 does not meet regulatory/company policy requirements; it is recommended that you consider replacing these devices with newer equivalents which do support the stronger hashing algorithms, for example replacing an SRX200 with an SRX300 model.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.6.13 Ensure SSH Key Authentication is not set for User Logins (Automated)

Profile Applicability:

- Level 1

Description:

SSH Key Based Authentication should not be used for User Logins

Rationale:

Due to the sensitive nature of SSH, potentially allowing full management of the targeted device, protecting SSH access using strong authentication methods is essential to the security of the device.

One method which is supported in SSH for stronger authentication is the use of Public/Private Encryption Key Pairs in place of a more traditional login prompt for a Username and Password. Instead, an administrator uploads the user's *Public key* to the JUNOS (or other) device to be managed.

When the user connects, they will use their *Private key* to encrypt some session specific data. The JUNOS device can verify the Users identity by decrypting that data using the *Public key* configured previously and comparing it to an expected result. If the results match, then the user must have access to the Private key, so is considered valid.

Unfortunately using SSH Keys to authenticate User Logins to JUNOS devices introduce a number of security issues:

- Public Keys may only be configured locally on each JUNOS device
- Public Keys are used *instead of* centralized AAA using TACACS+ or RADIUS as covered in Recommendation 6.8.1 Ensure External AAA Server is set
- The use of SSH Keys means only a single Authentication Factor (the keys) can be used, preventing the use of Multi Factor Authentication as covered in 6.6.14 Ensure Multi-Factor is used with External AAA
- JUNOS does not provide any method to automate rollover or locking of keys. If keys are compromised/lost, they must be changed on every JUNOS device on which they are configured.
- Some SSH implementation support the use of X.509 PKI Certificates for managing SSH Keys, but JUNOS does not.

Because of these limitations and the difficulty in auditing and managing SSH Keys on JUNOS devices, this method should not be used for Authentication of User logins or for the Root User.

In some instances, such as when using PyEZ or NETCONF based automation over SSH, it may be preferable to authenticate a limited number of automation services using SSH Keys, rather than "hard coding" user details into scripts. Where this is the case, it is imperative to have strong key management procedures in use to control and audit access to the Private Keys used and a process to allow for rollover and revocation of compromised keys.

Impact:

Careful configuration of permissions following the least privilege principle is essential for secure and reliable management of the network.

When configuring remote AAA, it is recommended that a local Emergency Access Account also be configured to allow management of the device in the event that AAA services are unavailable.

Audit:

To confirm whether any logins have been configured to use SSH Key based Authentication, issue the following command from the `[edit system login]` hierarchy:

```
[edit system login]
user@host# show | display set | match "user.*authentication" | match "ssh-
dsa|ssh-ecdsa|ssh-ed25519|ssh-rsa" | count
```

The above command should return a count of 0 lines.
If SSH Key based Authentication is being used for automation (eg. with PyEZ) the specific user accounts used for the automation service can be excluded from the previous command as follows:

```
[edit system login]
user@host# show | display set | match "user.*authentication" | match "ssh-
dsa|ssh-ecdsa|ssh-ed25519|ssh-rsa" | exclude "pyez-user|netconf-user" | count
```

In the example above the users to be excluded were `pyez-user` and `netconf-user`. With logins used for automation excluded, the above command should return a count of 0 lines.

Remediation:

For each User Login configured with SSH Key based Authentication, you can delete the SSH Key with the following command from the `[edit system login]` hierarchy:

```
[edit system login]
user@host# delete user <User ID> authentication
```

The user can then be configured with a password locally or, inline with Recommendation 6.8.1 Ensure External AAA Server is set , leave the authentication method blank and allow the External AAA to control Authentication.
Alternatively, you may wish to delete the local user account entirely using the following command:

```
[edit system login]
user@host# delete user <User ID>
```

Default Value:

By default, JUNOS does not use SSH Key based Authentication

References:

1. https://kb.juniper.net/InfoCenter/index?page=content&id=KB30588
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/ssh-rsa-edit-system-root-authentication-qfx-series.html
3. https://www.ssh.com/ssh/key/

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.6.14 Ensure Multi-Factor is used with External AAA (Manual)

Profile Applicability:

- Level 2

Description:

Multi-factor Authentication should be used for management sessions

Rationale:

Even with the password complexity restrictions and use of External AAA servers for centralized control of user Authentication, login with usernames and passwords is commonly exploited through Phishing, Brute Force or other methods.

Multi-Factor Authentication (sometimes called Two-Factor Authentication or 2FA) provides a significant additional layer of security for management sessions by requiring a username, password *and* some further method/s to all be provided to login.

The additional factor may use an X.509 "SSL" Certificate, a Time Based One Time Password (TOTP), a physical security token, a Fingerprint or may use some other method or even combination of these methods.

In all the cases above, the additional factor provides a significant additional challenge to an attacker looking to successfully pose as the user and compromise the network.

Multi-Factor authentication is widely supported by most External AAA services, either using paid for services like RSA SecureID or free platforms like Google Authenticator, so is included here as a general recommendation relating to AAA and login. However, because the Multi-Factor Authentication is implemented on the AAA Server, it is not possible to include an audit action or include this as a scored recommendation.

Impact:

As with any AAA service, Multi-Factor Authentication should be carefully tested and you should ensure you maintain a local password as a backup method to ensure you are not locked out of your network while implementing such a service.

Audit:

Remediation:

Default Value:

No External AAA or Multi-Factor Authentication is used by default.

References:

1. https://en.wikipedia.org/wiki/Multi-factor_authentication
2. http://tacacs.net/mfa.asp
3. https://www.rsa.com/en-us/products/rsa-securid-suite
4. https://wiki.freeradius.org/guide/2FA-Active-Directory-plus-Proxy
5. http://www.greenrocketsecurity.com/greenradius/2fa/

Additional Information:

While SMS One Time Passwords is a valid Multi-Factor Authentication method and easily/cheaply implemented, the susceptibility of SMS to interception makes this one of the least strong methods and other factors should be employed where ever possible.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

6.7 NTP

Network Time Protocol (NTP) allows administrators to centrally manage and synchronise the system time on all of their network, server and host devices; ensuring a consistent time stamp for logging and authentication protocols.

NTP is an internet standard, originally defined in RFC1305 (and updated in RFC5905 for NTP Version 4).

Juniper devices can be configured to act as an NTP Client or NTP Server under the `[edit system ntp]` hierarchy.

Keeping time settings consistent across a network is vital if log data is to be meaningful and usable in understanding faults and security incidents. Consistent time settings are also fundamental to the operation of many network protocols and services such as IPSec, PKI and 802.1x which may be critical to many networks.

While a complete discussion of NTP Architecture is beyond the scope of this Benchmark, it is **strongly recommended** that careful attention be paid to resilience, accuracy and reliability of NTP time sources used within your network.

IETF BCP 13 (Best Common Practice), suggests that *"Operators who are concerned with maintaining accurate time SHOULD use at least 4 independent, diverse sources of time. Four sources will provide sufficient backup in case one source goes down. If four sources are not available, operators MAY use fewer sources, subject to the risks outlined above."*

Options for NTP time sources may include *Public NTP Servers*, such as those provided by pool.ntp.org, *Shared NTP Servers*, such as those provided by many Internet Exchanges for use by members, or *Private NTP Servers* operated by your organisation for your own exclusive use and synchronised using MSF Radio, GPS or internal Crystal/Atomic Clocks.

The recommendations given in BCP13 may not be applicable in all cases and often just 2 or 3 sources may be appropriate, particularly where Private NTP sources are utilised. Alternatively, in highly secure environments 5, 7 or even more NTP time sources may be required in order to protect against one ore more sources being compromised by an attacker.

6.7.1 Ensure External NTP Servers are set (Automated)

Profile Applicability:

- Level 1

Description:

At least one, and preferably three or more, external NTP Servers should be configured

Rationale:

Keeping time settings consistent across a network is vital if log data is to be meaningful and usable in understanding faults and security incidents. Consistent time settings are also fundamental to the operation of some network protocols and services such as IPSec, PKI and 802.1x which may be critical to many networks.

To ensure that the time on your JUNOS router is consistent with other devices in your network, at least one, and preferably three or more, NTP Servers external to the device should be configured.

Although NTP provides for a Peer to Peer type implementation, where individual time servers are not specified and methods such as broadcast and multicast are utilized to synchronize time between hosts, in almost all real world cases a Server / Client model should be used for network devices - even if multicast or broadcast methods are used for other types of hosts. Using specified time sources allows you to better secure, monitor and manage your NTP implementation; simplifying debugging and allowing tighter control of NTP traffic.

While a complete discussion of NTP Architecture is beyond the scope of this Benchmark, it is **strongly recommended** that careful attention be paid to resilience, accuracy and reliability of NTP time sources used within your network.

Having multiple NTP servers helps to ensure fault tolerance and also protects against mis-configured or compromised servers causing radical time changes, something an attacker may want to achieve to cover their tracks or conduct replay attacks.

Impact:

If time is not synchronised between devices, log messages cannot readily be correlated to allow administrators to understand events on the network. In addition, many services such as IPSEC, PKI or 802.1x which rely on Encryption may not function correctly if time and date settings are not properly maintained.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system ntp | match server | except boot-server | count
```

The above command should return an integer value greater than or equal to 1 if NTP servers are explicitly configured.

Remediation:

Configure at least one External NTP Server using the following commands under the [edit system] hierarchy;

```
[edit system]
user@host#set ntp server <Servers IP>
```

Default Value:

By default Juniper routers do not have NTP servers configured and use locally managed time.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. https://www.giac.org/paper/gsec/2115/ntp-security/103613
4. [IETF BCP 13](https://tools.ietf.org/id/draft-ietf-ntp-bcp-13.html)
5. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.7.2 Ensure Multiple External NTP Servers are set (Automated)

Profile Applicability:

- Level 2

Description:

At least 3 External NTP Servers should be set

Rationale:

Keeping time settings consistent across a network is vital if log data is to be meaningful and usable in understanding faults and security incidents. Consistent time settings are also fundamental to the operation of some network protocols and services such as IPSec, PKI and 802.1x which may be critical to many networks.

In sensitive environments, to ensure that the time on your JUNOS devices is consistent with other devices in your network, at least three NTP Servers external to the device should be configured.

Although NTP provides for a Peer to Peer type implementation, where individual time servers are not specified and methods such as broadcast and multicast are utilized to synchronize time between hosts, in almost all real world cases a Server / Client model should be used for network devices - even if multicast or broadcast methods are used for other types of hosts. Using specified time sources allows you to better secure, monitor and manage your NTP implementation; simplifying debugging and allowing tighter control of NTP traffic.

IETF BCP 13 (Best Common Practice), suggests that "Operators who are concerned with maintaining accurate time SHOULD use at least 4 independent, diverse sources of time. Four sources will provide sufficient backup in case one source goes down. If four sources are not available, operators MAY use fewer sources, subject to the risks outlined above."

Options for NTP time sources may include *Public NTP Servers*, such as those provided by pool.ntp.org, *Shared NTP Servers*, such as those provided by many Internet Exchanges for use by members, or *Private NTP Servers* operated by your organisation for your own exclusive use and synchronised using MSF Radio, GPS or internal Crystal/Atomic Clocks.

It is **Strongly Recommended** that administrators of devices requiring Level 2 compliance consider the use of Private NTP Servers for some or all of the time sources within the NTP Architecture.

Using multiple NTP Servers, not only provides for a more reliable service, but also protects against "Falsetickers" (compromised or untrustworthy time sources providing incorrect time). This is based on the rule of needing 2*n*+1 True clocks, where *n* is the number of true clocks.

So protection against 1 falseticker requires 4 upstream servers, against 2 falsetickers 5 upstream and 7 are needed to protect against 3 compromised sources. See SelectingOffsiteNTPServers at NTP.org for a more detailed discussion.

Impact:

If time is not synchronised between devices, log messages cannot readily be correlated to allow administrators to understand events on the network. In addition, many services such as IPSEC, PKI or 802.1x which rely on Encryption may not function correctly if time and date settings are not properly maintained.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system ntp | match server | except boot-server | count
```

The above command should return an integer value greater than or equal to 3 if sufficient NTP servers are explicitly configured.

Remediation:

Configure at least 3 External NTP Servers using the following commands under the [edit system] hierarchy;

```
[edit system]
user@host#set ntp server <Servers IP>
```

Default Value:

By default Juniper routers do not have NTP servers configured and use locally managed time.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)

2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. [IETF BCP 13](https://tools.ietf.org/id/draft-ietf-ntp-bcp-13.html)
4. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)
5. [Selecting Offsite NTP Servers](https://support.ntp.org/bin/view/Support/SelectingOffsiteNTPServers)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment
Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.7.3 Ensure NTP Boot-Server is set (Automated)

Profile Applicability:

- Level 2

Description:

An NTP Boot-Server should be configured for the router to update its time on boot.

Rationale:

When the router boots or when a new Routing Engine is installed its time may have drifted or be set beyond the maximum amount where periodic updates can return it to the correct time, resulting in the correct time never being set.

To prevent this situation; a Boot Server should be set from which the JUNOS device will obtain its time as it loads.

Because the `ntpdate` utility, which contacts the Boot Server, runs prior to many of the other core demons, such as `rpd`, the Boot Server should be reachable from the device's management interface (`fxp0` on most routers, 'em0' or 'me0' on some other platforms) without any Routing Protocol learned routes or Tunnels being available.

For this reason, the Boot Server may often be a different NTP server to that used during normal operation, potentially just being the management interface of another router in the same management subnet.

A Boot Server should be specified wherever possible, however, reachability of an NTP Server or another network device through Out of Band Management is not possible in all deployment scenarios; therefore this Recommendation is given at Level 2 as additional equipment or cost may be required for implementation.

Impact:

If time is not synchronised between devices, log messages cannot readily be correlated to allow administrators to understand events on the network. In addition, many services such as IPSEC, PKI or 802.1x which rely on Encryption may not function correctly if time and date settings are not properly maintained.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system ntp | match boot-server
```

The above command should return a configured Boot-Server IP Address or Hostname which should be resolvable and reachable through the Out of Band Management port at device bootup.

Remediation:

To configure an NTP Boot Server, enter the following command from the `[edit system ntp]` hierarchy;

```
[edit system ntp]
user@host#set ntp boot-server <Server IP or Hostname>
```

Default Value:

By default Juniper routers do not have NTP servers configured and use locally managed time.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. https://www.giac.org/paper/gsec/2115/ntp-security/103613
4. [IETF BCP 13](https://tools.ietf.org/id/draft-ietf-ntp-bcp-13.html)
5. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.7.4 Ensure NTP uses version 4 (Automated)

Profile Applicability:

- Level 1

Description:

Version 4 of the NTP protocol should be utilized.

Rationale:

NTP is one of the oldest Internet Standard protocols and has been around for over 30 years. As with most protocols, during its lifetime, NTP has received numerous revisions and updates to ensure it remains reliable and secure to use in modern networks.

The current reference version of NTP is Version 4. Version 4 adds significant enhancements to the protocols security which means it is widely accepted as the defacto standard for secure implementation and should be used for all network devices.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system ntp | match server | match "version [1-3]" | count
```

The above command should return null or 0.

Remediation:

Configure each External NTP Server to use NTP Version 4 using the following commands under the [edit system ntp] hierarchy:

```
[edit system ntp]
user@host#set server <Servers IP>  version 4
```

Default Value:

By default all Juniper routers use NTP Version 4 when a server is explicitly configured.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)

2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. [IETF BCP 13](https://tools.ietf.org/id/draft-ietf-ntp-bcp-13.html)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment
Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.7.5 Ensure Authentication Keys are used for all NTP Servers (Automated)

Profile Applicability:

- Level 2

Description:

Authentication keys should be set for NTP Servers

Rationale:

Having established the need for NTP, it is essential to ensure that the devices time is not manipulated by an attacker as this could allow DoS to services relying on accurate time as well as replay attacks and other malicious activity.

NTP Version 3 introduced Authentication mechanisms for NTP messages using a Keyed Hash based Message Authentication Check (HMAC), where a hash of the message ensures both that the message is authentic and that it was not changed in transit. All JUNOS platforms support HMAC with NTP Versions 3 and 4 using MD5 and some platforms also support the more robust SHA1 and SHA2-256 algorithms.

It is strongly recommended that, as the MD5 and SHA1 algorithms are now considered deprecated, SHA2-256 based keys be used. In addition, to prevent compromise of one server leaking the keys for all NTP Servers, a different key should be used for each server. The use of SHA-256 and different keys per server are covered in separate Recommendations and not tested as part of the Audit Procedure for this Recommendation.

NOTE - Both the keys and the algorithm must match on all NTP peers being configured.

Impact:

If keys or algorithms do not match on NTP Servers and Client devices NTP will not be able to update and this could impact Logging, Authentication, Encryption/VPN or other services which rely on consistent time.

Audit:

From the command prompt, execute the following commands:

```
[edit]
user@host#show system ntp | match server | match key | count
```

The above command should return an integer value greater than or equal to 1 if any NTP servers are configured with encryption keys. This value should be the same as the total number of servers configured as tested in Recommendation 6.7.2 Ensure Multiple External NTP Servers are set

Remediation:

Keys are configured on a key ring and identified by an ID number. To add a key enter the following command from the `[edit system ntp]` hierarchy;

```
[edit system ntp]
user@host#set authentication-key <Key ID> type <algorithm> value <Key>
```

The <Key ID> is an arbitrary 32-bit non-zero integer used to identify this key locally on the device. The may be set to MD5 (the default), SHA1 or SHA2-256 (with SHA1 and SHA2 only being supported on some devices).
Next, for each server, configure the key to be used:

```
[edit system ntp]
user@host#set server key <Key ID>
```

Finally configure the key as trusted so that the router will accept NTP traffic encrypted using it. This mechanism provides an easy method to retire keys in the event of compromise. Enter following command from the `[edit system ntp]` hierarchy;

```
[edit system ntp]
user@host#set trusted-key <Key ID>
```

The <Key ID> which is trusted can be one key or several keys by enclosing the list in square brackets or repeating the command.

Default Value:

By default Juniper routers do not have NTP servers configured and use locally managed time.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. https://www.giac.org/paper/gsec/2115/ntp-security/103613

4. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.7.6 Ensure Different Authentication Keys for each NTP Server (Automated)

Profile Applicability:

- Level 2

Description:

Different authentication keys should be set for each NTP Server

Rationale:

Having established the need for NTP, it is essential to ensure that the devices time is not manipulated by an attacker as this could allow DoS to services relying on accurate time as well as replay attacks and other malicious activity.

NTP Version 3 introduced Authentication mechanisms for NTP messages using a Keyed Hash based Message Authentication Check (HMAC), where a hash of the message ensures both that the message is authentic and that it was not changed in transit. All JUNOS platforms support HMAC with NTP Versions 3 and 4 using MD5 and some platforms also support the more robust SHA1 and SHA2-256 algorithms.

In high security environments, prevent the compromise of a single server or key undermining your entire NTP infrastructure by using different keys for each NTP Server configured.

This is significant additional configuration, but does increase the difficulty for an attacker who would now need to compromise multiple keys or servers and also allows any compromise to be quickly responded to, with the affected server immediately removed from production and re-keyed while the network continues to use the remaining server/s.

NOTE - Both the keys and the algorithm must match on all NTP peers being configured.

Impact:

If keys or algorithms do not match on NTP Servers and Client devices NTP will not be able to update and this could impact Logging, Authentication, Encryption/VPN or other services which rely on consistent time.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system ntp | match "server|key"
```

The above command should return each of the configured NTP Servers for the JUNOS Device, as well as configured and trusted keys.
The following conditions *must all* be met:

- Every server has a 'key ' configured
- Each server uses a different ''
- A corresponding 'authentication-key' is configured for each 'key '
- Each 'authentication-key' used with a server is included in the 'trusted-key' list

Remediation:

Keys are configured on a key ring and identified by an ID number. To add a key enter the following commands from the `[edit system ntp]` hierarchy:

```
[edit system ntp]
user@host#set authentication-key <Key ID> type <algorithm> value <Key>
user@host#set trusted-key <Key ID>
```

Set the keys for all configured NTP servers using the following commands under the `[edit system ntp]` hierarchy:

```
[edit system ntp]
user@host#set server <Servers IP> key <key ID>
```

If this device is operating as an NTP Server and has clients which use different keys or algorithms, these can be set with the `peer` option:

```
[edit system ntp]
user@host#set peer <Peers IP> key <key ID>
```

NOTE - The Key ID must also be listed in the `trusted-key` list to be accepted.

Default Value:

By default Juniper routers do not have NTP servers configured and use locally managed time.

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. https://www.giac.org/paper/gsec/2115/ntp-security/103613
4. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.7.7 Ensure Strong Authentication Methods are used for NTP Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Strong authentication methods should be set for NTP Servers

Rationale:

Having established the need for NTP, it is essential to ensure that the devices time is not manipulated by an attacker as this could allow DoS to services relying on accurate time as well as replay attacks and other malicious activity.

NTP Version 3 introduced Authentication mechanisms for NTP messages using a Keyed Hash based Message Authentication Check (HMAC), where a hash of the message ensures both that the message is authentic and that it was not changed in transit. All JUNOS platforms support HMAC with NTP Versions 3 and 4 using MD5 and some platforms also support the more robust SHA1 and SHA2-256 algorithms.

Message Digest 5 (MD5) is an older hashing mechanism dating back to the early 90's. Since 2004 an increasing number of collision vulnerabilities have been shown in MD5 and the algorithm is no longer considered suitable for authentication and integrity protection of sensitive material or X.509 certificates.

While not supported across all devices, most JUNOS devices now support use of SHA1 and SHA2-256 HMAC for NTP message authentication. This feature is documented through Juniper Feature Explorer as *Enhancement to NTP authentication method* and is supported on most Junos devices from Junos OS 18.2R1 onward (though individual platform support varies).

Like MD5, SHA1 is now considered deprecated due to the risk of collisions. As a result, in high security environments it is recommended that SHA2-256 be used for authentication of all NTP Servers or Peers (where this Junos device itself is acting as an NTP Server).

NOTE - Both the keys and the algorithm must match on all NTP peers being configured.

Impact:

If keys or algorithms do not match on NTP Servers and Client devices NTP will not be able to update and this could impact Logging, Authentication, Encryption/VPN or other services which rely on consistent time.

Audit:

From the command prompt, execute the following commands from the `[edit system ntp]` hierarchy:

```
[edit system ntp]
user@host#show | match "authentication-key" | except "sha2" | count
```

The above command should return 0 if no keys are configured with algorithms *other than* SHA2-256.

Remediation:

Keys are configured on a key ring and identified by an ID number. To add a key enter the following command from the `[edit system ntp]` hierarchy;

```
[edit system ntp]
user@host#set authentication-key <Key ID> type <algorithm> value <Key>
```

<Key ID> is an arbitrary 32-bit non-zero integer used to identify this key locally on the device. The <algorithm> can be set to MD5 (the default), SHA1 or SHA256 (with SHA1 and SHA256 only being supported on some devices) - for Strong Authentication Methods you should use `sha256` *only*.
Configure the key as trusted so that the router will accept NTP traffic encrypted using it. This mechanism provides an easy method to retire keys in the event of compromise. Enter following command from the `[edit system ntp]` hierarchy;

```
[edit system ntp]
user@host#set trusted-key <Key ID>
```

The <Key ID> which is trusted can be one key or several keys by enclosing the list in square brackets or repeating the command.
Finally, update the keys for each NTP servers using the following command under the `[edit system ntp]` hierarchy:

```
[edit system ntp]
user@host#set server <Servers IP> key <key ID>
```

Default Value:

NTP is not configured by default

References:

1. [Juniper TechLibary, Time Management Administration Guide](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/time-management.html)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10.4
3. https://www.giac.org/paper/gsec/2115/ntp-security/103613
4. [Cisco, Network Time Protocol : Best Practices White Paper](https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html)
5. [Juniper Feature Explorer - Enhancement to NTP authentication method](https://apps.juniper.net/feature-explorer/feature-info.html?fKey=8439&fn=Enhancement%20to%20NTP%20authentication%20method)

Additional Information:

Some Juniper devices, such as the ACX Series, may synchronize directly with GPS using the GNSS Interface or other External Clock source using a BITS T1/E1 interface. In these cases the Router may be acting as a Stratum 1 NTP source for the network and may, or may not, also be configured to synchronize time from NTP Sources.

CIS Controls:

Version 6

11.4 Manage Network Devices Securely
Manage network devices using two-factor authentication and encrypted sessions.

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.8 Radius-server / Tacplus-server / Radius-options

Each user who will manage the device should have a unique username and password, which allows them to be identified for Authorization and Accounting purposes.

Centralized Authentication services such as RADIUS and TACACS+ provide essential mechanisms to protect network devices, tracking login attempts across devices and providing centralized lockout of compromised accounts or accounts belong to staff leaving the company - something which is extremely difficult in all but the smallest environments when user accounts are locally configured on each device.

All network devices should be configured with at least one External AAA service to securely manage access.

Juniper devices support multiple Authentication protocols - TACACS+ Servers are configured under `[edit system tacplus-server]`, while RADIUS servers can be configured under the `[edit system radius-server]` hierarchy, with global RADIUS options set under the `[edit system radius-options]` hierarchy.

Because these three configuration hierarchies are so closely related, they are grouped together in a single section for clarity.

6.8.1 Ensure External AAA Server is set (Automated)

Profile Applicability:

- Level 1

Description:

At least one external Authentication server should be configured.

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services.

Both protocols provide services to Authenticate users on routers, switches and other systems. Juniper devices support both RADIUS and TACACS+ Authentication and you should configure at least one External Authentication Server of either type as configured under `[edit system authentication-order]`.

For resilience it is generally recommended to configure multiple AAA Servers, which can be of the same type (both TACACS+ or both RADIUS) or can be mixed (one RADIUS and one TACACS+) as required so long as both are configured in `[edit system authentication-order]`.

The External AAA Servers used *must* support Multi-Factor/Two Factor Authentication (MFA/2FA) methods as discussed in Recommendation 6.6.14 Ensure Multi-Factor is used with External AAA.

The secure configuration of the External AAA Services for features such as account lockout, password aging, complexity or MFA support are beyond the scope of this Benchmark to test but are essential to the secure operation of your network environment.

Impact:

Ensure that External AAA Servers are tested prior to deploying in a live environment.

It is generally recommended to configure a single "Rescue" or "Emergency" account locally under the [edit system login] hierarchy to provide access in the event of a AAA failure or mis-configuration prior to deploying External AAA.

Audit:

From the command prompt, execute the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "radius-server|tacplus-server" | count
```

The above command should return a line count equal to or greater than 1 which will match the number of External AAA Servers configured.
NOTE - While not explicitly tested in this recommendation, the configured server type (RADIUS or TACPLUS) ***must*** *be included in the `[edit system authentication-order]` section to be used.*

Remediation:

Configure at least one External Authentication Server using the following commands under the `[edit system]` hierarchy; For RADIUS

```
[edit system]
user@host#set radius-server <server ip> secret <shared secret> source-address
<loopback IP>
```

For TACACS+

```
[edit system]
user@host#set tacplus-server <server ip> secret <shared secret> source-
address <loopback IP>
```

NOTE - the source-address is generally set as the Loopback, but for some environments the Fxp0.0/out of band interface may be used, or another interface preferred.

Default Value:

No External AAA is used by default

References:

1. Configuring RADIUS Authentication, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-radius-authentication.html#id-10624913)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirements 7.2 and 8

Additional Information:

In most environments the address assigned to either Lo0.0 or FXP0.0 (or equivalent Out Of Band Management ports like me0.0 depending on platform) in the Default or Master Virtual Router instance will be used.

Where AAA Servers are not accessible through the routes or no OOB Management Network is deployed, the source address of a different interface will sometimes be used instead. A different source address may be used for each AAA Server if required for reachability in your environment.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

6.8.2 Ensure Share-Secret is set for External AAA Servers (Automated)

Profile Applicability:

- Level 1

Description:

External AAA Servers should be configured with a Shared Secret.

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services.

Both protocols provide services to authenticate users on routers, switches and other systems. Because these servers are being trusted to authenticate and authorized your administrative users, it is vital to ensure the identity of the RADIUS or TACACS+ server.

Each configured External AAA Server *must* be configured with a Shared Secret to ensure mutual authentication of the Client (the JUNOS Device) and Server.

Impact:

Ensure that External AAA Servers are tested prior to deploying in a live environment.

It is generally recommended to configure a single "Rescue" or "Emergency" account locally under the [edit system login] hierarchy to provide access in the event of a AAA failure or mis-configuration prior to deploying External AAA.

Audit:

To confirm whether a Shared Secret is set, execute the following commands from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | display set | match "radius-server|tacplus-server" | match
"secret" | count
```

The above command should return a line count >=1, equal to the number of configured External AAA Servers, which can be confirmed with the following command:

```
[edit system]
user@host#show | display set | match "radius-server|tacplus-server" | count
```

Remediation:

Configure a Shared Secret for all External Authentication Server using the following commands under the `[edit system]` hierarchy; For RADIUS Servers:

```
[edit system]
user@host#set radius-server <server ip> secret <shared secret>
```

For TACACS+ Servers:

```
[edit system]
user@host#set tacplus-server <server ip> secret <shared secret>
```

Default Value:

No External AAA is configured by default.

References:

1. Configuring RADIUS Authentication, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-radius-authentication.html#id-10624913)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirements 7.2 and 8

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.8.3 Ensure a Different Shared Secret is Set for each External AAA Server (Manual)

Profile Applicability:

- Level 1

Description:

External AAA Servers should be configured with a Shared Secret.

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services.

Both protocols provide services to Authenticate and Authorization of users on routers, switches and other systems. Because these servers are being trusted to authenticate your administrative users, it is vital to ensure the identity of the RADIUS or TACACS+ server. With both protocols this is achieved by using a Shared Secret.

To ensure resilience and that compromise of a single AAA Server does not result in all AAA Servers being compromised, it is recommended that a different Secret Key be used for each AAA Server. This way, any server suspected of compromise can be taken offline and the remaining servers can remain trusted to provide AAA services.

Because the Shared Secrets are stored as salted hashed values in the JUNOS configuration, it is not possible to readily audit this Recommendation from the JUNOS device, so this Recommendation is not Scored.

Impact:

Ensure that External AAA Servers are tested prior to deploying in a live environment.

It is generally recommended to configure a single "Rescue" or "Emergency" account locally under the [edit system login] hierarchy to provide access in the event of a AAA failure or mis-configuration prior to deploying External AAA.

Audit:

Because the Shared Secrets are stored as salted hashed values in the JUNOS configuration, it is not possible to readily audit this Recommendation from the JUNOS device, so this Recommendation is not Scored.

Remediation:

Configure a Shared Secret for all External Authentication Server using the following commands under the `[edit system]` hierarchy; For RADIUS

```
[edit system]
user@host#set radius-server <server ip> secret <shared secret> source-address
<loopback IP>
```

For TACACS+

```
[edit system]
user@host#set tacplus-server <server ip> secret <shared secret> source-
address <Loopback IP>
```

Default Value:

No External AAA is configured by default.

References:

1. Configuring RADIUS Authentication, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-radius-authentication.html#id-10624913)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirements 7.2 and 8

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.8.4 Ensure MS-CHAPv2 RADIUS Authentication (Automated)

Profile Applicability:

- Level 1

Description:

MS-CHAPv2 should be used for RADIUS authentication if RADIUS Servers are configured

Rationale:

RADIUS is a centralized Authentication, Authorization and Accounting (AAA) protocol providing services to authenticate users on routers, switches and other systems.

By default, JUNOS devices which are configured to use RADIUS for External AAA use the Password Authentication Protocol (PAP) for Authenticating users. PAP is an old standard, dating back to Dial-up Internet connections where interception was not considered viable; so PAP sends the user's password in plain-text (unencrypted) over the network to the RADIUS server, exposing the password to interception and misuse.

All current JUNOS devices support the use of the stronger MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol, Version 2) standard for user Authentication, which is widely supported.

With CHAP, the password is never sent over the network. Instead a "challenge" is encrypted by the RADIUS Server and sent to the JUNOS device, which decrypts the challenge using the configured Secret. The JUNOS device combines the the decrypted Challenge with the password provided by the user into a Hash, which is returned to the RADIUS Server which performs the same Hash of the Challenge and the users password to determine whether to permit or deny the request.

Use of MS-CHAPv2 on JUNOS Devices also allows for users to change their password if the password has expired.

Where RADIUS Servers are configured for External AAA, it is recommended that MS-CHAPv2 be used instead of, the default, PAP standard for user Authentication.

Impact:

Ensure that External AAA Servers are tested prior to deploying in a live environment.

It is generally recommended to configure a single "Rescue" or "Emergency" account locally under the [edit system login] hierarchy to provide access in the event of a AAA failure or mis-configuration prior to deploying External AAA.

Audit:

Execute the following command from the `[edit system]` hierarchy:

```
[edit radius-options]
user@host#show radius-options
```

The above command should return:

```
password-protocol mschap-v2;
```

Remediation:

Configure RADIUS to use MS-CHAPv2 Authentication using the following commands under the `[edit system]` hierarchy;

```
[edit system]
user@host#set radius-options password-protocol mschap-v2
```

Default Value:

No External AAA is configured by default.

References:

1. Configuring RADIUS Authentication, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-radius-authentication.html#id-10624913)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirements 7.2 and 8

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.8.5 Ensure Source-Address is set for External AAA Servers (Automated)

Profile Applicability:

- Level 1

Description:

The Source-Address should be set for each External AAA Server configured

Rationale:

RADIUS and TACACS+ are centralized Authentication, Authorization and Accounting (AAA) services.

Both protocols provide services to Authenticate users on routers, switches and other systems. Juniper devices support both RADIUS and TACACS+ Authentication and you should configure at least one External Authentication Server of either type.

For resilience it is generally recommended to configure multiple AAA Servers, which can be of the same type (both TACACS+ or both RADIUS) or can be mixed (one RADIUS and one TACACS+) as required so long as both are configured in `[edit system authentication-order]`.

RADIUS and TACACS+ servers are sensitive systems and should typically be protected by Firewall Filters and ACLs on the RADIUS/TACACS+ Service restricting the Source Address of valid clients. To ensure that these restrictions can be correctly, and strictly, applied - it is important to ensure that the Juniper device always uses the same Source Address when sending packets to these services, irrespective of the route being used.

To do this you should explicitly set the Source Address used for each server (these can be different addresses for different individual servers if required). Typically either the Loopback Address (assigned to Lo0.0) or Out of Band Management address (assigned to FXP0.0) in the Default/Master Virtual Router instance should be used as the Source Address.

Impact:

Ensure that External AAA Servers are tested prior to deploying in a live environment.

It is generally recommended to configure a single "Rescue" or "Emergency" account locally under the `[edit system login]` hierarchy to provide access in the event of a AAA failure or mis-configuration prior to deploying External AAA.

Audit:

From the command prompt, execute the following commands from the `[edit system]` hierarchy:

```
[edit system]
user@host# show | display set | match "tacplus-server|radius-server" | match
"source-address" | count
```

The above command should return a line count which is equal to the number of configured External AAA Servers which can be found with the following command:

```
[edit system]
user@host# show | display set | match "tacplus-server|radius-server" | count
```

NOTE - While not explicitly tested in this recommendation, the configured server type (RADIUS or TACPLUS) ***must*** *be included in the* `[edit system authentication-order]` *section to be used.*

Remediation:

Configure at least one External Authentication Server using the following commands under the `[edit system]` hierarchy; For RADIUS

```
[edit system]
user@host#set radius-server <server ip> secret <shared secret> source-address
<loopback IP>
```

Or for TACACS+

```
[edit system]
user@host#set tacplus-server <server ip> secret <shared secret> source-
address <loopback IP>
```

Default Value:

No External AAA is used by default

References:

1. Configuring RADIUS Authentication, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-radius-authentication.html#id-10624913)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirements 7.2 and 8

Additional Information:

In most environments the address assigned to either Lo0.0 or FXP0.0 (or equivalent Out Of Band Management ports like me0.0 depending on platform) in the Default or Master Virtual Router instance will be used.

Where AAA Servers are not accessible through the routes or no OOB Management Network is deployed, the source address of a different interface will sometimes be used instead. A different source address may be used for each AAA Server if required for reachability in your environment.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

6.9 Root-Authentication

The Root account provides full access to the Juniper router and to the underlying BSD OS. An attacker gaining access to this user account would gain complete control of the platform.

6.9.1 Ensure a complex Root Password is Set (Automated)

Profile Applicability:

- Level 1

Description:

A complex Root Password should be set for the system.

Rationale:

Due to the importance of the Root user account, which has full control of the JUNOS system and underlying Unix OS, a complex password should be employed to help prevent attackers employing 'brute force' or 'dictionary' attacks to gain full control of the router. Passwords are stored, automatically by JUNOS, as a SHA1 hash in the configuration under the `[edit system root-authentication]` hierarchy.

A complex password should be employed which meets or exceeds the following requirements:

- Does not contain Dictionary words, names, dates, phone numbers or addresses.
- Is at least 8 characters in length.
- Contains at least one each of upper & lower case letters, numbers and special characters.
- Avoids more than 4 digits or same case letters in a row.

Because Root Authentication *must* be set before JUNOS will permit the first configuration commit on a new JUNOS system, password complexity requirements covered in other Recommendations may not yet be configured and do not apply to passwords retrospectively. Therefore it is important to manually ensure that a complex password is used for the Root account.

Impact:

Root Authentication *must* be set prior to JUNOS allowing the first commit on a new system. Ensure that, while the Root password is complex, it is safely stored in a Password Vault or remembered as it will be required for access to the system until other accounts are configured or to perform certain tasks.

Audit:

Because all Root Passwords are automatically stored by JUNOS as a SHA1 hash, or optionally using other hashing algorithms, it is not possible to confirm from the command

line the complexity and length of the password used.
Therefore, this recommendation is Scoring *only* that a Root password has been set and not that the password meets the suggested complexity requirements.

Remediation:

Root Authentication must be configured prior to the first commit on a new system. A Root password may be set from the CLI using either of the two methods below, from the `[edit system]` hierarchy.
To enter a new Root Password in plain text type:

```
[edit system]
user@host#set root-authentication plain-text-password
```

You will be prompted to enter the new Password twice and, if the Passwords match, JUNOS will add a SHA1 hash of the Password to the configuration.
Alternatively, if you are copying the configuration from an existing JUNOS system (using the same hashing algorithm) or template, you may apply an existing hash of the Root password:

```
[edit system]
user@host#set root-authentication encrypted-password "<hash>"
```

Default Value:

The Root Authentication is blank by default, but *must* be set prior to JUNOS allowing the first configuration to be committed.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 62, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.2.3
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/authentication-root-password-configuring.html

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.9.2 Ensure Root Password is Unique (Manual)

Profile Applicability:

- Level 1

Description:

The Root Password should be unique.

Rationale:

Due to the rights associated with the Root user account it must be protected at all costs to prevent malicious users taking ownership of the router.

Using the same password for an individual User or other usage exposes the extremely privileged Root user account to abuse by that user and introduces the need to manually change the Root password should that user leave the organization.

Further risks are presented by the lower level hashing algorithm which may be used to protect other system passwords. On some JUNOS systems or External AAA platforms these utilize MD5, a demonstrably less secure protocol then SHA1 which used for the Root password. Theoretically an attacker could exploit the weaker hashing used on these lesser system passwords to recover the Root password.

Finally, the Root password should not be reused on other systems, including other routers, and should be stored securely - such as using a Password Manager. If the Root Password was the same across all of the routers and other systems in your network, the compromise of one host could result in the compromise of all hosts.

Impact:

Root Authentication must be set prior to JUNOS allowing the first commit on a new system. Ensure that, while the Root password is complex, it is safely stored in a Password Vault or remembered as it will be required for access to the system until other accounts are configured or to perform certain tasks.

Audit:

Because all Root Passwords are automatically stored by JUNOS as a SHA1 hash, which will always be 160bits long, it is not possible to confirm the uniqueness of the Root Password.

Remediation:

Users will generally be prompted to set the Root password during initial setup of the router, however, a password may be set from the CLI using either of the two methods below from the `[edit system]` hierarchy; To enter a new Root Password in plain text type:

```
[edit system]
user@host#set root-authentication plain-text-password
```

You will be prompted to enter the new Password twice and, if the Passwords match, JUNOS will add a SHA1 hash of the Password to the configuration. If you already have a SHA1 hash of your Root Password (from an existing router configuration, for example), enter the following command:

```
[edit system]
user@host#set root-authentication encrypted-password "<SHA1 hash>"
```

If JWEB is installed on your router, the Root Password may also be changed through the `Configuration > Quick Configuration > Setup` page.

Default Value:

The Root Authentication is blank by default, but must be set prior to JUNOS allowing the first configuration to be committed.

References:

1. http://en.wikipedia.org/wiki/Privilege_escalation
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/authentication-root-password-configuring.html

Additional Information:

It is not possible from auditing the JUNOS device to confirm that the Root password is unique and is not reused on other systems. Therefore this Recommendation is not Scorable.

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.9.3 Ensure SSH Key Authentication is not set for Root Login (Automated)

Profile Applicability:

- Level 1

Description:

SSH Key Based Authentication should not be used for Root Login

Rationale:

Due to the sensitive nature of SSH, potentially allowing full management of the targeted device, protecting SSH access using strong authentication methods is essential to the security of the device.

One method which is supported in SSH for stronger authentication is the use of Public/Private Encryption Key Pairs in place of a more traditional login prompt for a Username and Password. Instead, an administrator uploads the user's Public key to the JUNOS (or other) device to be managed.

When the user connects, they will use their Private key to encrypt some session specific data. The JUNOS device can verify the Users identity by decrypting that data using the Public key configured previously and comparing it to an expected result. If the results match, then the user must have access to the Private key, so is considered valid.

Unfortunately using SSH Keys to authenticate User Logins to JUNOS devices introduce a number of security issues:

- Public Keys may only be configured locally on each JUNOS device
- Public Keys are used instead of centralized AAA using TACACS+ or RADIUS as covered in Recommendation 6.8.1 Ensure External AAA Server is set
- The use of SSH Keys means only a single Authentication Factor (the keys) can be used, preventing the use of Multi Factor Authentication as covered in 6.6.14 Ensure Multi-Factor is used with External AAA
- JUNOS does not provide any method to automate rollover or locking of keys. If keys are compromised/lost, they must be changed on every JUNOS device on which they are configured.
- Some SSH implementation support the use of X.509 PKI Certificates for managing SSH Keys, but JUNOS does not.

Because of these limitations and the difficulty in auditing and managing SSH Keys on JUNOS devices, this method should not be used for Authentication of User logins or for the Root

User, which is configured separately under the `[edit system root-authentication]` configuration hierarchy.

Audit:

To confirm whether Root Login has been configured to use SSH Key based Authentication, issue the following command from the `[edit system root-authentication]` hierarchy:

```
[edit system root-authentication]
user@host# show | match "ssh-" | count
```

The above command should return a count of 0.

Remediation:

If SSH Key based Authentication is configured for the Root Authentication, remove it using the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host# delete root-authentication
```

To set a new Root Password in plain text type:

```
[edit system]
user@host#set root-authentication plain-text-password
```

You will be prompted to enter the new Password twice and, if the Passwords match, JUNOS will add a hash of the Password to the configuration.
If you already have a hash of your Root Password (from an existing router configuration, for example), enter the following command:

```
[edit system]
user@host#set root-authentication encrypted-password "<hash>"
```

Note - Hashes use SHA1 by default, but may use other hashing mechanisms depending on the device configuration - ensure the device you are copying from is configured to use the same hashing method.
If JWEB is installed on your router, the Root Password may also be changed through the Configuration > Quick Configuration > Setup page.

Default Value:

The Root account does not have any authentication set by default, but at least one root-authentication method *must* be configured during initial configuration before JUNOS will allow the configuration to be committed.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/ssh-rsa-edit-system-root-authentication-qfx-series.html
2. https://www.ssh.com/ssh/key/

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.10 Services

Like any Operating System, JUNOS provides a number of services to the user. As with hardening any OS, some services should be configured more securely and some disabled. Services related to the general operation of the router are configured under the `[edit system services]` hierarchy.

6.10.1 SSH

The Secure Shell (SSH) service provides remote access to the JUNOS Command Line Interface (CLI), similar to Telnet. Unlike Telnet, which sends all data (including passwords) in Plain Text, SSH uses Encryption to protect data in transit over the network.

SSH is configured under the `[edit system services ssh]` hierarchy and the SSH Service is enabled by default on most JUNOS platforms.

Only apply the recommendations in this section where SSH is configured on the device. You can confirm whether the SSH service is configured by issuing the following command from the `[edit]` hierarchy in Configuration Mode:

```
[edit]

user@host# show system services | match "ssh \{|ssh\;"
```

If the terms "ssh {" or "ssh;" are returned, all Recommendations in this section should be considered.

If management via SSH, or related services such as NETCONF which use SSH for transport, is not required the SSH service should be disabled using the following command:

```
[edit]

user@host# delete system services ssh
```

6.10.1.1 Ensure SSH Service is Configured if Remote CLI is Required (Manual)

Profile Applicability:

- Level 1

Description:

SSH should be utilized for remote console sessions to Juniper routers.

Rationale:

SSH provides administrators with a remote console session on the router in a similar fashion to Telnet. Unlike Telnet, SSH encrypts all data as it transits the network and ensures the identity of the remote host.

Because of this extra protection, all remote console sessions should use SSH.

If Remote CLI or services which use SSH for transport, like Secure Copy (SCP) or NETCONF, are required SSH should be disabled.

Impact:

Disabling SSH may result in loss of remote management of the device and also impact other services, like NETCONF, which use SSH for transport.

Audit:

From the command prompt, execute the following command:

```
[edit]
user@host#show system services | match "ssh {" | count
```

This command should return a line count of 1 if SSH is configured.

Remediation:

To enable SSH access issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#set services ssh
```

Where SSH is used, all other Recommendations in this section should be considered.
If SSH is currently configured but is not required it should be disabled using the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#delete services ssh
```

Default Value:

For most platforms SSH access is enabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/ssh-edit-system.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.2 Ensure SSH is Restricted to Version 2 (Automated)

Profile Applicability:

- Level 1

Description:

Remote console connections should only use SSH Version 2.

Rationale:

SSH Version 1 has been subject to a number of serious vulnerabilities and is no longer considered to be a secure protocol, resulting in the adoption of SSH Version 2 as an Internet Standard in 2006. Juniper routers support both versions, but due to the weakness of SSH Version 1 only the later standard should be used.

Audit:

From the command prompt, execute the following command at the `[edit system services ssh]` configuration hierarchy:

```
[edit system services ssh]
user@host#show protocol-version
```

The above command should yield the following output:

```
protocol-version v2
```

Remediation:

To restrict SSH to Version 2 only, issue the following command from the `[edit system service ssh]` hierarchy:

```
[edit system services ssh]
user@host#set protocol-version v2
```

Default Value:

Version 2 should be the default on all current platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 222, National Security Agency (NSA)

2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.3 Ensure SSH Connection Limit is Set (Automated)

Profile Applicability:

- Level 1

Description:

SSH connections should be limited.

Rationale:

SSH is a common management protocol, so is often targeted by attackers trying to gain access to routers or execute Denial of Service (DoS) attacks.

To limit the effectiveness of DoS and Brute Force attacks targeting the JUNOS device using the SSH service the maximum number of concurrent connections should be limited. Any sessions attempted once this limit is reached will be rejected. A maximum limit of 10 concurrent sessions is recommended for most environments.

Audit:

From the command prompt, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show connection-limit
```

The above command should yield the following output:

```
connection-limit 10;
```

The value should be less than or equal to 10.

Remediation:

To restrict concurrent SSH connections, issue the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#set connection-limit <limit>
```

NOTE - *On some platforms the maximum configuration connection limit may be significantly lower than 10, for example, on an SRX110 the connection limit can be set to a value between 1 and 3.*

Default Value:

Up to 75 concurrent sessions are accepted by default on most current platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 222, National Security Agency (NSA)
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.4 Ensure SSH Rate Limit is Configured (Automated)

Profile Applicability:

- Level 1

Description:

SSH connections should be limited.

Rationale:

SSH is a common management protocol, so is often targeted by attackers trying to gain access to routers or execute Denial of Service (DoS) attacks.

To limit the effectiveness of DoS and Brute Force attacks targeting the JUNOS Device using the SSH service, rate limiting should be used to restrict the maximum number of new connections per second.

Any sessions attempted once this limit is reached will be rejected. A maximum limit 4 new sessions per second is recommended for most environments.

Audit:

From the command prompt, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show rate-limit
```

The above command should yield the following output:

```
rate-limit <limit>;
```

should be a value less than or equal to 4.

Remediation:

To restrict concurrent SSH connections, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set services ssh rate-limit <limit>
```

Default Value:

Up to 150 new sessions per second are accepted by default on most current platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 222, National Security Agency (NSA)
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.5 Ensure Remote Root-Login is denied via SSH (Automated)

Profile Applicability:

- Level 1

Description:

Prevent remote access to the Root user account on the device.

Rationale:

During normal operation, remote access to the Root user should not be required.

Because the Root user account has full access to the router and underlying BSD OS it is an extremely valuable target for attackers and must be protected from remote exploitation.

By disabling remote access to the Root user account we ensure that physical access to the console port is required in order to gain this level of access.

Root access only needs to be disabled for SSH connections, as it is never allowed over a Telnet or other remote access session.

Audit:

From the command prompt, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show | match root-login
```

The above command should yield the following output:

```
root-login deny;
```

Remediation:

To disable remote access to the Root account issue the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#set root-login deny
```

Default Value:

By default, if SSH is enabled, remote login with the Root account is permitted.

References:

1. Configuring the Root Login, JUNOS 9.2 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos92/swconfig-system-basics/configuringthe-root-login.html)

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.6 Ensure Strong Ciphers are set for SSH (Automated)

Profile Applicability:

- Level 1

Description:

SSH should be configured with strong ciphers

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Ciphers using older Encryption Algorithms such as Blowfish or RC4 which are no longer considered suitable for use to protect sensitive services like SSH.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Ciphers based on 3DES and AES *only*.

Audit:

To confirm the presence of insecure Ciphers, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show ciphers | display set | except "aes|3des" | count
```

The above command should return 0 or null if no weak ciphers are configured.
Then confirm that acceptable Ciphers have been restricted with the following command:

```
[edit system services ssh]
user@host#show ciphers | count
```

This command should return 1 if Ciphers are restricted.

Remediation:

To remove a single insecure cipher, issue the following command from the `[edit system services ssh]` hierarchy;

```
[edit system services ssh]
user@host#delete ciphers <cipher suite name>
```

If multiple insecure Ciphers were set, it will generally be easier to delete *all* the Cipher restrictions with the following command:

```
[edit system services ssh]
user@host#delete ciphers
```

Once all insecure Ciphers have been removed, add one or more stronger Ciphers (in this example *all* stronger Ciphers available on most JUNOS devices are set in a single command)

```
[edit system services ssh]
user@host#set ciphers [ 3des-cbc aes128-cbc aes128-ctr aes128-gcm@openssh.com
aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-gcm@openssh.com ]
```

Note - note all of the Ciphers in the example above are supported on all JUNOS devices.
In many cases the GCM mode AES ciphers may be unavailable, a shorter list of Ciphers may be set with the following command for these systems:

```
[edit system services ssh]
user@host#set ciphers [ 3des-cbc aes128-cbc aes128-ctr aes192-cbc aes192-ctr
aes256-cbc aes256-ctr  ]
```

Finally, single Ciphers or a smaller selection of these more secure Ciphers may be selected on the user's discretion.

```
[edit system services ssh]
user@host#set ciphers <cipher suite name>
```

Default Value:

For most platforms SSH access is enabled by default but ciphers are not restricted.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)

3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-ciphers.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.7 Ensure Only Suite B Ciphers are set for SSH (Automated)

Profile Applicability:

- Level 2

Description:

SSH should be configured with Ciphers based on the Suite B Standard

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Ciphers using older Encryption Algorithms such as Blowfish or RC4 which are no longer considered suitable for use to protect sensitive services like SSH.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using Ciphers recommended in the National Security Agency Suite B Standard.

Suite B standards for Cryptographic functions are developed and distributed by the US National Security Agency as part of Cryptographic Modernization Programme for protection of US Government data, both unclassified and classified (to Secret). Suite B standards for SSH are set out in RFC6239 and restrict Ciphers to AES-128 and AES-256 in Galois Counter Mode *only*.

When AES is used in Galois Counter Mode (AEAD_AES_128/256_GCM) for Confidentiality (Ciphers), it is also used to provide Integrity (replacing any Message Authentication Codes (MACs) which may be configured). For more details, please see RFC5647.

NOTE - The OpenSSH implementation used in JUNOS is not fully compliant with Suite B SSH set out in RFC6239, but these standards have been used as guidance for setting the more restrictive Level 2 recommendation.

Impact:

Some SSH Clients or other management applications or automation platforms utilizing SSH may not support the stronger ciphers used in Suite B, so may be unable to connect.

Ensure that all applications are fully tested before deploying this recommendation in a production environment.

Audit:

To confirm the presence of insecure Ciphers, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show ciphers | display set | except "gcm" | count
```

The above command should return 0 or null if no weak ciphers are configured.
Then confirm that acceptable Ciphers have been restricted with the following command:

```
[edit system services ssh]
user@host#show ciphers | count
```

This command should return 1 if Ciphers are restricted.

Remediation:

To remove a single insecure cipher, issue the following command from the `[edit system services ssh]` hierarchy;

```
[edit system services ssh]
user@host#delete ciphers <cipher suite name>
```

If multiple insecure Ciphers were set, it will generally be easier to delete *all* the Cipher restrictions with the following command:

```
[edit system services ssh]
user@host#delete ciphers
```

Once all insecure Ciphers have been removed, add one or more of the AES-GCM ciphers.

```
[edit system services ssh]
user@host#set ciphers [ aes128-gcm@openssh.com aes256-gcm@openssh.com ]
```

Default Value:

For most platforms SSH access is enabled by default but ciphers are not restricted.

Not all platforms or versions of JUNOS support AES in Galois/Counter Mode.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-ciphers.html
4. https://tools.ietf.org/html/rfc6239
5. https://tools.ietf.org/html/rfc5647

Additional Information:

The OpenSSH implementation used in JUNOS is not fully compliant with Suite B SSH set out in RFC6239, but these standards have been used as guidance for setting the more restrictive Level 2 recommendation. Specifically, RFC6239 requires the use of X.509v3 Certificates for Authentication when using Suite B SSH and this is *not* supported on JUNOS at the present time.

Not all JUNOS devices support AES in GCM mode, some devices may have to be replaced to meet this recommendation.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.8 Ensure Strong MACs are set for SSH (Automated)

Profile Applicability:

- Level 1

Description:

SSH should be configured with strong message authentication algorithms.

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Message Authentication using older algorithms and methods designed with performance rather than security in mind such as HMAC-MD5 or UMAC-128.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Message Authentication Code (MAC) methods based on the more modern SHA2 algorithm.

Audit:

To confirm the presence of insecure Message Authentication Codes, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show macs | display set | except "sha2" | count
```

The above command should return 0 or null if no weak MACs are configured.
Then confirm that acceptable MACs have been restricted with the following command:

```
[edit system services ssh]
user@host#show macs | count
```

This command should return 1 if MACs are restricted.

Remediation:

To remove a single insecure MAC method, issue the following command from the `[edit system services ssh]` hierarchy;

```
[edit system services ssh]
user@host#delete macs <mac name>
```

If multiple insecure MAC methods were set, it will generally be easier to delete *all* the MAC method restrictions with the following command:

```
[edit system services ssh]
user@host#delete macs
```

Once all insecure MAC methods have been removed, add one or more stronger MACS (in this example *all* stronger MACS available on most JUNOS devices are set in a single command)

```
[edit system services ssh]
user@host#set macs [ hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-
512 hmac-sha2-512-etm@openssh.com ]
```

Finally, single MAC methods or a smaller selection of these more secure MACs may be selected on the users discretion.

```
[edit system services ssh]
user@host#set macs <mac name>
```

Default Value:

For most platforms SSH access is enabled by default but macs are not restricted.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-macs.html

Additional Information:

Support for SHA2 was introduced in JUNOS 12.1, so should be present on all currently supported devices.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.9 Ensure Strong Key Exchange Methods are set for SSH (Automated)

Profile Applicability:

- Level 1

Description:

SSH should be configured with strong key exchange algorithms.

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Key Exchange using older algorithms and methods such as Diffie-Hellman Group 1 with SHA1.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Key Exchange methods based on Diffie-Hellman using stronger Elliptic Curve or SHA2 algorithms.

Audit:

To confirm the presence of insecure Key Exchange methods, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show key-exchange | display set | except "sha2|ecdh|curve" | count
```

The above command should return 0 or null if no weak key exchange methods are configured.
Then confirm that acceptable Key Exchange methods have been restricted with the following command:

```
[edit system services ssh]
user@host#show key-exchange | count
```

This command should return 1 if Ciphers are restricted.

Remediation:

To remove a single insecure Key Exchange method, issue the following command from the `[edit system services ssh]` hierarchy;

```
[edit system services ssh]
user@host# delete key-exchange <mac name>
```

If multiple insecure Key Exchange methods were set, it will generally be easier to delete *all* the Key Exchange method restrictions with the following command:

```
[edit system services ssh]
user@host# delete key-exchange
```

Once all insecure methods have been removed, add one or more stronger Key Exchange methods (in this example *all* stronger methods available on most JUNOS devices are set in a single command)

```
[edit system services ssh]
user@host# set key-exchange [ curve25519-sha256 ecdh-sha2-nistp256 ecdh-sha2-
nistp384 ecdh-sha2-nistp521 group-exchange-sha2 ]
```

Finally, single Key Exchange methods or a smaller selection of these more secure methods may be selected on the user's discretion.

```
[edit system services ssh]
user@host# set key-exchange <method>
```

Default Value:

For most platforms SSH access is enabled by default but key exchange methods are not restricted.

On FIPS releases the `curve25519-sha256`, `dh-group1-sha1`, `group-exchange-sha` & `group-exchange-sha2` methods are not supported.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-macs.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.10 Ensure Only Suite B Key Exchange Methods are set for SSH (Automated)

Profile Applicability:

- Level 2

Description:

SSH should be configured to use only Suite B key exchange algorithms.

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Key Exchange using older algorithms and methods such as Diffie-Hellman Group 1 with SHA1.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Key Exchange methods recommended in the National Security Agency Suite B Standard.

Suite B standards for Cryptographic functions are developed and distributed by the US National Security Agency as part of Cryptographic Modernization Program for protection of US Government data, both unclassified and classified (to Secret). Suite B standards for SSH are set out in RFC6239 and restrict Key Exchange to Elliptic Curve Diffie Hellman with NIST P Values and SHA2 only.

NOTE - *The OpenSSH implementation used in JUNOS is not fully compliant with Suite B SSH set out in RFC6239, but these standards have been used as guidance for setting the more restrictive Level 2 recommendation.*

Impact:

Some SSH Clients or other management applications or automation platforms utilizing SSH may not support the stronger Key Exchange Methods used in Suite B, so may be unable to connect.

Ensure that all applications are fully tested before deploying this recommendation in a production environment.

Audit:

To confirm the presence of none Suite B Key Exchange methods, execute the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show key-exchange | display set | except "nist" | count
```

The above command should return 0 or null if no weak key exchange methods are configured.
Then confirm that acceptable Key Exchange methods have been restricted with the following command:

```
[edit system services ssh]
user@host#show key-exchange | count
```

This command should return 1 if Ciphers are restricted.

Remediation:

To remove a single non-Suite B Key Exchange method, issue the following command from the `[edit system services ssh]` hierarchy;

```
[edit system services ssh]
user@host# delete key-exchange <mac name>
```

If multiple insecure Key Exchange methods were set, it will generally be easier to delete *all* the Key Exchange method restrictions with the following command:

```
[edit system services ssh]
user@host# delete key-exchange
```

Once all insecure methods have been removed, add one or more stronger Key Exchange methods (in this example *all* Suite B methods available on most JUNOS devices are set in a single command)

```
[edit system services ssh]
user@host# set key-exchange [ ecdh-sha2-nistp256 ecdh-sha2-nistp384  ecdh-
sha2-nistp512 ]
```

NOTE - *The ecdh-sha2-nistp512 Key Exchange method is not cited specifically in RFC6239, but* ***is*** *acceptable in addition/in place of the other NIST Elliptic Curve Diffie Hellman exchange methods for the purposes of this recommendation.*

Finally, single Key Exchange methods or a smaller selection of these more secure methods may be selected on the user's discretion.

```
[edit system services ssh]
user@host# set key-exchange <method>
```

Default Value:

For most platforms SSH access is enabled by default but key exchange methods are not restricted.

On FIPS releases the `curve25519-sha256`, `dh-group1-sha1`, `group-exchange-sha` & `group-exchange-sha2` methods are not supported.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-macs.html
4. https://tools.ietf.org/html/rfc6239

Additional Information:

The OpenSSH implementation used in JUNOS is not fully compliant with Suite B SSH set out in RFC6239, but these standards have been used as guidance for setting the more restrictive Level 2 recommendation. Specifically, RFC6239 requires the use of X.509v3 Certificates for Authentication when using Suite B SSH and this is not supported on JUNOS at the present time.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.11 Ensure Strong Key Signing Algorithms are set for SSH (Automated)

Profile Applicability:

- Level 1

Description:

SSH should be configured with strong key signing algorithms

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Key Signing methods using older algorithms and methods such as 1024 bit DSA keys.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Key Signing methods based on RSA or Elliptic Curve algorithms, while weaker signing methods are explicitly disabled.

Audit:

Ensure that DSA Keys are explicitly disabled by issuing the following command at the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show hostkey-algorithm | match "no-ssh-dss" | count
```

This command should return a value of 1.

Remediation:

To explicitly disable DSA signatures, type the following command at the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#set hostkey-algorithm no-ssh-dss
```

Enable one or more stronger ciphers using the following commands:

```
[edit system services ssh]
user@host#set hostkey-algorithm ssh-ecdsa
user@host#set hostkey-algorithm ssh-ed25519
user@host#set hostkey-algorithm ssh-rsa
```

Default Value:

For most platforms SSH-ECDSA, SSH-ED25519, SSH-DSS (1024 bit DSA keys) and SSH-RSA are permitted by default.

SSH-DSS is not supported on JUNOS in FIPS Mode, so cannot be enabled in FIPS mode.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-host-key-algorithm.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.12 Ensure Only Suite B Based Key Signing Algorithms are set for SSH (Automated)

Profile Applicability:

- Level 2

Description:

SSH should be configured with Suite B based key signing algorithms

Rationale:

SSH (Secure Shell) is the defacto standard protocol used for remote administration of network devices and Unix servers, providing an encrypted and authenticated alternative to Telnet. However, this ubiquity and requirement to support a wide range of clients and deployment scenarios, as well as SSH's age, mean SSH needs to support a variety of Ciphers of varying strengths.

By default, for the widest range of client compatibility, JUNOS supports SSH Key Signing methods using older algorithms and methods such as 1024 bit DSA keys.

SSH is a vital tool for administering most JUNOS devices, providing privileged access and potentially transporting sensitive information including passwords. It is recommended that SSH sessions be protected by restricting JUNOS to using stronger Key Signing methods based on National Security Agency Suite B Standards, while weaker signing methods are explicitly disabled.

Suite B standards for Cryptographic functions are developed and distributed by the US National Security Agency as part of Cryptographic Modernization Programme for protection of US Government data, both unclassified and classified (to Secret). Suite B standards for SSH are set out in RFC6239 and restrict Key Signing to x509v3-ecdsa-sha2-nistp256 or x509v3-ecdsa-sha2-nistp384 only.

NOTE - *The OpenSSH implementation used in JUNOS is not fully compliant with Suite B SSH set out in RFC6239, but these standards have been used as guidance for setting the more restrictive Level 2 recommendation. In particular, at time of writing, JUNOS does not support SSH Authentication through the use of X.509 Certificates - so it is not possible to be fully compliant with the Suite B recommendations, however ECDSA based Key Signing is supported, including with the NIST P 256bit and 384bit P Values, for Public Keys.*

Impact:

Some SSH Clients or other management applications or automation platforms utilizing SSH may not support the stronger ECDSA Key Signing standard, so may be unable to connect.

Ensure that all applications are fully tested before deploying this recommendation in a production environment.

Audit:

Ensure that DSA Keys are explicitly disabled by issuing the following command at the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#show hostkey-algorithm | match "no-ssh-(dss|rsa|ed25519)" | count
```

This command should return a value of 3.

Remediation:

To explicitly disable DSA, RSA and ED25519 signatures, type the following commands at the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host#set hostkey-algorithm no-ssh-dss
user@host#set hostkey-algorithm no-ssh-rsa
user@host#set hostkey-algorithm no-ssh-ed25519
```

Enable ECDSA for SSH Public Keys using the following commands:

```
[edit system services ssh]
user@host#set hostkey-algorithm ssh-ecdsa
```

Default Value:

For most platforms SSH-ECDSA, SSH-ED25519, SSH-DSS (1024 bit DSA keys) and SSH-RSA are permitted by default.

SSH-DSS is not supported on JUNOS in FIPS Mode, so cannot be enabled in FIPS mode.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. Configuring SSH Service for Remote Access to the Router, JUNOS Software System Basics Guide, Juniper Networks

(http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/ssh-services-configuring.html)

3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-ssh-host-key-algorithm.html
4. https://tools.ietf.org/html/rfc6239

Additional Information:

JUNOS does not, at the time of writing, support use of X.509 Certificates for verifying Public Keys and allowing for PKI based management of access using SSH. Therefore it is not possible to be fully compliant with the Suite B Standards for SSH set out in RFC 6239 on JUNOS.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.1.13 Ensure SSH Key Authentication is Disabled (Manual)

Profile Applicability:

- Level 2

Description:

SSH Key based Authentication should be disabled (if not used for automation)

Rationale:

Due to the sensitive nature of SSH, potentially allowing full management of the targeted device, protecting SSH access using strong authentication methods is essential to the security of the device.

One method which is supported in SSH for stronger authentication is the use of Public/Private Encryption Key Pairs in place of a more traditional login prompt for a Username and Password. Instead, an administrator uploads the user's Public key to the JUNOS (or other) device to be managed.

When the user connects, they will use their Private key to encrypt some session specific data. The JUNOS device can verify the Users identity by decrypting that data using the Public key configured previously and comparing it to an expected result. If the results match, then the user must have access to the Private key, so is considered valid.

Unfortunately using SSH Keys to authenticate User Logins to JUNOS devices introduce a number of security issues:

- Public Keys may only be configured locally on each JUNOS device
- Public Keys are used instead of centralized AAA using TACACS+ or RADIUS as covered in Recommendation 6.8.1 Ensure External AAA Server is set
- The use of SSH Keys means only a single Authentication Factor (the keys) can be used, preventing the use of Multi Factor Authentication as covered in 6.6.14 Ensure Multi-Factor is used with External AAA
- JUNOS does not provide any method to automate rollover or locking of keys. If keys are compromised/lost, they must be changed on every JUNOS device on which they are configured.
- Some SSH implementation support the use of X.509 PKI Certificates for managing SSH Keys, but JUNOS does not.
- Because of these limitations and the difficulty in auditing and managing SSH Keys on JUNOS devices, this method should not be used for Authentication of User logins or for the Root User.

Due to these limitations, it is recommended that SSH Key based Authentication be disabled when it is not required to support automation systems.

In some instances, such as when using PyEZ or NETCONF based automation over SSH, it may be preferable to authenticate a limited number of automation services using SSH Keys, rather than "hard coding" user details into scripts. Where this is the case, then this recommendation *should not be implemented* as it disables all use of SSH Key based Authentication.

When using SSH Keys for automation, it is imperative to have strong key management procedures in use to control and audit access to the Private Keys used and a process to allow for rollover and revocation of compromised keys. Consider using a Centralized SSH Key Management solution when trying to achieve this at scale.

Impact:

Ensure that SSH Key based Authentication is not required for automation systems and that any User Logins previously using SSH Keys have been configured with an alternative authentication methods before disabling SSH Key based Authentication.

Audit:

To confirm whether SSH Key based Authentication has been disabled, issue the following command from the `[edit system services ssh]` hierarchy:

```
[edit system services ssh]
user@host# show no-public-keys | count
```

The command should return a line count of 1.

Remediation:

To disable the use of SSH Key based Authentication, issue the following command from the `[edit system service ssh]` hierarchy:

```
[edit system services ssh]
user@host# set no-public-keys
```

Default Value:

SSH Key based authentication is supported, but no keys are configured by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-public-keys-edit-system-services.html
2. https://kb.juniper.net/InfoCenter/index?page=content&id=KB30588
3. https://www.ssh.com/ssh/key/

Additional Information:

The command to implement this was not introduced until JUNOS Version 15.1, which is later than the JTAC Recommended Release for some current platforms at the time of writing.

SSH Key based authentication may be required for some Automation systems.

Because of these caveats, this Recommendation is non-Scorable. However, where Automation is not used and the command is supported, it is highly recommended that SSH key based Authentication be disabled.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

6.10.2 Web-Management

Juniper devices may have the JWeb service installed to allow users to monitor and configure the device using a Web Browser based GUI.

Options for JWeb are set under `[edit system services web-management]` hierarchy and JWeb is enabled by default on some JUNOS platforms.

Only apply the recommendations in this section where the JWeb GUI is configured on the device.

You can confirm whether the JWeb service is configured by issuing the following command from the `[edit]` hierarchy in Configuration Mode:

```
[edit]

user@host# show system services | match "web-management {"
```

If the term "web-management {" is returned, all Recommendations in this section should be considered.

If management via JWeb, is not required the Web-Management service should be disabled using the following command:

```
[edit]

user@host# delete system services web-management
```

Note - Not all current JUNOS devices support JWeb web-management

6.10.2.1 Ensure Web-Management is not Set to HTTP (Automated)

Profile Applicability:

- Level 1

Description:

Network devices should not be managed using unencrypted HTTP sessions

Rationale:

JWeb can be configured to provide a Web GUI over either HTTP or HTTPS.

HTTP transmits all data (including passwords) in clear text over the network and provides no assurance of the identity of the hosts involved.

Because of this HTTP should never be used for sensitive tasks such as managing network devices or entering login credentials and HTTP Web-Management should be disabled.

Impact:

Ensure that management using HTTPS or other secure methods is configured and working before disabling HTTP access. Otherwise you may be unable to connect back to the device for management.

Audit:

From the command prompt, execute the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show  | match "http" | count
```

This should return a line count of 0.

Remediation:

To disable HTTP access issue the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#delete http
```

Default Value:

Varies by platform.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html
3. https://www.juniper.net/documentation/en_US/release-independent/junos/topics/task/configuration/ex-series-j-web-interface-starting.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.2.2 Ensure Web-Management is Set to use HTTPS (Automated)

Profile Applicability:

- Level 1

Description:

JWeb should only be accessed using HTTPS

Rationale:

JWeb can be configured to provide a Web GUI over either HTTP or HTTPS.

HTTP transmits all data (including passwords) in clear text over the network and provides no assurance of the identity of the hosts involved.

Because of this HTTP should never be used for sensitive tasks such as managing network devices or entering login credentials and HTTPS should be configured for Web-Management instead.

Impact:

Ensure an alternative method to manage the JUNOS device is configured and working prior to changing the Certificate used for HTTPS to ensure continued access in the event of any errors.

Audit:

To confirm if HTTPS is configured for Web-Management, enter the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show | match "https {" | count
```

The command should return a line count of 1.

Remediation:

To enable HTTPS access using the System Generated "Self Signed" Certificate, issue the following command from the `[edit system service web-management]` hierarchy;

```
[edit system services web-management]
user@host#set https system-generated-certificate
```

Alternatively, you may which to use a Local Certificate which is stored in the device's Configuration File:

```
[edit system services web-management]
user@host#set https local-certificate <Certificate Name>
```

<Certificate Name> should match an X.509 Certificate loaded under the `[edit security certificates]` hierarchy as shown below:

```
[edit security certificates]
user@host# set <Certificate Name> load-key-file <File Name/URL>
```

Where <File Name/URL> is either the name and path of a local Certificate and Key Pair file, or the URL from which the file can be fetched.
Note - This method leaves the Certificate and Private Key as part of the devices Configuration file, potentially exposing them. This is not the preferred method to configure a certificate in most instances.
Finally, you can configure JUNOS to use a PKI-Certificate:

```
[edit system services web-management]
user@host#set https pki-local-certificate <Certificate Name>
```

Where <Certificate Name> is an X.509 Certificate which has already been loaded to the JUNOS device's local PKI store.

Default Value:

Varies by platform. For some Branch and SME focused devices, like the SRX300 or EX2300, JWeb is enabled by default. For most larger Enterprise and SP devices JWeb is disabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
2. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.2.3 Ensure Web-Management is Set to use PKI Certificate for HTTPS (Automated)

Profile Applicability:

- Level 2

Description:

JWeb should only be accessed using HTTPS with a PKI Certificate

Rationale:

JWeb can be configured to provide a Web GUI over either HTTP or HTTPS.

When configured to use HTTPS X.509 Certificates are used to:

- Share Public Encryption Keys
- Provide Identity Information
- Validate the Web Server's Identity
- Enforce Encryption Key Rollover by limiting their validity period

JWeb can be configured to use Self Signed "System-Generated" X.509 Certificates, where the JUNOS device makes an identity claim, such as "I am myrouter.myorg.com", without any external validation. When an administrator connects to JWeb their browser will generate a Security Error due to this lack of validation, which the user will need to accept in order to proceed to the interface.

Without validation from a trusted Certificate Authority (CA), either an Internal or Public CA, administrators may be unable to detect when a management session is being intercepted or impersonated by an attacker. Additionally, a Self Signed certificate cannot be centrally revoked should a compromise be detected, relying instead on each user manually removing trust for the compromised Certificate.

A Certificate Authority is a Trusted Third Party which validates X.509 Certificates by signing them, using a secure Hashing algorithm and their own Private Key. A CA may be part of an organization's internal Public Key Infrastructure (PKI) or an Public CA service such as those provided by Verisign, Entrust or Microsoft.

Commonly, for signing Certificates used for internal management and systems, Organizations will configure their own PKI rather than paying for Public CA Services - configuring their End Points to trust Certificates signed by their CA through Group Policy or similar methods.

Either option is equally acceptable for use with JWeb, but Self Signed Certificates should not be used.

In addition, JUNOS offers two options for the storage and management of Certificates and their associated Private Keys:

- in the configuration under the `[edit security certificates]` hierarchy
- in a protected PKI store in memory

While the keys are hashed when stored in the configuration file, they are still exposed through backups and management access to the device. Storing Certificates and Keys in the device's PKI store means that the Private Keys are never accessible and that additional protections to this restricted area of memory can be used.

Due to these limitations PKI Certificates from a trusted Certificate Authority should always be used for JWeb Management and should always be stored in the device's PKI store rather than local configuration.

Impact:

Ensure an alternative method to manage the JUNOS device is configured and working prior to changing the Certificate used for HTTPS to ensure continued access in the event of any errors.

Audit:

To confirm if HTTPS for Web-Management is configured to use a PKI Certificate, enter the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show https | match "pki-local-certificate" | count
```

The command should return a line count of 1.

Remediation:

To configure Web-Management with a PKI Certificate issue the following command from the `[edit system service web-management]` hierarchy:

```
[edit system services web-management]
user@host# set https pki-local-certificate <Certificate ID>
```

Where <Certificate ID> is the name of a Certificate which has already been loaded to the devices PKI Store.

To create a new Public/Private Key Pair in the devices PKI Store and generate Certificate Signing Request issue the following commands from Operational Mode:

```
user@host> request security pki generate-key-pair certificate-id <Certificate
ID> type <Algorithm> size <Size>

user@host> request security pki generate-certificate-request certificate-id
<Certificate ID> domain-name <Device DNS Name> subject <Device Subject DN>
```

Where:

- <Certificate ID> is the Name that will be used for this Certificate throughout configuration
- <Algorithm> is the Encryption Algorithm to be used (this should be either RSA or ECC)
- <Size> is the number of Bits used for the keys (use at least 2048bits for RSA or 256bits for ECC)
- <Device DNS Name> is the FQDN which will be used to manage the device and
-<Device Subject DN> is the Distinguished Name used to identify this device and certificate.

Optionally, fields for email address, the device's IP Address and and output Filename for the PKCS#10 CSR which will be generated can be included.
The CSR should then be submitted to the Certificate Authority for review and signing.
Once the CA returns the Certificate it can be uploaded to the JUNOS device and imported with the following command from Operational Mode:

```
user@host> request security pki local-certificate load certificate-id
<Certificate ID> filename <File Upload Location>
```

Default Value:

Varies by platform. For some Branch and SME focused devices, like the SRX300 or EX2300, JWeb is enabled by default. For most larger Enterprise and SP devices JWeb is disabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html

Additional Information:

JUNOS Devices also support loading, auto-enrollment and management of X.509 Certificates using Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol v2 (CMPv2) enabled Certificate Authorities.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.2.4 Ensure Idle Timeout is Set for Web-Management (Automated)

Profile Applicability:

- Level 1

Description:

Idle JWeb sessions should be timed out after 15 minutes.

Rationale:

If JWeb Management sessions are left unattended it may be possible for an attacker to use the session to take control of the JUNOS device.

To prevent this, or at least limit the scope of such an attack, an idle timeout should be set to end sessions where no activity has occurred for a defined period of time.

The Payment Card Industry Data Security Standard (PCI DSS) recommends that administrative sessions should be timed out if left idle for 15 minutes.

Audit:

From the command prompt, execute the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show session idle-timeout
```

An integer value less than or equal to 15 should be returned, which is the Idle Timeout in Minutes.

Remediation:

To enable Idle Timeouts for JWeb issue the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#set session idle-timeout <Time in Minutes>
```

Default Value:

Depends on platform, JWEB is installed on J-Series by default and optional on all other platforms. No idle timeout is set by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 8.1.8
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.2.5 Ensure Session Limited is Set for Web-Management (Automated)

Profile Applicability:

- Level 1

Description:

Concurrent Web-Management sessions should be limited

Rationale:

JUNOS Devices can be managed through a powerful Web Management GUI called JWeb.

Operating the JWeb, or any other, management service uses resources on the device's Routing Engine (RE). An attacker may attempt to initialize a large number of management sessions concurrently in order to exhaust resources and achieve a Denial of Service (DoS) attack.

To prevent this the maximum number of concurrent JWeb sessions should be set at 5 or less.

Audit:

From the command prompt, execute the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show session session-limit
```

An integer value should be returned which represents the configured session limit. The value should be less than or equal to 5.

Remediation:

To enable Session limits for JWeb issue the following command from the `[edit system services web-management]` hierarchy;

```
[edit system services web-management]
user@host#set session-limit 5
```

Default Value:

Varies by platform. For some Branch and SME focused devices, like the SRX300 or EX2300, JWeb is enabled by default. For most larger Enterprise and SP devices JWeb is disabled by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.2.6 Ensure Web-Management Interface Restriction is Set (Automated)

Profile Applicability:

- Level 1

Description:

JWeb access should be restricted to trusted networks

Rationale:

By default, when configured, the JWeb service will listen for incoming connections on all interfaces which have an IP Address configured, exposing JWeb to users on all networks through which the device is reachable.

Because control of Network Systems can have a serious impact on the security of your environment, the JUNOS device should only be manageable over some of its interfaces; in particular a JUNOS device providing connectivity to untrusted networks such as the Internet should only be manageable from trusted sources.

This can be accomplished by limiting the interfaces on which the JWeb HTTPS service operates and this restriction should be applied on all JUNOS devices. Firewall Filters or Security Policy (SRX) should also be used to further restrict management to authorized sources (see Recommendations in Section 2 - Firewall for further details).

Impact:

Ensure that JWeb Management is operational and reachable using the selected interfaces before applying interface restrictions in a production environment.

Audit:

To confirm whether the JWeb Interface restrictions have been applied, execute the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show https interfaces
```

The configured Interface or Interfaces should be returned.

Remediation:

To apply JWEB Interface restrictions issue the following commands from the `[edit system services web-management https]` hierarchy:
To set a single Interface:

```
[edit system services web-management https]
user@host#set interface <interface>
```

Or to set multiple Interfaces:

```
[edit system services web-management https]
user@host#set interface [ <interface 1> <interface 2> <interface n> ]
```

Default Value:

Varies by platform. For some Branch and SME focused devices, like the SRX300 or EX2300, JWeb is enabled by default. For most larger Enterprise and SP devices JWeb is disabled by default.

When configured, by default JWeb listens on all interfaces for Web Management sessions.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html

Additional Information:

On SRX devices JWeb will only be accessible via interfaces/zones configured with `host-inbound-traffic system-services https` under the `[edit security zones security-zone <Zone Name>]` hierarchy. Both restrictions should still be applied and https should *only* be configured for zones where management traffic is required.

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

6.10.2.7 Ensure Web-Management Interface Restriction is set to OOB Management (Automated)

Profile Applicability:

- Level 2

Description:

JWeb access should be restricted to trusted networks

Rationale:

By default, when configured, the JWeb service will listen for incoming connections on all interfaces which have an IP Address configured, exposing JWeb to users on all networks through which the device is reachable.

Because control of Network Systems can have a serious impact on the security of your environment, the JUNOS device should only be manageable using Out Of Band (OOB) Management networks reached through the devices' dedicated Management Interface (called FXP0.0 on most platforms).

This can be accomplished by limiting the interfaces on which the JWeb HTTPS service operates to only include the devices' OOB Interface. Firewall Filters or Security Policy (SRX) should also be used to further restrict management to authorized sources (see Recommendations in Section 2 - Firewall for further details).

Some JUNOS devices do not have dedicated OOB Management ports. In some cases a "revenue port" can be configured to act as a Management port, such as by defining a "management" functional zone with a Branch/SME SRX Firewall. This type of restricted OOB Management Port is accepted as meeting this recommendation, but is not tested for under the audit procedure as a variety of ports might be used.

Impact:

Ensure that JWeb Management is operational and reachable using the selected interfaces before applying interface restrictions in a production environment.

Audit:

First confirm that JWeb Interface restrictions have been applied by executing the following command from the `[edit system services web-management]` hierarchy:

```
[edit system services web-management]
user@host#show https interfaces | count
```

A line count of 1 should be returned, confirming that Interface restrictions have been applied.

```
[edit system services web-management]
user@host#show https interfaces | display set | except "fxp0|em0|me0|jmgmt0"
| count
```

A line count of 0 should be returned.
Where a different dedicated OOB Management Port is used, such as with a Branch SRX using a management zone, the interface may be added to the `except` clause in the previous command when auditing this recommendation.

Remediation:

To apply JWEB Interface restrictions issue the following commands from the `[edit system services web-management https]` hierarchy:
To set a single Interface:

```
[edit system services web-management https]
user@host#set interface <interface>
```

Or to set multiple Interfaces:

```
[edit system services web-management https]
user@host#set interface [ <interface 1> <interface 2> <interface n> ]
```

Interfaces should only be fxp0.0, em0.0, me0.0 or jmgmt0.0 (dependent on platform) dedicated Out Of Band Management ports.

Default Value:

Varies by platform. For some Branch and SME focused devices, like the SRX300 or EX2300, JWeb is enabled by default. For most larger Enterprise and SP devices JWeb is disabled by default.

When configured, by default JWeb listens on all interfaces for Web Management sessions.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/system-edit-web-management.html
2. https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-understanding-management-ethernet-interfaces.html

Additional Information:

On SRX devices JWeb will only be accessible via interfaces/zones configured with `host-inbound-traffic system-services https` under the `[edit security zones security-zone <Zone Name>]` hierarchy.

Both restrictions should still be applied and https should *not* be configured for any Security Zones (although it is still acceptable in the Management Functional Zone used to provide an OOB Management Port for Branch/SME SRX Devices).

CIS Controls:

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

6.10.3 XNM-* (JUNOScript)

JUNOScript is a Juniper proprietary XML based Network Management (which is why it is configured under the slightly confusing XNM moniker) interface for JUNOS allowing custom applications to be created to configure, manage and monitor Juniper devices through Remote Procedure Calls (RPCs). It was used as the basis of several Juniper Network Management Systems and may still be used in some automation and management scripts.

JUNOScript was the basis for the open standard NETCONF API, which has largely replaced JUNOScript for most current Network Management Platforms or Automation Systems. Configuration options for NETCONF are covered elsewhere in this Benchmark.

Options for JUNOScript are configured under the `[edit system services xnm-plain-text]` and `[edit system services xnm-ssl]` hierarchies.

Only apply the recommendations in this section where JUNOScript is configured on the device.

You can confirm whether the JUNOScript service is configured by issuing the following command from the `[edit]` hierarchy in Configuration Mode:

```
[edit]

user@host# show system services | match "xnm-.*{ | count"
```

If a positive integer is return, all Recommendations in this section should be considered.

If you do not need to support legacy JUNOScript application, you should disable the service by issuing the following commands from the `[edit system services]` hierarchy:

```
[edit system services]

user@host# delete xnm-plain-text



[edit system services]

user@host# delete xnm-ssl
```

6.10.3.1 Ensure XNM-Clear-Text Service is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

Cleartext Management Services should be disabled.

Rationale:

JUNOScript Clients can access the router using a variety of transport modes including Clear-Text, Telnet, SSH and SSL.

When Clear-Text is used the JUNOScript Client connects to the JUNOS Device on port TCP/3221.

As the name suggests Authentication information, commands and router configuration are all transported across the network in Clear (unencrypted) Text form, making it trivial for an attacker to steal login credentials, learn configuration or hijack the session to execute their own commands.

Because of this, Clear Text mode should *never* be used to manage JUNOS Devices.

Impact:

Ensure that JUNOSCript Clients using the Clear Text interface are not being used to manage the JUNOS Device before disabling the service in a production environment.

Audit:

To confirm whether Clear Text JUNOScript is configured, issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show services | match xnm-clear-text | count
```

The above command should return a line count of 0.

Remediation:

The XNM-Clear-Text service is not enabled by default, however if it has been configured on your router it can by disabled by issuing the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#delete services xnm-clear-text
```

Default Value:

The XNM-Clear-Text Service is disabled by default and cannot be enabled on JUNOS FIPS Mode.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
2. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/junos-xml-management-protocol/junos-xml-management-protocol.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.3.2 Ensure XNM-SSL Connection Limit is Set (Automated)

Profile Applicability:

- Level 2

Description:

If the XNM-SSL service is configured, connection limits should be set.

Rationale:

JUNOScript can be configured to use SSL transport to prevent the exposure of sensitive data and authentication details on the network. If configured the XNM-SSL service will provide services on port TCP/3220.

An attacker may attempt to open a large number of sessions to the XNM-SSL service to exhaust the routers resources or an authorized user may do so accidently, especially given that the service is designed to allow a scripting and automation interface to JUNOS. To limit the impact of any such incident, the number of concurrent connections to the XNM-SSL service should explicitly limited.

A relatively low value of 10 is recommended, but may not be appropriate for all environments so it is left to the administrator's discretion.

Impact:

If the connection limit has been reached, additional JUNOScript sessions will be rejected until an existing session has ended.

Audit:

To confirm whether a JUNOScript SSL Session Limit has been configured, enter the following command at the `[edit system services xnm-ssl]` hierarchy:

```
[edit system services xnm-ssl]
user@host#show connection-limit
```

The above command should return a positive integer, the number of permitted concurrent connections, if configured.

Remediation:

The XNM-SSL Connection Limit can be configured by issuing the following command from the [edit system services xnm-ssl] hierarchy;

```
[edit system services xnm-ssl]
user@host#set connection-limit <limit>
```

Where <limit> is the permitted number of concurrent connections required.

Default Value:

The XNM-SSL Service is disabled by default.

When it is first configured the default Connection Limit is 75.

References:

1. Configuring SSL Service for JUNOScript Client Applications, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-ssl-service-for-junoscript-client-applications.html)
2. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/junos-xml-management-protocol/junos-xml-management-protocol.html

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.3.3 Ensure XNM-SSL Rate Limit is Set (Automated)

Profile Applicability:

- Level 2

Description:

If the XNM-SSL service is configured, the Rate Limit should be set.

Rationale:

JUNOScript can be configured to use SSL transport to prevent the exposure of sensitive data and authentication details on the network. If configured the XNM-SSL service will provide services on port TCP/3220.

An attacker may attempt to open a large number of sessions to the XNM-SSL service to exhaust the routers resources or an authorized user may do so accidently, especially given that the service is designed to allow a scripting interface to JUNOS.

To limit the impact of any such incident, the rate at which new connections to the XNM-SSL service should explicitly limited. Rate Limits are set in terms of the number of connection attempts per minute. Established connections do not count towards this count. A relatively low value of 60 (the equivalent of one attempt per second, sustained over a minute) is recommended, but may not be appropriate for all environments so it is left to the administrator's discretion.

Impact:

If the Rate Limit is exceeded, new connection attempts will be rejected until the new connection rate drops below the configured limit.

Audit:

To confirm if an JUNOScript SSL Rate Limit is applied, enter the following command at the `[edit system services xnm-ssl]` hierarchy:

```
[edit system services xnm-ssl]
user@host#show rate-limit
```

The above command should return a positive integer, which is the Rate Limit in Connection Attempts per Minute.

Remediation:

The XNM-SSL Rate Limit can be configured by issuing the following command from the `[edit system services xnm-ssl]` hierarchy;

```
[edit system services xnm-ssl]
user@host#set rate-limit <limit>
```

Where <limit> is the desired Rate Limit measured in Connection Attempts per Minute.

Default Value:

The XNM-SSL Service is disabled by default. When it is first configured the default Rate Limit is 150 connection attempts per second.

References:

1. Configuring SSL Service for JUNOScript Client Applications, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-ssl-service-for-junoscript-client-applications.html)
2. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/junos-xml-management-protocol/junos-xml-management-protocol.html

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.3.4 Ensure XNM-SSL SSLv3 Support is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

If the XNM-SSL service is configured, SSLv3 should not be enabled.

Rationale:

JUNOScript can be configured to use SSL/TLS transport to prevent the exposure of sensitive data and authentication details on the network. If configured the XNM-SSL service will provide services on port TCP/3220.

Secure Sockets Layer version 3 (SSLv3) is an old standard for securing communication, which has proved vulnerable to a number of systemic weaknesses and is now considered unsuitable for use for securing sensitive sessions, such as those used by JUNOScript. SSLv3 has been replaced by the Transport Layer Security (TLS) standard.

Although support for SSLv3 has been disabled by in most JUNOS Releases, it is still possible to enable support for SSLv3 using a hidden configuration command in some currently supported versions of JUNOS.

Because this would enable a significantly weaker standard, it is strongly recommended that SSLv3 Support should never be enabled.

Impact:

If a JUNOScript client does not support the newer TLS standard, it will be unable to connect to the JUNOS Device.

Audit:

To confirm whether a JUNOScript SSLv3 Support has been configured, enter the following command at the `[edit system services xnm-ssl]` hierarchy:

```
[edit system services xnm-ssl]
user@host#show sslv3-support | count
```

The above command should return a line count of 0.

Remediation:

XNM-SSL SSLv3 Support can be disabled by issuing the following command from the [edit system services xnm-ssl] hierarchy;

```
[edit system services xnm-ssl]
user@host#delete sslv3-support
```

Default Value:

The XNM-SSL Service is disabled by default.

SSLv3 was disabled by default in Junos OS 13.2R8, 13.3R6, 14.1R5, 14.2R3 (depending on platform). Support for the SSLv3-support command was removed in JUNOS Version 15.1

References:

1. Configuring SSL Service for JUNOScript Client Applications, JUNOS 9.3 System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/software/junos/junos93/swconfig-system-basics/configuring-ssl-service-for-junoscript-client-applications.html)
2. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/junos-xml-management-protocol/junos-xml-management-protocol.html
3. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10656

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.4 NETCONF

The Network Configuration Protocol (NETCONF) is an open standards based service for Remote Administration and Automation of Network Devices which was developed from Juniper's proprietary JUNOScript API (see Section 6.10.3 XNM-* (JUNOScript)).

NETCONF uses XML based configuration to trigger Remote Procedure Calls (RPCs) on the Network Device and is defined in RFC6241 and the service is configured under the `[edit system services netconf]` hierarchy.

Remote NETCONF sessions to JUNOS Devices use SSH for Secure Transport on TCP/830 (by default), based on the RFC4742 NETCONF-over-SSH standard. NETCONF can also be configured to use Reverse SSH, whereby the JUNOS Device initiates the SSH connection to the NETCONF Configuration Server rather than the other way around.

When configured for NETCONF-over-SSH, the configuration for SSH Version, Ciphers, MACs and related options set under the `[edit system services ssh]` hierarchy apply and, by default, the NETCONF protocol is available on the standard SSH port (TCP/22) as well as the NETCONF-over-SSH port (TCP/830). If NETCONF-over-SSH is configured all configuration items from Section 6.10.1 SSH should also be applied.

NETCONF is not enabled on JUNOS Devices by default. Only apply the recommendations in this section where NETCONF is configured on the device.

You can confirm whether the NETCONF service is configured by issuing the following command from the `[edit]` hierarchy in Configuration Mode:

```
[edit]

user@host# show system services | match "netconf \{|netconf\;" | count
```

If a line count of 1 or higher is return, NETCONF is enabled on your system and you should apply all recommendations in this section.

If NETCONF is not required, the NETCONF service should be disabled using the following command:

```
[edit]

user@host# delete system services netconf
```

6.10.4.1 Ensure NETCONF Rate Limit is Set (Automated)

Profile Applicability:

- Level 1

Description:

If the NETCONF service is configured, the Rate Limit should be set.

Rationale:

NETCONF can be configured to use SSH transport to allow remote access while preventing the exposure of sensitive data and authentication details on the network. If configured, the NETCONF-over-SSH service will provide services on port TCP/830.

An attacker may attempt to open a large number of sessions to the NETCONF-over-SSH service to exhaust the routers resources or an authorized user may do so accidently, especially given that the service is designed to allow an automation interface to JUNOS.

To limit the impact of any such incident, the rate of new connections to the NETCONF service should explicitly limited. Rate Limits are set in terms of the number of new connection attempts per minute. Established connections do not count towards this count. A relatively low value of 60 (the equivalent of one attempt per second, sustained over a minute) is recommended, but may not be appropriate for all environments so it is left to the administrator's discretion.

Impact:

If the Rate Limit is exceeded, new connection attempts will be rejected until the new connection rate drops below the configured limit.

Audit:

To confirm whether the NETCONF-over-SSH Rate Limit has been set, issue the following command from the `[edit system services netconf]` hierarchy:

```
[edit system services netconf]
user@host# show ssh rate-limit
```

This should return the configured Rate Limit in New Connection Attempts per Minute.

Remediation:

The NETCONF-over-SSH Rate Limit can be configured by issuing the following command from the `[edit system services netconf]` hierarchy;

```
[edit system services netconf]
user@host#set ssh rate-limit <limit>
```

Where is the desired Rate Limit measured in New Connection Attempts per Minute.

Default Value:

The NETCONF-over-SSH Service is disabled by default. When it is first configured the default Rate Limit is 150 connection attempts per second.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/rate-limit-edit-system.html

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.4.2 Ensure NETCONF Connection Limit is Set (Automated)

Profile Applicability:

- Level 1

Description:

If the NETCONF service is configured, the Connection Limit should be set.

Rationale:

NETCONF can be configured to use SSH transport to allow remote access while preventing the exposure of sensitive data and authentication details on the network. If configured, the NETCONF-over-SSH service will provide services on port TCP/830.

An attacker may attempt to open a large number of sessions to the NETCONF-over-SSH service to exhaust the routers resources or an authorized user may do so accidently, especially given that the service is designed to allow an automation interface to JUNOS.

To limit the impact of any such incident, the number of concurrent connections to the NETCONF service should explicitly limited.

A relatively low value of 10 is recommended, but may not be appropriate for all environments so it is left to the administrator's discretion.

Impact:

If the connection limit has been reached, additional NETCONF-over-SSH sessions will be rejected until an existing session has ended.

Audit:

To confirm whether the NETCONF-over-SSH Connection Limit has been set, issue the following command from the `[edit system services netconf]` hierarchy:

```
[edit system services netconf]
user@host# show ssh connection-limit | count
```

A line count of 1 should be returned if the Connection Limit is set.

Remediation:

The NETCONF-over-SSH Connection Limit can be configured by issuing the following command from the `[edit system services netconf]` hierarchy;

```
[edit system services netconf]
user@host#set ssh connection-limit <limit>
```

Where <limit> is the desired Connection Limit.

Default Value:

The NETCONF-over-SSH Service is disabled by default. When it is first configured the default Connection Limit is 75.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/connection-limit-edit-system.html
2. https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/netconf-guide/netconf.html

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5 REST

The Representational State Transfer Application Programming Interface or REST API is a service for Remote Administration and Automation of Juniper Network Devices. Details of the API can be found here:
https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/rest-api/rest-api.html

The JUNOS REST API allows a Remote Administrator or Automation System to queries and configure the JUNOS Device by sending HTTP GET and POST commands to trigger NETCONF RPCs over HTTP (port TCP/3000) or HTTPS (TCP/3443) transport. The REST API also supports an interactive REST API Explorer web interface.

REST API is not enabled on JUNOS Devices by default. Only apply the recommendations in this section where REST is configured on the device.

You can confirm whether the REST API service is configured by issuing the following command from the `[edit]` hierarchy in Configuration Mode:

```
[edit]

user@host# show system services | match "rest \{|rest\;" | count
```

If a line count of 1 or higher is return, the REST API is enabled on your system and you should apply all recommendations in this section.

If REST API is not required, the service should be disabled using the following command:

```
[edit]

user@host# delete system services rest
```

6.10.5.1 Ensure REST is Not Set to HTTP (Automated)

Profile Applicability:

- Level 1

Description:

Network devices should not be managed using unencrypted HTTP sessions

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

HTTP transmits all data (including passwords) in clear text over the network and provides no assurance of the identity of the hosts involved.

Because of this HTTP should never be used for sensitive tasks such as managing network devices or entering login credentials; so REST HTTP should always be disabled.

Impact:

Management of the device through REST HTTP will be lost - ensure that other management options are configured and working before disabling this service on production systems.

Audit:

To check whether REST HTTP is configured, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show http | count
```

If the command returns a line count of 1 or greater, then REST HTTP is enabled.

Remediation:

To disable REST HTTP, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# delete http
```

Default Value:

By default the REST API is disabled.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/http-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.2 Ensure REST is Set to HTTPS (Automated)

Profile Applicability:

- Level 1

Description:

The REST API should only be accessed using HTTPS

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

HTTP transmits all data (including passwords) in clear text over the network and provides no assurance of the identity of the hosts involved.

Because of this HTTP should never be used for sensitive tasks such as managing network devices or entering login credentials and HTTPS transport used whenever the REST API is configured.

When configuring HTTPS, a `Server Certificate` in the Device's PKI Store is required. This can be either a "Self Signed Certificate" or a Certificate issued by a configured/supported Certificate Authority (including internal CAs). A Certificate issues from a CA is preferred.

Audit:

To check whether REST HTTPS is configured, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https | count
```

If the command returns a line count of 1 or greater, then REST HTTPS is enabled.

Remediation:

To configure REST over HTTPS, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https server-certificate <Certificate ID>
```

Where <Certificate ID> is the name of a Certificate which has already been loaded to the devices PKI Store.

To create a new Public/Private Key Pair in the devices PKI Store and generate Certificate Signing Request issue the following commands from Operational Mode:

```
user@host> request security pki generate-key-pair certificate-id <Certificate
ID> type <Algorithm> size <Size>

user@host> request security pki generate-certificate-request certificate-id
<Certificate ID> domain-name <Device DNS Name> subject <Device Subject DN>
```

Where:

<Certificate ID> is the Name that will be used for this Certificate throughout configuration

<Algorithm> is the Encryption Algorithm to be used (this should be either RSA or ECC)

<Size> is the number of Bits used for the keys (use at least 2048bits for RSA or 256bits for ECC)

<Device DNS Name> is the FQDN which will be used to manage the device and <Device Subject DN> is the Distinguished Name used to identify this device and certificate.

Optionally, fields for email address, the device's IP Address and output Filename for the PKCS#10 CSR which will be generated can be included.

The CSR should then be submitted to the Certificate Authority for review and signing.

Once the CA returns the Certificate it can be uploaded to the JUNOS device and imported with the following command from Operational Mode:

```
user@host> request security pki local-certificate load certificate-id
<Certificate ID> filename <File Upload Location>
```

Alternatively, a "Self Signed" Certificate can be generated using the Public/Private Key Pair previously generated with the following command:

```
user@host> request security pki local-certificate generate-self-signed
certificate-id <Certificate ID>
```

Use of Self Signed Certificates is not recommended in secure environments.

Default Value:

By default the REST API is disabled.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html

3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html
4. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html

Additional Information:

JUNOS Devices also support loading, auto-enrollment and management of X.509 Certificates using Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol v2 (CMPv2) enabled Certificate Authorities.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.3 Ensure REST is Set to use PKI Certificate for HTTPS (Automated)

Profile Applicability:

- Level 2

Description:

The REST API should only be accessed using HTTPS with a PKI Certificate

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

When configured to use HTTPS X.509 Certificates are used to:

- Share Public Encryption Keys
- Provide Identity Information
- Validate the Web Server's Identity
- Enforce Encryption Key Rollover by limiting their validity period

JWeb can be configured to use Self Signed "System-Generated" X.509 Certificates, where the JUNOS device makes an identity claim, such as "I am myrouter.myorg.com", without any external validation. When an administrator connects to JWeb their browser will generate a Security Error due to this lack of validation, which the user will need to accept in order to proceed to the interface.

Without validation from a trusted Certificate Authority (CA), either an Internal or Public CA, administrators may be unable to detect when a management session is being intercepted or impersonated by an attacker. Additionally, a Self Signed certificate cannot be centrally revoked should a compromise be detected, relying instead on each user manually removing trust for the compromised Certificate.

A Certificate Authority is a Trusted Third Party which validates X.509 Certificates by signing them, using a secure Hashing algorithm and their own Private Key. A CA may be part of an organization's internal Public Key Infrastructure (PKI) or a Public CA service such as those provided by Verisign, Entrust or Microsoft.

Commonly, for signing Certificates used for internal management and systems, Organizations will configure their own PKI rather than paying for Public CA Services - configuring their End Points to trust Certificates signed by their CA through Group Policy or similar methods.

Either option is equally acceptable for use with JWeb, but Self Signed Certificates should not be used.

Impact:

REST API Management may be lost if the Certificate is not valid or issued from a Certificate Authority which the Network Management/Automation Systems are not configured to trust.

Audit:

To check whether REST HTTPS is configured to use a Self Signed Certificate, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https server-certificate
```

This should return the <Certificate ID> that the REST HTTPS is configured to use.
Next we confirm that the configured Certificate is loaded in the devices' PKI Store:

```
[edit system services rest]
user@host# run show security pki local-certificate certificate-id
<Certificate ID>
```

If information on the Certificate's issuer, Validity Period and Algorithm are displayed, then the Certificate has been install.
Finally, confirm that a Certificate Signing Request (CSR) exists for the configured <Certificate ID> by issuing the following command:

```
[edit system services rest]
user@host# run show security pki certificate-request certificate-id
<Certificate ID>
```

If the Certificate has been requested from an external Certificate Authority, a CSR will be returned. Otherwise the following will be returned:

```
Certificate identifier: <Certificate ID>
  Certificate request not present
```

This indicates that a Self Signed Certificate is being used, which should be replaced with a Certificate issued by a trusted CA.

Remediation:

To configure REST over HTTPS, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https server-certificate <Certificate ID>
```

Where <Certificate ID> is the name of a Certificate which has already been loaded to the devices PKI Store.
To create a new Public/Private Key Pair in the devices PKI Store and generate Certificate Signing Request issue the following commands from Operational Mode:

```
user@host> request security pki generate-key-pair certificate-id <Certificate
ID> type <Algorithm> size <Size>

user@host> request security pki generate-certificate-request certificate-id
<Certificate ID> domain-name <Device DNS Name> subject <Device Subject DN>
```

Where:
<Certificate ID> is the Name that will be used for this Certificate throughout configuration
<Algorithm> is the Encryption Algorithm to be used (this should be either RSA or ECDSA)
<Size> is the number of Bits used for the keys (use at least 2048bits for RSA or 256bits for ECDSA)
<Device DNS Name> is the FQDN which will be used to manage the device and <Device Subject DN> is the Distinguished Name used to identify this device and certificate.
Optionally, fields for email address, the device's IP Address and output Filename for the PKCS#10 CSR which will be generated can be included.
The CSR should then be submitted to the Certificate Authority for review and signing.
Once the CA returns the Certificate it can be uploaded to the JUNOS device and imported with the following command from Operational Mode:

```
user@host> request security pki local-certificate load certificate-id
<Certificate ID> filename <File Upload Location>
```

Default Value:

By default the REST API is disabled.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html
4. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html

Additional Information:

JUNOS Devices also support loading, auto-enrollment and management of X.509 Certificates using Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol v2 (CMPv2) enabled Certificate Authorities.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.4 Ensure REST HTTPS is Set to use Mutual Authentication (Automated)

Profile Applicability:

- Level 2

Description:

The REST HTTPS API should be configured for Mutual Authentication

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

When configured to use HTTPS, X.509 Certificates are used to validate the JUNOS Devices identity to API Clients when they connect. Optionally, TLS Mutual Authentication may also be configured, whereby the REST API Client must also provide an X.509 Certificate signed by a mutually trusted Certificate Authority before it is permitted to connect.

Using a mutually trusted Certificate Authority (CA), either an Internal or Public CA, allows for both the Client Device (such as a Network Automation Server) and JUNOS Device to detect when a management session is being intercepted or impersonated by an attacker. Additionally, a centralized CA is able to revoke any Certificate's which may be compromised or have been issued to Clients who are no longer authorized.

A Certificate Authority is a Trusted Third Party which validates X.509 Certificates by signing them, using a secure Hashing algorithm and their own Private Key. A CA may be part of an organization's internal Public Key Infrastructure (PKI) or an Public CA service such as those provided by Verisign, Entrust or Microsoft.

Commonly, for signing Certificates used for internal management and systems, Organizations will configure their own PKI rather than paying for Public CA Services - configuring their End Points to trust Certificates signed by their CA through Group Policy or similar methods.

Either option is equally acceptable for use REST TLS Mutual Authentication, but a `ca-profile` must be configured on the JUNOS Device (even where the device has preconfigured trust for some Public CAs).

TLS/HTTPS Mutual Authentication does not replace User Authentication, which is still performed via an HTTP Authentication Header using details configured Local or Remote (via RADIUS/TACACS+) User.

Impact:

REST API Management may be lost if the Certificate is not valid or if Automation/Network Management Systems using the REST API are not also configured to support Mutual Authentication using valid Certificates from the same Certificate Authority.

Audit:

To check whether REST HTTPS is configured to require Mutual Authentication, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https mutual-authentication
```

If Mutual Authentication is configured, this command should return <CA Profile>, which is the name of the Certificate Authority Profile configured on the JUNOS Device and used for Mutual Authentication.
Then confirm that the configured CA is present on the JUNOS Device and associated with a CA-Certificate:

```
[edit system services rest]
user@host# run show security pki ca-certificate ca-profile <CA Profile>
```

Ensure that the details of the returned CA Certificate match those of the Certificate Authority that you trust and intend to use for this purpose.

Remediation:

To configure REST HTTPS Mutual Authentication, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https mutual-authentication <CA Profile>
```

Where <CA Profile> is the name of an existing Certificate Authority Profile configured on the JUNOS Device for a Trusted CA.
To configure a new CA Profile, use the following commands from the `[edit security pki]` hierarchy:

```
[edit security pki]
user@host# set ca-profile <CA Profile> ca-identity <CA ID>
```

It is recommended that a Certificate Revocation List be set for the CA Profile, by including the <CRL URL> using the following command:

```
[edit security pki]
user@host# set ca-profile <CA Profile> revocation-check crl <CRL URL>
```

Finally, the CAs' Public Certificate should be obtained an uploaded to the JUNOS Device and linked to the CA Profile:

```
[edit security pki]
user@host# run request security pki ca-certificate load ca-profile <CA
Profile> filename <path and filename>
```

Default Value:

By default the REST API is disabled.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html
4. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html

Additional Information:

JUNOS Devices also support loading, auto-enrollment and management of X.509 Certificates using Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol v2 (CMPv2) enabled Certificate Authorities.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.5 Ensure REST HTTPS Cipher List is Set (Automated)

Profile Applicability:

- Level 1

Description:

The REST API should only be accessed using HTTPS with secure Cipher Suites.

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

When configured to use HTTPS, the device supports a wide range of Cipher Suites which define the Encryption, Hashing and Key Exchange methods and algorithms. By default, in the interests of compatibility, this includes support for a number of older, weaker algorithms such as RC4 Encryption or MD5 Hashing, which are no longer considered suitable for protecting sensitive data or device management.

To ensure that these weaker algorithms and methods are not used, the REST API HTTPS Service should be configured to use only Cipher Suites which do not include RC4 or 3DES for Data Encryption and MD5 or SHA1 for Hashing.

Impact:

REST API Management may be lost if the Network Management System or Hosts do not support the secure Cipher Suites.

Audit:

To check whether REST HTTPS is configured to use insecure Cipher Suites, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https cipher-suites | match "rc4|3des|md5|sha" | exclude
"sha256|sha384" | count
```

A line count of 0 should be returned if no insecure Cipher Suites are configured.

Remediation:

To restrict the Cipher Suites used REST over HTTPS, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https cipher-list [ rsa-with-aes-128-cbc-SHA256 rsa-with-aes-
256-cbc-SHA256 dhe-rsa-with-aes-128-cbc-SHA256 dhe-rsa-with-aes-256-cbc-
SHA256 rsa-with-aes-128-gcm-SHA256 rsa-with-aes-256-gcm-SHA384 dhe-rsa-with-
aes-128-gcm-SHA256 dhe-rsa-with-aes-256-gcm-SHA384 ecdhe-rsa-with-aes-128-
cbc-SHA256 ecdhe-rsa-with-aes-256-cbc-SHA384 ecdhe-rsa-with-aes-128-gcm-
SHA256 ecdhe-rsa-with-aes-256-gcm-SHA384 ]
```

No all Cipher Suites are required to meet this recommendation. A shorter list, or individual Cipher Suites, may be configured using the same command.
Some JUNOS Devices do not support all of the above Cipher Suite (most notably, AES in Galois Counter Mode support is not universal), unsupported Cipher Suites can be skipped.

Default Value:

By default the REST API is disabled. When the REST API HTTPS Service is enabled, all Cipher Suites (including those with RC4 and insecure ciphers) are accepted, except for JUNOS FIPS mode, which supports *only* `rsa-with-aes-256-gcm-SHA384`, `dhe-rsa-with-aes-128-gcm-SHA256`, `dhe-rsa-with-aes-256-gcm-SHA384`, `ecdhe-rsa-with-aes-128-gcm` and `ecdhe-rsa-with-aes-256-gcm`.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html
4. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/cipher-list-edit-system-services-rest-https.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.6 Ensure REST HTTPS Cipher List is Set to Suite B Only (Automated)

Profile Applicability:

- Level 2

Description:

The REST API should only be accessed using HTTPS with secure Cipher Suites.

Rationale:

The JUNOS REST API can be configured for access using either HTTP or HTTPS for connections.

When configured to use HTTPS, the device supports a wide range of Cipher Suites which define the Encryption, Hashing and Key Exchange methods and algorithms. By default, in the interests of compatibility, this includes support for a number of older, weaker algorithms such as RC4 Encryption or MD5 Hashing, which are no longer considered suitable for protecting sensitive data or device management.

In Secure Environments, the REST API HTTPS Service should be configured to accept only Cipher Suites listed in the National Security Agencies Suite B Standards.

Suite B standards for Cryptographic functions are developed and distributed by the US National Security Agency as part of Cryptographic Modernization Program for protection of US Government data, both unclassified and classified (to Secret). The Suite B Profile for Transport Layer Security (TLS) is set in RFC6460 and specifies two acceptable Profiles using ECDH with standard NIST Elliptic Curves, AES in Galois Counter Mode and SHA2.

Impact:

REST API Management may be lost if the Network Management System or Hosts do not support the secure Cipher Suites.

Audit:

To check whether REST HTTPS is configured to use insecure Cipher Suites, enter the following command from the `[edit system services rest]` hierarchy:
First, confirm that the two accepted Cipher Suites are configured

```
[edit system services rest]
user@host# show https cipher-suites | display set | match "ecdhe-rsa-with-
aes-128-gcm-SHA256|ecdhe-rsa-with-aes-256-gcm-SHA384" | count
```

A line count of 1 or 2 should be returned if one or both of the acceptable Suites are configured.
Then, confirm that no other Cipher Suites are permitted.

```
[edit system services rest]
user@host# show https cipher-suites | display set | exclude "ecdhe-rsa-with-
aes-128-gcm-SHA256|ecdhe-rsa-with-aes-256-gcm-SHA384" | count
```

A line count of 0 should be returned if no other Cipher Suites are configured.

Remediation:

To restrict the Cipher Suites used REST over HTTPS, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https cipher-list [ ecdhe-rsa-with-aes-128-gcm-SHA256 ecdhe-
rsa-with-aes-256-gcm-SHA384 ]
```

Either Cipher Suite may be omitted, but *at least* one of these Cipher Suites *must* be set. No other Cipher Suites may be used.

Default Value:

By default the REST API is disabled. When the REST API HTTPS Service is enabled, all Cipher Suites (including those with RC4 and insecure ciphers) are accepted, except for JUNOS FIPS mode, which supports *only* `rsa-with-aes-256-gcm-SHA384`, `dhe-rsa-with-aes-128-gcm-SHA256`, `dhe-rsa-with-aes-256-gcm-SHA384`, `ecdhe-rsa-with-aes-128-gcm` and `ecdhe-rsa-with-aes-256-gcm`.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html
4. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/cipher-list-edit-system-services-rest-https.html

Additional Information:

Not all JUNOS Devices support AES in Galois Counter Mode, which is required for compliance with FIPS and SUite B Standards.

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.5.7 Ensure REST API Explorer is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

The REST API Explorer should be disabled

Rationale:

When enabled, the JUNOS REST API can provide a Web GUI interface known as the REST API Explorer to allow developers to learn the API or test RPC calls.

The API Explorer is not designed for use in production environments and adds an unnecessary additional attack surface which could be exploited to compromise the JUNOS Device.

Because it is an unneeded service, intended for use only in development environments, the API Explorer should be disabled on all production systems.

Impact:

The REST API Explorer should only be used in Development or Lab environments, it is not required in order to support normal REST API functionality.

Audit:

To confirm whether the REST API Explorer is enabled, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show enable-explorer | count
```

If a line count of 1 is returned, the API Explorer is enabled.

Remediation:

To disable the REST API Explorer, issue the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# delete enable-explorer
```

This will disable the API Explorer for both HTTP and HTTPS access.

Default Value:

The REST API is disabled by default. If REST is enabled, the API Explorer is disabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 1.1.6
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/enable-explorer-edit-system-services-rest.html
3. https://www.juniper.net/documentation/en_US/junos/topics/example/rest-api-explorer-example.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.10.5.8 Ensure REST Allowed Sources is Set (Automated)

Profile Applicability:

- Level 1

Description:

REST API Clients should be restricted to allowed sources.

Rationale:

The REST API service allows remote scripts or users to connect to a JUNOS Device and execute RPC commands to operate and configure the device, potentially granting full control if connecting using a privileged account.

To protect the REST API from unauthorized use, access should be restricted to specific Network Management Systems using the `allowed-sources` option to add a whitelist of one or more individual IP Addresses.

Impact:

Hosts which are not included in the Allowed Sources whitelist will no longer be permitted to access the REST API.

Audit:

To confirm if Allowed Sources are configured for the REST API, enter the following command at the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show control allowed-sources
```

The command should return a list of one, or more, IP Addresses which are permitted to access the JUNOS Device using the REST API service.

Remediation:

To add an IP Address to the REST API Allowed Sources whitelist, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set control allowed-sources <Source IP>
```

Where <Source IP> is a single host IP Address.
To add multiple addresses to the Allowed Sources whitelist, enter the following command:

```
[edit system services rest]
user@host# set control allowed-sources [<Source IP 1> <Source IP 2> <Source
IP ...> ]
```

To remove a single address from the current list (for example, if the host is no longer used for Network Management) enter the following command:

```
[edit system services rest]
user@host# delete control allowed-sources <Source IP>
```

Default Value:

By default the REST API is disabled.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html

Additional Information:

Filtering of Source Addresses is applied on the Routing Engine by the REST API Service and not on the PFE. This recommendation is considered an additional line of defence, but a "Protect RE" filter should be configured under the `[edit firewall]` hierarchy and applied to the device's `lo0.0` interface.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.10.5.9 Ensure REST Connection Limit is Set (Automated)

Profile Applicability:

- Level 1

Description:

If the REST API service is configured, the Connection Limit should be set.

Rationale:

The REST API may be accessed remotely, using either HTTP (though this is not recommended) or HTTPS.

An attacker may attempt to open a large number of sessions to the REST API service to exhaust the routers resources or an authorized user may do so accidently, especially given that the service is designed to allow an automation interface to JUNOS.

To limit the impact of any such incident, the number of concurrent connections to the REST API service should explicitly limited.

A relatively low value of 10 is recommended, but may not be appropriate for all environments so it is left to the administrator's discretion.

Impact:

If the connection limit has been reached, additional REST API sessions will be rejected until an existing session has ended.

Audit:

To confirm whether a Connection Limit has been set for the REST API, enter the following command at the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show control connection-limit | count
```

The command should return a line count of 1 if the Connection Limit has been set.

Remediation:

To enable a REST API Connection Limit, enter the following command at the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set control connection-limit <limit>
```

Where <limit> is the desired Connection Limit.

Default Value:

The REST API Service is disabled by default. When enabled, the default Connection Limit for most platforms is 64.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/connection-limit-edit-system-services-rest.html
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html

Additional Information:

Some devices, support only 8 (SRX300/320) or 16 (SRX34x/550) concurrent connections.

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

6.10.5.10 Ensure REST Service Address is Set (Automated)

Profile Applicability:

- Level 1

Description:

The REST API Service Address should be set.

Rationale:

The REST API service allows remote scripts or users to connect to a JUNOS Device and execute RPC commands to operate and configure the device, potentially granting full control if connecting using a privileged account.

To protect the REST API from unauthorized use, access should be restricted to specific network management segments.

By default, when enabled, the REST API listens on port TCP/3000 (for HTTP) or TCP/3443 (for HTTPS) on all IP Addresses configured on the JUNOS Device. The `addresses` option can be configured with one or more IP Addresses to restrict the REST API to listening only on these addresses.

In general, this would be the IP Address used for the devices' Out of Band Management interface (such as fxp0) where possible.

Impact:

Hosts will be unable to connect to the REST API HTTPS Service on any addresses which are not configured.

Audit:

To confirm if the REST API's Service Address has been limited, enter the following command at the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https addresses
```

The command should return a list of one, or more, IP Addresses which if configured on Interfaces will be used for the REST API HTTPS Service.

Remediation:

To restrict the IP Address/es on which the REST API will listen, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https addresses <Service IP>
```

Where <Service IP> is a single IP Address configured on one of the JUNOS Device's interfaces.
To add multiple addresses, enter the following command:

```
[edit system services rest]
user@host# set https addresses [<Service IP 1> <Service IP 2> <Service IP
...> ]
```

To remove a single address from the current list enter the following command:

```
[edit system services rest]
user@host# delete https addresses <Service IP>
```

Default Value:

By default the REST API is disabled. When enabled, the REST API HTTPS Service listens on all configured IP Addresses.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html

CIS Controls:

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.10.5.11 Ensure REST Service Address is Set to OOB Management Only (Automated)

Profile Applicability:

- Level 2

Description:

The REST API Service Address should be set to OOB Management.

Rationale:

The REST API service allows remote scripts or users to connect to a JUNOS Device and execute RPC commands to operate and configure the device, potentially granting full control if connecting using a privileged account.

To protect the REST API from unauthorized use, access should be restricted to specific network management segments.

By default, when enabled, the REST API listens on port TCP/3000 (for HTTP) or TCP/3443 (for HTTPS) on all IP Addresses configured on the JUNOS Device. The `addresses` option can be configured with one or more IP Addresses to restrict the REST API to listening only on these addresses.

In Secure Environments, all Management Services including the REST API should be restricted to being access only through the JUNOS Device's dedicate Out of Band Management Interface (fxp0, em0, etc).

Impact:

Hosts will be unable to connect to the REST API HTTPS Service on any addresses which are not configured.

Audit:

To confirm if the REST API's Service Address has been limited, enter the following command at the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# show https addresses
```

The command should return a list of one, or more, IP Addresses which if configured on Interfaces will be used for the REST API HTTPS Service.

These addresses should only include addresses configured on the device's Out of Band Management interface. Confirm this by checking the interface configuration.
The name of the Out of Band Management port varies considerably between platforms, typically:

- `fxp0` on most routing platforms and SRX firewalls
- `me[0-9]` on most EX and some QFX switches
- `em[0-9]` on some EX and QFX switches
- `jmgmt0` on NFX platforms

You can view configured addresses with the following command:

```
[edit system services rest]
user@host# run show interfaces <OOB Interface> terse
```

Where <OOB Interface> is the name of the Out of Band Management Interface for this device.

Remediation:

To restrict the IP Address/es on which the REST API will listen, enter the following command from the `[edit system services rest]` hierarchy:

```
[edit system services rest]
user@host# set https addresses <Service IP>
```

Where <Service IP> is a single IP Address configured on the Device's Out of Band Management Interface.
To add multiple addresses, enter the following command:

```
[edit system services rest]
user@host# set https addresses [<Service IP 1> <Service IP 2> <Service IP
...> ]
```

To remove a single address from the current list enter the following command:

```
[edit system services rest]
user@host# delete https addresses <Service IP>
```

Default Value:

By default the REST API is disabled. When enabled, the REST API HTTPS Service listens on all configured IP Addresses.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/https-edit-system-services-rest.html
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/rest-api-configuring.html

CIS Controls:

Version 6

11.4 Manage Network Devices Securely
Manage network devices using two-factor authentication and encrypted sessions.

Version 7

4.7 Limit Access to Script Tools
Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

6.10.6 Ensure Telnet is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

Cleartext Management Services should be disabled.

Rationale:

Telnet is a remote management protocol that allows users to connect to the command line of a JUNOS router or other device.

Because Telnet transmits all data (including passwords) in cleartext (unencrypted) over the network and provides no assurance of the identity of the hosts involved, it can allow an attacker to gain sensitive configuration, password and other data and is also vulnerable to session hijacking and injection attacks.

This makes Telnet and other unencrypted management applications completely unsuitable for managing network devices and Telnet should be disabled.

Impact:

Ensure administrative access via SSH or other secure method is configured and working before disabling Telnet in a production environment to ensure that administrative access is not lost.

Audit:

To check if Telnet is enabled, execute the following command from the `[edit system services]` hierarchy:

```
[edit system services]
user@host#show | match "telnet;|telnet {" | count
```

The above command should return a line count of 0.

Remediation:

To disable Telnet access issue the following command from the `[edit system telnet]` hierarchy;

```
[edit system services]
user@host# delete telnet
```

Default Value:

Telnet is disable by default on most current platforms. Telnet cannot be configured on JUNOS in FIPS Mode.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.7 Ensure Reverse Telnet is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

Cleartext Management Services should be disabled.

Rationale:

Telnet is a remote management protocol that allows users to connect to the command line of a JUNOS router or other device.

Because Telnet transmits all data (including passwords) in cleartext (unencrypted) over the network and provides no assurance of the identity of the hosts involved, it can allow an attacker to gain sensitive configuration, password and other data and is also vulnerable to session hijacking and injection attacks.

This makes Telnet and other unencrypted management applications completely unsuitable for managing network devices and Telnet should be disabled.

Reverse Telnet is a service that can be configured on JUNOS devices, allowing a user to connect via the auxiliary port to the CLI of another device by establishing a Telnet session, on port 2900/TCP by default. Because Telnet is used as the underlying protocol, Reverse Telnet is subject to the same risks and this service should be disabled.

Impact:

Ensure that alternate administrative access using a secure protocol such as SSH or Reverse SSH is provisioned and tested before removing this service in a production environment.

Audit:

To confirm whether Reverse Telnet is configured, execute the following command from the `[edit system services]` hierarchy:

```
[edit system services]
user@host#show | match "reverse telnet" | count
```

The command should return a line count of 0.

Remediation:

To disable Reverse Telnet access issue the following command from the `[edit system service]` hierarchy;

```
[edit system services]
user@host#delete reverse telnet
```

Default Value:

Reverse Telnet is disabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.3 and 8.2.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-reverse-telnet-reverse-ssh-configuring.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

6.10.8 Ensure FTP Service is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

FTP should be disabled.

Rationale:

File Transfer Protocol (FTP) can be used for loading and exporting configuration from a Juniper device, which can run an FTP Server Service to support these functions.

FTP transfers data in plaintext and should be avoided, with the Secure Copy functions of SSH used instead.

In addition, the FTP service allows files to be read from and written to the devices file system, presenting a risk if misused.

The FTP Service should be disabled on all JUNOS devices and users should avoid using FTP in operational mode commands.

Impact:

Ensure no processes or support systems rely on FTP file transfers from the JUNOS device and migrate any such transfers to a secure alternative prior to disabling FTP in a production environment.

Audit:

To confirm whether the FTP Service is configured, execute the following command from the `[edit system services]` hierarchy:

```
[edit system services]
user@host#show | match ftp | count
```

A line count of 0 should be returned.

Remediation:

To disable the FTP service, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#delete services ftp
```

Default Value:

FTP is enabled on most platforms by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.2.2

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.10.9 Ensure Finger Service is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

The Finger service should be disabled.

Rationale:

Finger is a simple TCP service dating back to the early 1970's that provides information on users logged into a system to other users on the network.

While this was a useful feature in the early days of the Internet, providing information about a router to unauthenticated users is not quite so desirable in today's Internet and presents a serious threat to the security of a JUNOS network device.

The finger daemon itself has suffered from numerous vulnerabilities across many platforms and, as with any unneeded service, should be disabled for this reason also.

Audit:

To confirm whether the Finger Service is configured, execute the following command from the `[edit system services]` hierarchy:

```
[edit system services]
user@host#show | match finger | count
```

A line count of 0 should be returned.

Remediation:

The Finger service is not enabled by default, however if it has been configured on your router it can by disabled by issuing the following command from the `[edit system services]` hierarchy;

```
[edit system services]
user@host#delete finger
```

Default Value:

Finger is disabled on most versions of JUNOS by default. The service cannot be used on FIPS versions of JUNOS.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.2.2
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/access-remote-finger-service-configuring.html

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.10.10 Ensure Unused DHCP Service is Not Set (Automated)

Profile Applicability:

- Level 1

Description:

The DHCP Server should be disabled when not required.

Rationale:

When hardening any computer system for security, it is important to disable or uninstall any application that is not required. The same rule applies to routers and other network devices.

JUNOS devices are able to operate as a Dynamic Host Configuration Protocol (DHCP) server, providing IP Address and other information to client systems on connected networks. DHCP Services are configured either under the `[edit system services dhcp]` (using the Legacy DHCPD process) or `[edit system services dhcp-local-server]` (using the newer Extended JDHCPD process) hierarchies.

In most larger environments, DHCP services will be provided by separate DHCP Servers rather than JUNOS Routers, Switches or Firewalls - although these may still be used in smaller networks or Branch Offices. On some JUNOS platforms the DHCP Service is configured by default, but it is recommended that it is disabled if it is not required.

Impact:

Ensure that DHCP Services are not required before disabling them.

Audit:

To confirm whether either DHCP Service is configured, execute the following command from the `[edit system services]` hierarchy:

```
[edit system services]
user@host#show | match "dhcp.*{"
```

When DHCP is configured above command should return either `dhcp {` or `dhcp-local-server {`
If `dhcp {` was returned, confirm whether Pool is configured with the following command:

```
[edit system services]
user@host#show dhcp | match "pool.*{" | count
```

A line count of at least 1 should be returned to indicate a Pool is configured.
If `dhcp-local-server {` was returned from the first command, confirm whether a pool is configured with the following command:

```
[edit system services]
user@host# top show access address-assignment | match "pool.*{" | count
```

A line count of at least 1 should be returned to indicate a Pool is configured.
If DHCP is enabled but no pools are configured, or none of the configured pools are still required, then this should be considered an Audit Failure and DHCP should be removed.

Remediation:

To disable DHCP services which are not required, issue the one of the following command from the `[edit system services]` configuration hierarchy:
For DHCP configured with the Legacy DHCPD process:

```
[edit system services]
user@host#delete dhcp
```

Or, for DHCP configured with the Enhanced JDHCPD process:

```
[edit system services]
user@host#delete dhcp-local-server
```

Default Value:

Varies by platform. Some Branch/SME focused devices ship with DHCP services configured by default, while most Service Provider or Larger Enterprise devices have DHCP disabled by default.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 2.2.2
2. https://www.juniper.net/documentation/en_US/junos/topics/concept/security-dhcp-routing-instance-understanding.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.11 Ports

Juniper routers have two special ports that are used to connect directly to the routing system. These ports are configured under the `[edit system services]` hierarchy.

6.11.1 Ensure Auxiliary Port is Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The Auxiliary Port should be disabled when not required.

Rationale:

The Auxiliary Port on a Juniper Device is used to connect Modems and other devices to allow remote administration of the router when other connectivity is not possible.

Connections to the Auxiliary Port are treated in a very similar fashion to local Console Port connections.

Although this is a useful function, in most deployments the Auxiliary Port is not utilized at all and so should be disabled, which is the default in all current Junos versions, to prevent potential abuse.

Impact:

The Auxiliary port will not be available.

Audit:

From the command prompt, execute the following command from the `[edit system ports]` hierarchy:

```
[edit system ports]
user@host#show auxiliary | match "disable" | count
```

A line count of 1 should be returned if the Auxiliary Port is disabled.

Remediation:

To disable the Auxiliary Port, issue the following command from the `[edit system ports]` hierarchy;

```
[edit system ports]
user@host#set auxiliary disable
```

Default Value:

The Auxiliary port is disabled by default on most current platforms.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 55, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/auxiliary-edit-system.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.11.2 Ensure Auxiliary Port is Set as Insecure If Used (Automated)

Profile Applicability:

- Level 2

Description:

The Auxiliary Port should be set as Insecure if used.

Rationale:

The Auxiliary Port on a Juniper Device is used to connect Modems and other devices to allow remote administration of the router when other connectivity is not possible.

Connections to the Auxiliary Port are treated in a very similar fashion to local Console Port connections.

Although this is a useful function, connections via the Auxiliary Port represent a less secure method of remote administration compared to services such as SSH or HTTPS so the Aux Port is Disabled by default.

Where the Auxiliary Port is absolutely required for a deployment, logins to the Auxiliary Port using the highly privileged Root or Superuser accounts should be prevented by setting the JUNOS Device's Auxiliary Port as being *Insecure* in order to limit the scope for abuse.

Impact:

The Auxiliary port will not permit logins using the Root or Superuser accounts.

Audit:

From the command prompt, execute the following command from the `[edit system ports]` hierarchy:

```
[edit system ports]
user@host#show auxiliary | match "insecure" | count
```

A line count of 1 should be returned if the Auxiliary Port is set as Insecure.

Remediation:

To set the Auxiliary Port as Insecure, issue the following command from the `[edit system ports]` hierarchy;

```
[edit system ports]
user@host#set auxiliary insecure
```

Default Value:

Root login via the Auxiliary port is disabled by default on most platforms. If enabled, Insecure mode is not configured by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 55, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/auxiliary-edit-system.html

Additional Information:

Ensure that:

- at least one local login account is configured under [edit system login] for recovery
- at least one non-console management utility is configured
- and that the Root password is securely recorded *before* applying this recommendation.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.11.3 Ensure Console Port is Set to Disabled (Automated)

Profile Applicability:

- Level 2

Description:

The JUNOS Device's Console Port should be disabled.

Rationale:

Administrators often use Console Port on a JUNOS Device to configure the Device via the CLI when they have physical access to the device.

In high security environments or deployments where the physical security of the JUNOS Device cannot be assured, such as CPE (Customer Premises Equipment), Point of Sales (POS) or Branch Office installations, disabling the console port will increase the difficulty of accessing the router for an attacker with physical access.

Connecting to the console will not allow access to the CLI without restarting the JUNOS Device to access recovery options, an event which will show up in your monitoring and audit logs.

Impact:

The JUNOS Device's CLI will no longer be accessible through the Console Port without rebooting the device.

Audit:

To confirm whether the Console Port has been disabled, enter the following command from the `[edit system ports]` hierarchy:

```
[system ports]
user@host#show console | match disabled | count
```

The command should return a line count of 1 if the Console Port has been disabled.

Remediation:

To disable the Console Port, issue the following command from the `[edit system ports]` hierarchy;

```
[edit system ports]
user@host#set console disabled
```

Default Value:

By default, the Console Port is enabled

References:

1. Router Security Configuration Guide, Version 1.1b, Page 58, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-securing-console-port-configuring.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.11.4 Ensure Console Port is Set as Insecure (Automated)

Profile Applicability:

- Level 2

Description:

The JUNOS Device's Console Port should be set as Insecure.

Rationale:

Administrators often use Console Port to configure the JUNOS Device when they have physical access to the device.

In high security environments or deployments where the physical security of the router is minimal, such as CPE (Customer Premises Equipment), Point of Sale (POS) or Branch Office installations, it is important to prevent both customers and intruders from accessing the Device's CLI or using the Password Recovery process using the Console Port.

Normally if an attacker is able to connect a console cable and then restart the device, it is possible to reset the root password in order to gain full control.

To prevent this, the Console Port should be set as `Insecure`. This option, which persists after restart, prevents login to the JUNOS Device's Console Port using the Root account. When rebooting the JUNOS Device, the Root password will be required before beginning the Password Recovery process, such as booting into Single User Mode or running the Password Recovery Utility (depending on model).

Impact:

The Console Port will not permit logins using the Root account.

On reboot, access to the Password Recovery process will require the Root password to be entered.

Audit:

To confirm whether the Console Port has been set as Insecure, issue the following command from the `[edit system ports]` hierarchy:

```
[edit system ports ]
user@host#show console | match insecure | count
```

This command should return a line count of 1, indicating that the Console Port has been set as Insecure.

Remediation:

To set the Console Port as Insecure, issue the following command from the `[edit system ports]` hierarchy;

```
[edit system ports]
user@host#set console insecure
```

Default Value:

By default Root password recovery is possible from the console.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 58, National Security Agency (NSA)
2. Recovering the Root Password, JUNOS Software System Basics Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/frameset.html)
3. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-securing-console-port-configuring.html

Additional Information:

Ensure that:

- at least one local login account is configured under `[edit system login]` for recovery
- at least one non-console management utility is configured
- and that the Root password is securely recorded

before applying this recommendation.

Password Recovery without access to the configured Root Password will *not be possible* once the Console Port is set to Insecure.

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

6.11.5 Ensure Log-out-on-disconnect is Set for Console (Automated)

Profile Applicability:

- Level 1

Description:

Console sessions should be logged out as soon as the console cable is unplugged from the routers console port.

Rationale:

Administrators often use a console port to configure JUNOS Devices when they have physical access to the device.

When the administrator unplugs the cable from the console port, their session may be left logged in; allowing the next person who connects to the console port to access the router with the privileges and audit trail of the original administrator.

To prevent this, the JUNOS Devices should be configured to automatically log out console port sessions as soon as the cable is disconnected.

Audit:

To confirm whether Automatic Logout for Console sessions has been configured, enter the following command from the `[edit system ports]` hierarchy:

```
[edit system ports ]
user@host#show console | match log-out | count
```

This command should return a line count of 1 if the Console Port has been configured to automatically disconnect sessions when the cable is unplugged.

Remediation:

To log console sessions out when the console cable is unplugged, issue the following command from the `[edit system ports console]` hierarchy;

```
[edit system ports console]
user@host#set log-out-on-disconnect
```

Default Value:

By default, console sessions continue after the console cable is unplugged.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 58, National Security Agency (NSA)

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

6.12 SYSLOG

SYSLOG is a standard protocol for forwarding and handling log information in an IP Network.

It is essential that SYSLOG messages be recorded, both locally and on a remote SYSLOG Server or SIEM to allow incidents to be detected, investigated and (where appropriate) prosecuted.

Options for system logging and the SYSLOG service are configured under the `[edit system syslog]` hierarchy.

6.12.1 Ensure External SYSLOG Host is Set with Any Facility and Informational Severity (Automated)

Profile Applicability:

- Level 1

Description:

Logging data must be sent to at least one external SYSLOG server.

Rationale:

Log information from a JUNOS Device can be vital in detecting an attack and to allow incidents to be analyzed, investigated and (where appropriate) prosecuted. SYSLOG information is also helpful in diagnosing and resolving non-security related operational issues on the network.

Because of this, one of the first tasks an attacker will attempt to accomplish after gaining access to a Network Device is to alter or delete logs to cover their tracks.

To prevent an attacker or a fault denying you access to log data, it is vital to send logs to at least one External Logging and/or SIEM (Security Incident and Event Manager) Server. JUNOS Devices use the industry standard SYSLOG protocol for this.

SYSLOG entries are generated by a range of sources on a JUNOS Device, such as `authorization` which reports Authentication and Authorization events or `PFE` for events encountered by the Packet Forwarding Engine. Each of these sources are referred to as a *Facility*.

In addition to indicating what facility generated a log message, JUNOS SYSLOG also indicates and allows the administrator to filter based on the *Severity* Level for each message. There are eight possible levels, which are as follows:

- Emergency (0)
- Alert (1)
- Critical (2)
- Error (3)
- Warning (4)
- Notice (5)
- Informational (6)
- Any (7) (called Debug on many SYSLOG systems)

Each increase in level represents an increase in the detail and number of log messages created. Each level includes the messages from all preceding levels, so Critical includes all messages from both the Alert and Emergency levels.

To ensure that vital messages about the Health and Security of the JUNOS Device are not missed, or lost should an attacker delete local logs, *at least* one External SYSLOG or SIEM Server should be configured to receive log messages from `any` Facility and *at least* `info` Severity.

Impact:

Network Devices, particularly Firewalls, can generate a significant volumes of log data, it is essential that the target SYSLOG server is suitably resourced to handle the expected volume of messages and it is strongly recommended that robust archiving and retention processes be employed.

Audit:

From the command prompt, execute the following command from the `[edit system syslog]` hierarchy:

```
[edit system syslog]
user@host# show | display set | match "host .* any [any|info]" | except
"other-routing-engine|scc|sfc0" | count
```

The above command should return a line count equal to or greater than 1, which is the number of configured External SYSLOG Hosts set with the required Facility and Severity.

Remediation:

SYSLOG data is recorded locally by default, you can configure external SYSLOG servers by issuing the following command from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host#set host <Server> any <Severity>
```

Where:

- <Server> is the IP Address or Fully Qualified Domain Name of the Remote Syslog Server
- <Severity> should be either `any` or `info`

Some SYSLOG or SIEM Servers may require additional configuration items such as `explicit-priority` or `structured-data` options to be configured.
It is possible to filter SYSLOG messages to be forwarded to the host using a `match` or `match-`

`string` condition. This should *not* be set for the device's the Remote SYSLOG Host/s configured in meeting this Recommendation.

Default Value:

Log messages are not sent to remote hosts by default, but are stored locally in files in the `/var/log/` folder.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/host-edit-system.html
4. https://www.juniper.net/documentation/en_US/junos/topics/concept/syslog-messages-configuration-overview.html

Additional Information:

Mid Range and High End SRX Devices require additional logging to be configured under the `[edit security log stream]` hierarchy for security related events generated by Flowd and related Data Plane security services.

CIS Controls:

Version 7

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

6.12.2 Ensure At Least 2 External SYSLOG Hosts are Set with Any/Info (Automated)

Profile Applicability:

- Level 2

Description:

Logging data must be sent to at least two external SYSLOG servers.

Rationale:

Log information from a JUNOS Device can be vital in detecting an attack and to allow incidents to be analyzed, investigated and (where appropriate) prosecuted. SYSLOG information is also helpful in diagnosing and resolving non-security related operational issues on the network.

Because of this, one of the first tasks an attacker will attempt to accomplish after gaining access to a Network Device is to alter or delete logs to cover their tracks.

To prevent an attacker or a fault denying you access to log data, it is vital to send logs to at least one External Logging and/or SIEM (Security Incident and Event Manager) Server. JUNOS Devices use the industry standard SYSLOG protocol for this.

SYSLOG entries are generated by a range of sources on a JUNOS Device, such as `authorization` which reports Authentication and Authorization events or `PFE` for events encountered by the Packet Forwarding Engine. Each of these sources are referred to as a *Facility*.

In addition to indicating what facility generated a log message, JUNOS SYSLOG also indicates and allows the administrator to filter based on the *Severity* Level for each message. There are eight possible levels, which are as follows:

- Emergency (0)
- Alert (1)
- Critical (2)
- Error (3)
- Warning (4)
- Notice (5)
- Informational (6)
- Any (7) (called Debug on many SYSLOG systems)

Each increase in level represents an increase in the detail and number of log messages created. Each level includes the messages from all preceding levels, so Critical includes all messages from both the Alert and Emergency levels.

To ensure that vital messages about the Health and Security of the JUNOS Device are not missed, or lost should an attacker delete local logs, *at least* two External SYSLOG or SIEM Servers should be configured to receive log messages from `any` Facility and *at least* `info` Severity.

SYSLOG messages are sent in a "fire and forget" manner over UDP, with no acknowledgement or ability to resend missed messages in the event a server is unable to handle them. Adding a second server significantly reduces the risk that messages are lost in the event of a network or server issue.

Impact:

Network Devices, particularly Firewalls, can generate a significant volumes of log data, it is essential that the target SYSLOG servers are suitably resourced to handle the expected volume of messages and it is strongly recommended that robust archiving and retention processes be employed.

Audit:

From the command prompt, execute the following command from the `[edit system syslog]` hierarchy:

```
[edit system syslog]
user@host# show | display set | match "host .* any [any|info]" | except
"other-routing-engine|scc|sfc0" | count
```

The above command should return a line count equal to or greater than 2, which is the number of configured External SYSLOG Hosts set with the required Facility and Severity.

Remediation:

SYSLOG data is recorded locally by default, you can configure external SYSLOG servers by issuing the following commands from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host# set host <Server 1> any <Severity>

[edit system syslog]
user@host# set host <Server 2> any <Severity>
```

Where:

- <Server 1> is the IP Address or Fully Qualified Domain Name of the first Remote SYSLOG or SIEM Server
- <Server 2> is the IP Address or FQDN of a *separate* second Remote SYSLOG or SIEM Server. For added resilience, you may wish to place the second server on a different network to the first and this is recommended where possible.
- <Severity> should be either `any` or `info`

Some SYSLOG or SIEM Servers may require additional configuration items such as `explicit-priority` or `structured-data` options to be configured.
It is possible to filter SYSLOG messages to be forwarded to the host using a `match` or `match-string` condition. This should *not* be set for the device's the Remote SYSLOG Hosts configured in meeting this Recommendation.

Default Value:

Log messages are not sent to remote hosts by default, but are stored locally in files in the `/var/log/` folder.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 10
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/host-edit-system.html
4. https://www.juniper.net/documentation/en_US/junos/topics/concept/syslog-messages-configuration-overview.html

Additional Information:

Mid Range and High End SRX Devices require additional logging to be configured under the `[edit security log stream]` hierarchy for security related events generated by Flowd and related Data Plane security services.

CIS Controls:

Version 7

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

6.12.3 Ensure Local Logging is Set for Firewall Events (Automated)

Profile Applicability:

- Level 1

Description:

Logging data for Firewall Events should be saved to a local file.

Rationale:

The JUNOS Device's built in Firewall (configured under `[edit firewall]` and discussed in more detail elsewhere in this Benchmark) can be the first line of defense, so the logging it produces can be vital in responding to a security incident as well as a useful tool for diagnosing faults relating to the Firewall.

A local SYSLOG file should be configured to record all firewall related events.

Impact:

Logging of Firewall events may record a large volume of messages. You may wish to specify the size of files to be recorded, the number of zipped older files the JUNOS Devices should keep and automatic archiving settings to appropriate values for the device and environment you are using. Details of the related commands are linked in the References section.

Audit:

From the command prompt, execute the following command:

```
[edit system syslog]
user@host# show | display set | match "file .* firewall any" | count
```

The command should return a line count of 1, indicating that messages from the `firewall` facility and `any` severity are being recorded to a file.

Remediation:

To configure a local SYSLOG file for Firewall events, issue the following command from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host#set file <filename> firewall any
```

Where <filename> is the file, in the default `/var/log/` folder, that should be used to log these messages. You may, for example, choose to call the file `firewall`, in which case it can be read with the `show log firewall` command.

Default Value:

SYSLOG for Firewall events is not sent to a separate file by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/file-edit-accounting-options.html

Additional Information:

On SRX Firewalls, the `firewall` facility is used for the *stateless* firewall filters configured under `[edit firewall]` and *not* the *stateful* firewalling configured under `[edit security policies]`.

By default, on SME/Branch SRXs, messages relating to Security Policy are logged to `/var/log/messages` and prefaced with `RT_FLOW` in each message, indicating the messages are from `flowd`.

On High End SRXs, Data Plane Security Logging is handled separately to Control Plane Logging, and needs to be configured under the `[edit security log stream]` hierarchy.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.12.4 Ensure Local Logging is Set for Authentication and Authorization Events (Automated)

Profile Applicability:

- Level 1

Description:

Logging data for Authentication and Authorization events should be saved to a local file.

Rationale:

Authentication and Authorization events are generated whenever a user logs in to the router or performs an action which requires Authorization, such as making a change.

This information can provide a record of activity on the JUNOS Device when responding to both Security Incidents and Operational Issues.

A local SYSLOG file should be configured to record all Authentication and Authorization related events, which are both generated by the `authorization` facility.

Impact:

Authentication and Authorization events will be logged to the configured file in the JUNOS Device's `/var/log/` folder. You may wish to specify the size of files to be recorded, the number of zipped older files the JUNOS Devices should keep and automatic archiving settings to appropriate values for the device and environment you are using. Details of the related commands are linked in the References section.

Audit:

From the command prompt, execute the following command:

```
[edit system syslog]
user@host#show | display set | match "file .* authorization any" | count
```

The command should return a line count of 1, indicating that messages from the `authorization` facility and `any` severity are being recorded to a file.
Where <filename> is the file, in the default `/var/log/` folder, that should be used to log these messages. You may, for example, choose to call the file `auth`, in which case it can be read with the `show log auth` command.

Remediation:

To configure a local SYSLOG file for Auth events, issue the following command from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host#set file <filename> authorization any
```

Default Value:

Authorization events at Info level are logged to the `/var/log/messages` file by default on most JUNOS systems, but the additional events from the `any` level are not recorded by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/file-edit-accounting-options.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.12.5 Ensure Local Logging is Set for Interactive-Commands (Automated)

Profile Applicability:

- Level 1

Description:

Logging data for Interactive Commands should be saved to a local file.

Rationale:

When responding to a security incident or fault, a record of all of the commands issued on the JUNOS Devices, either through the CLI or through management APIs such as JUNOScript or NETCONF, can provide vital clues.

A local SYSLOG file should be configured to record all `interactive-commands` issued on the JUNOS Device, along with details of the user who issued them and when. Having this data available locally, as well as on remote SYSLOG or SIEM Servers, can aide Incident Responders and enable a faster resolution to both Security and Operational related issues.

Impact:

Events detailing Interactive Commands will be logged to the configured file in the JUNOS Device's `/var/log/` folder. You may wish to specify the size of files to be recorded, the number of zipped older files the JUNOS Devices should keep and automatic archiving settings to appropriate values for the device and environment you are using. Details of the related commands are linked in the References section.

Audit:

From the command prompt, execute the following command:

```
[edit system syslog]
user@host#show | display set | match "file .* interactive-commands any;" |
count
```

The command should return a line count of 1, indicating that messages from the `interactive-commands` facility and `any` severity are being recorded to a file.

Remediation:

To configure a local SYSLOG file for Interactive Commands, issue the following command from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host#set file <filename> interactive-commands any
```

Where <filename> is the file, in the default `/var/log/` folder, that should be used to log these messages. You may, for example, choose to call the file `interactive-commands`, in which case it can be read with the `show log interactive-commands` command.

Default Value:

Messages from the `interactive-commands` facility are logged to the `/var/log/interactive-commands` file at the `info` Severity Level, by default on most JUNOS platforms (though this may vary by platform and version).

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/file-edit-accounting-options.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.12.6 Ensure Local Logging is Set to Messages File (Automated)

Profile Applicability:

- Level 1

Description:

Logging data should be saved locally to the default messages file.

Rationale:

As part of the `factory-default` configuration, all JUNOS devices are configured to log SYSLOG events from several Facilities to a standard `/var/log/messages` file.

The exact logging for this file may vary slightly by platform, but will always include `critical` messages from `any` facility and `authorization` messages at `info` level.

When responding to a Security Incident, it is not uncommon for additional external resources or JTAC support to be engaged. Removing logging to this standard location may slow down and hamper Incident Responders, particularly those who may not be familiar with organization specific standards, as they look for expected logs in this file, either manually or using automated/scripting tools.

The fact that the `/var/log/messages` file is missing may also be interpreted by Incident Responders as being a part of the intrusion or incident, resulting in further time being lost investigating something which is not, in this case, related to the incident.

For these reasons, the default logging to the `/var/log/messages` file should *always* be left in place on all JUNOS Devices, with any additional details or levels logged to other files as required.

Impact:

The default local logging to the `/var/log/messages` file will be used.

Audit:

From the command prompt, execute the following command:

```
[edit system syslog]
user@host#show | display set | match "file messages [authorization info|any
critical]" | count
```

The command should return a line count equal to or greater than 2, indicating that logging of `authorization` and `any` events to the `/var/log/messages` file is configured as per the `factory-default` configuration.

Remediation:

To configure a local SYSLOG messages file, issue the following commands from the `[edit system syslog]` hierarchy;

```
[edit system syslog]
user@host#set file messages any critical

[edit system syslog]
user@host#set file messages authorization info
```

On some JUNOS platforms, the `factory-default` configuration may include additional elements to be logged to the `/var/log/messages` file.
You can confirm what the `factory-default` settings for SYSLOG are on your JUNOS Device by issuing the following commands *from a new configuration mode session - which does not have any outstanding changes.*
First, confirm that there are no pending changes:

```
[edit]
user@host# show | compare
```

If any difference were highlighted *do not proceed* with the next set of commands until you have either rolled back or committed the outstanding changes.
Next load the `factory-default` configuration (*do not commit this configuration*):

```
[edit]
user@host# load factory-default
```

Now we can compare the `factory-default` configuration to your current Active Configuration (`rollback 0`):

```
[edit]
user@host# edit system syslog file messages

[edit system syslog file messages]
user@host# show | compare
```

Finally, roll the Candidate Configuration back to the current Active Configuration and quit from Configuration Mode:

```
[edit system syslog file messages]
user@host# top
```

```
[edit]
user@host# rollback 0
load complete

[edit]
user@host# quit
```

Any logging which was missing from the current Active Configuration should be added to restore the original configuration.

Default Value:

Messages from `any` Facility at `critical` Severity and from the `authorization` Facility at `info` Severity are logged to the `/var/log/messages` file on all JUNOS Devices. Some devices may have additional logging to this file by default.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 130, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/file-edit-accounting-options.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.13 Ensure Autoinstallation is Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Autoinstallation should be disabled.

Rationale:

The Autoinstallation feature allows the JUNOS Device to automatically download and apply configuration from an FTP, TFTP or HTTP server on boot, having obtained IP Address details via DHCP or BOOTP.

Autoinstallation provides an extremely useful function for rapid deployment of large numbers of devices, however Autoinstallation provides no method to authenticate the identity of the Installation Servers or validity of the supplied configuration files.

This may allow an attacker to change the device's configuration at boot (or after forcing a reboot through a DoS attack) by impersonating the DHCP, FTP, TFTP or HTTP servers or by carrying out session hijacking. This would be a multistage attack, as Autoinstallation *should* only be used if the device does not find an existing configuration locally - so the attacker would also need to have been able to disrupt the configuration or boot process through some other vector, but this may be viable for an attacker who already has some foothold on the device to escalate their privileges.

If successful the attacker would have gained complete control over the JUNOS Device.

Because all of the protocols used by Autoinstallation transfer data in plain text, it is trivial for an attacker to intercept the traffic and obtain a complete copy of the configuration, possibly containing authentication details to both the device and Operational Support Services.

Autoinstallation is useful during deployments of large number of devices, but due to these limitations should only be used in a tightly controlled, isolated, build environment where the authenticity of servers and configuration can be assured and snooping on sensitive details can be eliminated. Autoinstallation should *never* be used over untrusted or public networks, such as over the Internet.

Many JUNOS Devices have Autoinstallation enabled by default to support large deployments using the feature, but Autoinstallation should be disabled on all devices once deployed to production.

Impact:

This should have no impact on production systems, as Autoinstallation should only be used when no non-`factory-default` configuration is present on the JUNOS Device at boot.

Audit:

To confirm whether Autoinstallation is disabled, execute the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "autoinstallation" | count
```

This command should return a line count of 0 if Autoinstallation is disabled.

Remediation:

To disable Autoinstallation issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#delete autoinstallation
```

Default Value:

The Autoinstallation service is enabled by default on many JUNOS Devices.

References:

1. Payment Card Industry Data Security Standard (PCI DSS), Version 3.2.1, Requirement 1.2.2, 2.3 and 8.2.1
2. https://www.juniper.net/documentation/en_US/junos/topics/concept/security-autoinstallation-overview.html
3. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/autoinstallation-edit-system.html

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.14 Ensure Configuration File Encryption is Set (Automated)

Profile Applicability:

- Level 2

Description:

Configuration files should be encrypted.

Rationale:

On many JUNOS platforms the configuration files are stored on a removal flash file system.

A malicious user with even momentary physical access to the router could readily remove the flash card, gaining access to the device's configuration which is likely to contain extremely sensitive details.

Exposure to this type of attack increased in Branch Office or Customer Premises Equipment (CPE) installations or where devices are transported by third parties post configuration.

To prevent an attacker accessing the configuration files from flash, JUNOS Devices offer a facility to encrypt the `/config` and `/var/db/config` directories using AES or DES algorithms.

Note - Export restrictions mean that AES is not available in all regions.

Impact:

The configuration files will be encrypted on storage and the JUNOS Device will use the key stored in it's EEPROM to decrypt the configuration file at boot.

Adding the `unique` option will cause the JUNOS Device to combine the device Serial Number with the entered key when creating the Encryption Key, meaning that the configuration can *only* be loaded by *this* JUNOS Device - *even with the key being configured*.

Audit:

To confirm whether Configuration File Encryption is enabled, execute the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show match "encrypt-configuration-files" | count
```

The above command return a line count of 1, indicating that Encryption of Configuration Files is enabled.

Remediation:

To enable Configuration File Encryption, you must first set an encryption key by issuing the following command from Operational Mode:

```
user@host>request system set-encryption-key
```

You will be prompted to enter and then verify the key.
The preferred encryption algorithm may be specified by adding the `algorithm` option, or left as default. If the device is running the US/Domestic version of JUNOS the default algorithm will be AES. Devices running the Export version of JUNOS will default to the weaker DES standard and cannot be configured to support AES.
Optionally, the `unique` option may be specified. This will cause JUNOS to combine the device's Serial Number as part of the Encryption Key, making the configuration unloadable on any other JUNOS device, *even with the key set at the prompt.*
Once a key has been set the following command should be issued from the `[edit system]` hierarchy:

```
[edit system]
user@host# set encrypt-configuration-files
```

The encryption will not be carried out until the configuration is committed.

Default Value:

Configuration file encryption is disabled by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/encrypting-and-decrypting.html

Additional Information:

The stronger AES algorithm should be used wherever it is supported, but AES is not supported in Export versions of JUNOS - which are restricted to using DES.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.15 Ensure Multicast Echo is Set to Disabled (Automated)

Profile Applicability:

- Level 2

Description:

The Routing Engine should ignore Echo Requests sent to Multicast addresses.

Rationale:

An attacker may use multicast Echo Requests (pings) during recognizance of a network to obtain a list of network systems and what services they may be offering.

An example of this would be sending a ping to 224.0.0.18, hoping to discover routers in the network running VRRP.

In most environments it is not necessary for the Routing Engine to respond to Multicast Echo Requests to function correctly; however in some cases this will be required, such as for troubleshooting in environments with Multicast Routing support. Only disable this functionality if you are certain you do not need it.

Impact:

The JUNOD Device will not respond to ICMP Echo Requests (pings) sent to Multicast Addresses used by the device.

Audit:

To confirm whether Multicast Echo Responses are Disabled, enter the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "no-multicast-echo" | count
```

A line count of 1 should be returned, indicating that the device will ignore ICMP Echo Requests sent to Multicast addresses.

Remediation:

To ignore multicast Echo Requests, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set no-multicast-echo
```

Default Value:

By default JUNOS Devices respond to multicast Echo Requests for multicast groups it is a member of.

References:

1. https://juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-multicast-echo-edit-system.html
2. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/multicast-ping-packet-response-disabling.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.16 Ensure Ping Record Route is Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The Routing Engine should ignore Echo Requests with the Record Route option set.

Rationale:

When the Record Route Option is set on an Echo Request (ping), the hosts processing the packet should record their Interface addresses and a Timestamp on the response packet as it traverses the network (up to 9 hops) allowing the host that made the request to see the path that the response takes through the network, including discovering details of Provider Edge (PE) switches in MPLS VPN services and Loopback Interfaces.

Attackers may use Echo Requests with the Record Route option set during recognizance of a network to obtain details of the networks topology,

The Record Route Option is considered to be largely deprecated, with no valid uses expected in almost all production networks; therefore, the JUNOS Device should be configured not to to include these details when responding to Echo Requests with the Record Route Option set.

Impact:

ICMP Echo Requests (pings) with the Record Route Option set will still receive a response (unless blocked elsewhere), but the JUNOS Device will not return the additional Route and Interface details.

Audit:

To confirm that Ping Record Route responses are Disabled, execute the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "no-ping-record-route" | count
```

A line count of 1 should be returned, indicating that the JUNOS Device will not respond to ICMP Echo Requests with the Record Route Option set.

Remediation:

To disable reporting of Interface details in responses to Echo Requests with the Record Route option set, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set no-ping-record-route
```

Default Value:

By default the Routing Engine responds to Echo Requests with the Record Route option set, adding the receiving interfaces IP address to the header of the packet.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/icmp-ip-address-timestamp-disabling.html
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-ping-record-route-edit-system.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.17 Ensure Ping Timestamps are Set to Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The Routing Engine should not return Timestamp information to Ping Requests

Rationale:

When the Timestamp Request option is set in a Echo Request (ping) packet, a host generally responds with its current system time when the ping is received.

Attackers may use Echo Requests with the Timestamp option set during recognizance of a network to obtain details of the configuration and state.

The use of these options is largely deprecated, with no valid usage in almost all modern networks; therefore, the JUNOS Device should be configured not to return the Timestamp in ICMP Echo Responses.

Impact:

ICMP Echo Requests (pings) with the Request Timestamp Option set will still receive a response (unless blocked elsewhere), but the JUNOS Device will not return the additional Timestamp information.

Audit:

To confirm whether Pings Responses are configured not to include Timestamp information, execute the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "no-ping-time-stamp" | count
```

A line count of 1 should be returned, indicating that ICMP Echo Responses will not include Timestamp information.

Remediation:

To ignore Echo Requests with the Timestamp Request option set, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set no-ping-time-stamp
```

Default Value:

By default the Routing Engine responds to Echo Requests with the Timestamp Request option set, including the current system time of the router.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/icmp-ip-address-timestamp-disabling.html
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-ping-time-stamp-edit-system.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.18 Ensure Time-Zone is Set to UTC (Automated)

Profile Applicability:

- Level 2

Description:

All devices should use the UTC time zone.

Rationale:

When a network comprises of hosts across multiple countries or states, the use of local time zones can make analysis of log events confusing and error prone, particularly when localized "Daylight Savings Time" or equivalent changes occur, affecting one area but not another.

To prevent confusion Coordinated Universal Time (UTC) should be used for all routers to allow consistent logging timestamps. UTC can be considered equivalent to GMT+0 for the purposes of setting time zones (it is actually GMT with added leap seconds defined by atomic clocks at the US Naval Observatory).

By having all Servers and Network Devices utilizing the same time-zone for logging; correlation and co-ordination is greatly simplified and Incident Response time is decreased.

Impact:

System time, for example viewed with the `show system uptime` command, and timestamps in log messages will be given in UTC.

Audit:

To confirm that the Time Zone has not been configured to something other than UTC/GMT, enter the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show time-zone | except "GMT;|UTC;" | count
```

A line count of 0 should be returned, indicating that the Time Zone has been set to the default of UTC or explicitly to GMT with no offset (which is directly equivalent).

Remediation:

To configure the Time Zone, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set time-zone UTC
```

Default Value:

By default the time-zone is set to UTC.

References:

1. Router Security Configuration Guide, Version 1.1b, Page 174, National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/time-zone-edit-system.html

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

6.19 Ensure Hostname is Not Set to Device Make or Model (Automated)

Profile Applicability:

- Level 1

Description:

The device make and model should not appear in the hostname.

Rationale:

The first step in any attack is reconnaissance. An attacker will attempt to learn about the target network, its hosts and network devices.

A key piece of information for an attacker is what type of device he/she is attacking. By using the routers Model number, type, manufacturer or software version as part of its hostname, we give an attacker this valuable piece of information with no effort or risk of exposure. This is particularly true where the hostname is used in DNS.

This should not be interpreted as recommending "security through obscurity" as a valid approach - rather that, as defenders, we would rather an attacker be required to perform more active reconnaissance to gather information about the target network - so that Intrusion Prevention Systems, Firewalls, Honeypots and other Security solutions are given a greater opportunity to detect and defend against the activity.

Impact:

The hostname will appear in the CLI prompt, in SNMP information and in log messages.

Audit:

To confirm that the Hostname does not contain the make or model number, issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show host-name | match "Juniper|JUN|ACX|EX|MX|NFX|PTX|QFX|SRX" |
display inheritance | count
```

A line count of 0 should be returned, indicating that the hostname does not include the model prefix of primary Juniper platforms or terms like Juniper, JUNOS or JUN-OS (note, the `match` statement is not case sensitive in it's default operation, so both "JUN" and "jun" would be matched.).
Note - In some instances, some hostnames which may be unrelated to model number may

match this filter.
For example, an organization's naming policy may require that hostnames include the ISO 3166 standard two letter Country Code for the country in which the device is deployed. If the device were deployed in Mexico, then this would be `mx`, which would match the filter in the test above. Or a device might be deployed at the "Equinix Harbour Exchange" facility in London, which is typically abbreviated to HEX, and this would also match the filter.

Remediation:

To configure the hostname, issue the following command from the `[edit system]` hierarchy;

```
[edit system]
user@host#set host-name <hostname>
```

The hostname should not include any indication of the make or model of the device.

Default Value:

Varies by platform.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/host-name-edit-system.html

Additional Information:

On devices with multiple Routing Engines, in TX Matrix or in SRX HA Clusters the host-name will often be configured as part of an apply-group so that each RE/node has a different host-name applied. The `display inheritance` option has been included in the Audit Procedure to detect this, but the Remediation Procedure does not provide instructions for changing apply-groups.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.20 Ensure Default Address Selection is Set (Automated)

Profile Applicability:

- Level 2

Description:

The primary address configured on the loopback should be used as the source in all JUNOS generated packets.

Rationale:

To ensure a consistent source address for traffic from the JUNOS Device, the Loopback address should be configured as the default source address for traffic generated by the Routing Engine. By default the primary address on the Routed or Management Interface from which the traffic will be sent will be used.

When configured, packets for NTP, SNMP Traps, SSH, SYSLOG and other protocols initiated by the router will all use the Loopback address for the packets source unless explicitly configured to use a different address at a more specific hierarchy. This predictable source address makes it easier to configure strict Firewall filters on neighboring network devices.

Impact:

The Primary Address configured on the device's loopback interface will be used as the source for all system generated traffic, unless a different address is specified elsewhere.

Audit:

To confirm whether Default Address Selection has been configured, enter the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#show | match "default-address-selection" | count
```

A line count of 1 should be returned, indicating that Default Address Selection has been set.

Remediation:

To set the default source address to the loopback interface enter the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host#set default-address-selection
```

Ensure that a loopback address has been configured for the device from the `[edit interfaces lo0]` hierarchy.

Default Value:

No Loopback Address is configured by default and the source address for system generated traffic will be that of the Routed or Management interface nearest the destination.

References:

1. Router Security Configuration Guide, Version 1.1b, Section 4.1.4 (page 58), National Security Agency (NSA)
2. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/default-address-selection-edit-system.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

6.21 Ensure ICMP Redirects are Disabled for IPv4 (Automated)

Profile Applicability:

- Level 1

Description:

The Routing Engine should not send ICMP Redirect Messages.

Rationale:

ICMP Redirect Messages provide a method for a router to communicate routing information with a host and is intended for use when a router receives packets to forward to a destination to which the host should have a direct route. In a well designed, modern, network ICMP Redirects should not be needed or add any useful functionality.

An attacker may abuse this feature to obtain topology information about a target network and potentially identify weaknesses for later exploitation or to target the router or hosts with a Denial of Service (DoS) or Man in the Middle (MITM) attacks.

To prevent this abuse, ICMP Redirect message generation should be disabled globally where it is not required.

Impact:

In some networks, for instances where subnets populated by hosts include multiple non-redundant gateways, removing redirects may result in traffic being doubled on some gateways interfaces as traffic is received and then forwarded on the same port.

Audit:

From the `[edit system]` configuration hierarchy, issue the following command:

```
[edit system]
user@host# show | match "no-redirects;" | count
```

The command should return a count of 1 line.

Remediation:

To disable ICMP redirects globally for IPv4, issue the following command from the `[edit system]` heirachy:

```
[edit system]
user@host# set no-redirects
```

Default Value:

JUNOS devices send ICMP Redirect messages by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-redirects-edit-system.html
2. http://www.cymru.com/gillsr/documents/icmp-redirects-are-bad.pdf

Additional Information:

For environments where disabling ICMP Redirects globally is not possible, please refer to the Level 2 recommendation 3.6 Ensure ICMP Redirects are set to disabled (on all untrusted networks) for more information on disabling redirects on an per Interface basis.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.22 Ensure ICMP Redirects are Disabled for IPv6 (Automated)

Profile Applicability:

- Level 1

Description:

The Routing Engine should not send ICMP Redirect Messages.

Rationale:

ICMP Redirect Messages provide a method for a router to communicate routing information with a host and is intended for use when a router receives packets to forward to a destination to which the host should have a direct route. In a well designed, modern, network ICMP Redirects should not be needed or add any useful functionality.

An attacker may abuse this feature to obtain topology information about a target network and potentially identify weaknesses for later exploitation or to target the router or hosts with a Denial of Service (DoS) or Man in the Middle (MITM) attacks.

To prevent this abuse, ICMP Redirect message generation should be disabled globally where it is not required.

Impact:

In some networks, for instances where subnets populated by hosts include multiple non-redundant gateways, removing redirects may result in traffic being doubled on some gateways interfaces as traffic is received and then forwarded on the same port.

Audit:

Confirm whether the device is configured for IPv6 by issuing the following command:

```
[edit]
user@host# show | match "family inet6" | count
```

If the returned value is a positive integer, then IPv6 is configured and redirects should be disabled.
To confirm that ICMP Redirects are disabled for IPv6, issue the following command from the `[edit system]` configuration hierarchy:

```
[edit system]
user@host# show | match "no-redirects-ipv6;" | count
```

The command should return a count of 1 line.

Remediation:

To disable ICMP redirects globally for IPv6, issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host# set no-redirects-ipv6
```

Default Value:

JUNOS devices send ICMP Redirect messages by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-redirects-ipv6-edit-system-interfaces-ex-series.html
2. http://www.cymru.com/gillsr/documents/icmp-redirects-are-bad.pdf

Additional Information:

For environments where disabling ICMP Redirects globally is not possible, please refer to the non-Scorable Recommendation 3.7 Ensure ICMP Redirects are set to disabled (on all untrusted IPv6 networks) for more information on disabling redirects on an per Interface basis.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.23 Ensure Password is Set for PIC-Console-Authentication (Automated)

Profile Applicability:

- Level 1

Description:

Connections to the PIC Console should require a password.

Rationale:

Many JUNOS Devices (including M, MX & T Series Routers, PTX Series and High End SRXs) utilize Physical Interface Cards to provide interface flexibility.

Some PICs include additional Console Ports for performing advanced diagnostics on the Packet Forwarding Engine (PFE) with physical access to the device. An attacker, who was able to gain access to this normally unauthenticated port, may be able to impact the device or seek to escalate their privileges, bypassing normal authentication mechanisms.

To prevent this, `pic-console-authentication` should be configured using a secure password which is not the same as that used by any user or the Root account.

Impact:

The configured password will be required before accessing the PIC Console to perform diagnostics.

Audit:

To confirm whether a password has been set for the PIC Console, issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host# show pic-console-authentication | count
```

A line count of 1 indicates that a password has been set.

Remediation:

To set a password for access to the PIC Console, issue the following command from the `[edit system]` hierarchy:

```
[edit system]
user@host# set pic-console-authentication plain-text-password
```

The JUNOS Device will prompt you to enter a new password, which must meet the complexity requirements configured under `[edit system login]`, as shown below:

```
[edit system]
user@host# set pic-console-authentication plain-text-password
New password:
Retype new password:
```

Default Value:

No authentication is required to access the PIC Console by default.

References:

1. https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/pic-console-access-configuring.html

Additional Information:

Not all JUNOS Devices have PICs with PIC Consoles, but as many devices are modular and such a PIC could be added at a later date - it is recommended that authentication be configured for all devices.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**General Recommendations**		
1.1	Ensure Device is running Current Junos Software (Manual)	□	□
1.2	Ensure End of Life JUNOS Devices are not used (Manual)	□	□
1.3	Ensure device is physically secured (Manual)	□	□
1.4	Ensure configuration is backed up on a regular schedule (Manual)	□	□
1.5	Ensure backup data is stored and transferred securely (Manual)	□	□
1.6	Ensure maximum RAM is installed (Manual)	□	□
1.7	Ensure logging data is monitored (Manual)	□	□
1.8	Ensure Retired JUNOS Devices are Disposed of Securely (Manual)	□	□
2	**Firewall**		
2.1	Ensure "Protect RE" Firewall Filter is set for inbound traffic to the Routing Engine (Manual)	□	□
2.2	Ensure "Protect RE" Firewall Filter includes explicit terms for all Management Services (Manual)	□	□
2.3	Ensure "Protect RE" Firewall filter includes Rate-Limiting for Management Services terms (Manual)	□	□
2.4	Ensure "Protect RE" Firewall Filter includes explicit terms for all Protocols (Manual)	□	□
2.5	Ensure "Protect RE" Firewall Filter includes Flood Attack Protection terms (Manual)	□	□
2.6	Ensure firewall filters contain explicit deny and log term (Manual)	□	□
2.7	Ensure internal sources are blocked on external networks (Manual)	□	□
3	**Interfaces <Interface Name>**		
3.1	**DLn – Dialer Interfaces**		
3.1.1	Ensure Caller ID is set (Automated)	□	□
3.1.2	Ensure access profile is set to use CHAP (Automated)	□	□
3.1.3	Forbid Dial in Access (Automated)	□	□
3.2	**Family Inet VRRP-Group (Interface Redundancy)**		
3.2.1	Ensure VRRP authentication-key is set (Automated)	□	□
3.2.2	Ensure authentication-type is set to MD5 (Automated)	□	□
3.3	Ensure unused interfaces are set to disable (Manual)	□	□
3.4	Ensure interface description is set (Automated)	□	□

3.5	Ensure proxy-arp is disabled (Automated)	□	□
3.6	Ensure ICMP Redirects are set to disabled (on all untrusted IPv4 networks) (Manual)	□	□
3.7	Ensure ICMP Redirects are set to disabled (on all untrusted IPv6 networks) (Manual)	□	□
3.8	Ensure Loopback interface address is set (Automated)	□	□
3.9	Ensure only one loopback address is set (Automated)	□	□
3.10	Ensure inbound firewall filter is set for Loopback interface (Automated)	□	□
4	**Protocols**		
4.1	**BGP**		
4.1.1	Ensure peer authentication is set to MD5 (Automated)	□	□
4.1.2	Ensure peer authentication is set to IPSEC SA (Manual)	□	□
4.1.3	Ensure EBGP peers are set to use GTSM (Automated)	□	□
4.1.4	Ensure Bogon Filtering is set (where EBGP is used) (Manual)	□	□
4.1.5	Ensure Ingress Filtering is set for EBGP peers (Manual)	□	□
4.1.6	Ensure RPKI is set for Origin Validation of EBGP peers (Manual)	□	□
4.2	**ISIS**		
4.2.1	Ensure IS-IS neighbor authentication is set to MD5 (Automated)	□	□
4.2.2	Ensure IS-IS neighbor authentication is set to SHA1 (Automated)	□	□
4.2.3	Ensure authentication check is not suppressed (Automated)	□	□
4.2.4	Ensure loose authentication check is not configured (Automated)	□	□
4.2.5	Ensure IS-IS Hello authentication check is not suppressed (Automated)	□	□
4.2.6	Ensure PSNP authentication check is not set to suppressed (Automated)	□	□
4.2.7	Ensure CSNP authentication check is not set to suppressed (Automated)	□	□
4.3	**OSPF**		
4.3.1	Ensure OSPF authentication is set to MD5 (Automated)	□	□
4.3.2	Ensure OSPF authentication is set to IPSEC SA with SHA (Automated)	□	□
4.4	**OSPF3**		
4.4.1	Ensure OSPFv3 authentication is set to IPSEC SA (Automated)	□	□
4.5	**RIP**		
4.5.1	Ensure RIP authentication is set to MD5 (Automated)	□	□

4.5.2	Ensure RIP is set to check for zero values in reserved fields (Automated)	□	□
4.6	**<protocol> bfd**		
4.6.1	Ensure BFD Authentication is Set (Automated)	□	□
4.6.2	Ensure BFD Authentication is Not Set to Loose-Check (Automated)	□	□
4.7	**LDP**		
4.7.1	Ensure authentication is set to MD5 (Automated)	□	□
4.7.2	Ensure authentication is set to AES-CMAC (Automated)	□	□
4.8	**MSDP**		
4.8.1	Ensure authentication is set to MD5 (Automated)	□	□
4.9	**Neighbor-discovery**		
4.9.1	Ensure Secure Neighbor Discovery is configured (Automated)	□	□
4.10	**Router-discovery**		
4.10.1	Ensure ICMP Router Discovery is disabled (Automated)	□	□
4.11	**RSVP**		
4.11.1	Ensure authentication is set to MD5 (Automated)	□	□
4.12	**LLDP and LLDP-MED**		
4.12.1	Ensure LLDP is Disabled if not Required (Manual)	□	□
4.12.2	Ensure LLDP-MED is Disabled if not Required (Manual)	□	□
5	**SNMP**		
5.1	Ensure Common SNMP Community Strings are NOT used (Automated)	□	□
5.2	Ensure SNMPv1/2 are set to Read Only (Automated)	□	□
5.3	Ensure a client list is set for SNMPv1/v2 communities (Automated)	□	□
5.4	Ensure “Default Restrict” is set in all client lists (Automated)	□	□
5.5	Ensure SNMP Write Access is not set (Automated)	□	□
5.6	Ensure AES128 is set for all SNMPv3 users (Automated)	□	□
5.7	Ensure SHA1 is set for SNMPv3 authentication (Automated)	□	□
5.8	Ensure interface restrictions are set for SNMP (Automated)	□	□
5.9	Ensure SNMP is set to OOB management only (Automated)	□	□
6	**System**		
6.1	**Accounting**		
6.1.1	Ensure Accounting Destination is configured (Automated)	□	□
6.1.2	Ensure Accounting of Logins (Automated)	□	□
6.1.3	Ensure Accounting of Configuration Changes (Automated)	□	□
6.1.4	Recommend Accounting of Interactive Commands (where External AAA is used) (Automated)	□	□
6.2	**Archival**		
6.2.1	Ensure Archive on Commit (Automated)	□	□

6.2.2	Ensure at least one SCP Archive Site is configured (Automated)	□	□
6.2.3	Ensure NO Plain Text Archive Sites are configured (Automated)	□	□
6.3	**Authentication-Order**		
6.3.1	Ensure external AAA is used (Automated)	□	□
6.3.2	Ensure Local Accounts can ONLY be used during loss of external AAA (Automated)	□	□
6.4	**Diag-Port-Authentication**		
6.4.1	Ensure Authentication is configured for Diagnostic Ports (Automated)	□	□
6.4.2	Ensure Diagnostic Port Authentication uses a complex password (Manual)	□	□
6.5	**Internet-Options**		
6.5.1	Ensure ICMPv4 rate-limit is Set (Automated)	□	□
6.5.2	Ensure ICMPv6 rate-limit is Set (Automated)	□	□
6.5.3	Ensure ICMP Source-Quench is Set to Disabled (Automated)	□	□
6.5.4	Ensure TCP SYN/FIN is Set to Drop (Automated)	□	□
6.5.5	Ensure TCP RST is Set to Disabled (Automated)	□	□
6.6	**Login**		
6.6.1	**Retry Options**		
6.6.1.1	Ensure Max 3 Failed Login Attempts (Automated)	□	□
6.6.1.2	Ensure Max Login Backoff Threshold of 2 (Automated)	□	□
6.6.1.3	Ensure Minimum Backoff Factor of 5 (Automated)	□	□
6.6.1.4	Ensure Minimum Session Time of at least 20 seconds (Automated)	□	□
6.6.1.5	Ensure Lockout-period is set to at least 30 minutes (Automated)	□	□
6.6.2	Ensure Login Class is set for all Users Accounts (Automated)	□	□
6.6.3	Ensure Idle Timeout is set for all Login Classes (Automated)	□	□
6.6.4	Ensure Custom Login Classes have Permissions Defined (Automated)	□	□
6.6.5	Ensure all Custom Login Classes Forbid Shell Access (Automated)	□	□
6.6.6	Ensure Predefined Login Classes are not used (Automated)	□	□
6.6.7	Ensure Remote Login Class for Authorization through External AAA (Automated)	□	□
6.6.8	Ensure login message is set (Automated)	□	□
6.6.9	Ensure local passwords require multiple character sets (Automated)	□	□
6.6.10	Ensure at least 4 set changes in local passwords (Automated)	□	□

6.6.11	Ensure local passwords are at least 10 characters (Automated)	□	□
6.6.12	Ensure SHA512 is used to hash local passwords (Automated)	□	□
6.6.13	Ensure SSH Key Authentication is not set for User Logins (Automated)	□	□
6.6.14	Ensure Multi-Factor is used with External AAA (Manual)	□	□
6.7	**NTP**		
6.7.1	Ensure External NTP Servers are set (Automated)	□	□
6.7.2	Ensure Multiple External NTP Servers are set (Automated)	□	□
6.7.3	Ensure NTP Boot-Server is set (Automated)	□	□
6.7.4	Ensure NTP uses version 4 (Automated)	□	□
6.7.5	Ensure Authentication Keys are used for all NTP Servers (Automated)	□	□
6.7.6	Ensure Different Authentication Keys for each NTP Server (Automated)	□	□
6.7.7	Ensure Strong Authentication Methods are used for NTP Authentication (Automated)	□	□
6.8	**Radius-server / Tacplus-server / Radius-options**		
6.8.1	Ensure External AAA Server is set (Automated)	□	□
6.8.2	Ensure Share-Secret is set for External AAA Servers (Automated)	□	□
6.8.3	Ensure a Different Shared Secret is Set for each External AAA Server (Manual)	□	□
6.8.4	Ensure MS-CHAPv2 RADIUS Authentication (Automated)	□	□
6.8.5	Ensure Source-Address is set for External AAA Servers (Automated)	□	□
6.9	**Root-Authentication**		
6.9.1	Ensure a complex Root Password is Set (Automated)	□	□
6.9.2	Ensure Root Password is Unique (Manual)	□	□
6.9.3	Ensure SSH Key Authentication is not set for Root Login (Automated)	□	□
6.10	**Services**		
6.10.1	**SSH**		
6.10.1.1	Ensure SSH Service is Configured if Remote CLI is Required (Manual)	□	□
6.10.1.2	Ensure SSH is Restricted to Version 2 (Automated)	□	□
6.10.1.3	Ensure SSH Connection Limit is Set (Automated)	□	□
6.10.1.4	Ensure SSH Rate Limit is Configured (Automated)	□	□
6.10.1.5	Ensure Remote Root-Login is denied via SSH (Automated)	□	□
6.10.1.6	Ensure Strong Ciphers are set for SSH (Automated)	□	□
6.10.1.7	Ensure Only Suite B Ciphers are set for SSH (Automated)	□	□
6.10.1.8	Ensure Strong MACs are set for SSH (Automated)	□	□

6.10.1.9	Ensure Strong Key Exchange Methods are set for SSH (Automated)	□	□
6.10.1.10	Ensure Only Suite B Key Exchange Methods are set for SSH (Automated)	□	□
6.10.1.11	Ensure Strong Key Signing Algorithms are set for SSH (Automated)	□	□
6.10.1.12	Ensure Only Suite B Based Key Signing Algorithms are set for SSH (Automated)	□	□
6.10.1.13	Ensure SSH Key Authentication is Disabled (Manual)	□	□
6.10.2	**Web-Management**		
6.10.2.1	Ensure Web-Management is not Set to HTTP (Automated)	□	□
6.10.2.2	Ensure Web-Management is Set to use HTTPS (Automated)	□	□
6.10.2.3	Ensure Web-Management is Set to use PKI Certificate for HTTPS (Automated)	□	□
6.10.2.4	Ensure Idle Timeout is Set for Web-Management (Automated)	□	□
6.10.2.5	Ensure Session Limited is Set for Web-Management (Automated)	□	□
6.10.2.6	Ensure Web-Management Interface Restriction is Set (Automated)	□	□
6.10.2.7	Ensure Web-Management Interface Restriction is set to OOB Management (Automated)	□	□
6.10.3	**XNM-* (JUNOScript)**		
6.10.3.1	Ensure XNM-Clear-Text Service is Not Set (Automated)	□	□
6.10.3.2	Ensure XNM-SSL Connection Limit is Set (Automated)	□	□
6.10.3.3	Ensure XNM-SSL Rate Limit is Set (Automated)	□	□
6.10.3.4	Ensure XNM-SSL SSLv3 Support is Not Set (Automated)	□	□
6.10.4	**NETCONF**		
6.10.4.1	Ensure NETCONF Rate Limit is Set (Automated)	□	□
6.10.4.2	Ensure NETCONF Connection Limit is Set (Automated)	□	□
6.10.5	**REST**		
6.10.5.1	Ensure REST is Not Set to HTTP (Automated)	□	□
6.10.5.2	Ensure REST is Set to HTTPS (Automated)	□	□
6.10.5.3	Ensure REST is Set to use PKI Certificate for HTTPS (Automated)	□	□
6.10.5.4	Ensure REST HTTPS is Set to use Mutual Authentication (Automated)	□	□
6.10.5.5	Ensure REST HTTPS Cipher List is Set (Automated)	□	□
6.10.5.6	Ensure REST HTTPS Cipher List is Set to Suite B Only (Automated)	□	□
6.10.5.7	Ensure REST API Explorer is Not Set (Automated)	□	□
6.10.5.8	Ensure REST Allowed Sources is Set (Automated)	□	□
6.10.5.9	Ensure REST Connection Limit is Set (Automated)	□	□

6.10.5.10	Ensure REST Service Address is Set (Automated)	□	□
6.10.5.11	Ensure REST Service Address is Set to OOB Management Only (Automated)	□	□
6.10.6	Ensure Telnet is Not Set (Automated)	□	□
6.10.7	Ensure Reverse Telnet is Not Set (Automated)	□	□
6.10.8	Ensure FTP Service is Not Set (Automated)	□	□
6.10.9	Ensure Finger Service is Not Set (Automated)	□	□
6.10.10	Ensure Unused DHCP Service is Not Set (Automated)	□	□
6.11	**Ports**		
6.11.1	Ensure Auxiliary Port is Set to Disabled (Automated)	□	□
6.11.2	Ensure Auxiliary Port is Set as Insecure If Used (Automated)	□	□
6.11.3	Ensure Console Port is Set to Disabled (Automated)	□	□
6.11.4	Ensure Console Port is Set as Insecure (Automated)	□	□
6.11.5	Ensure Log-out-on-disconnect is Set for Console (Automated)	□	□
6.12	**SYSLOG**		
6.12.1	Ensure External SYSLOG Host is Set with Any Facility and Informational Severity (Automated)	□	□
6.12.2	Ensure At Least 2 External SYSLOG Hosts are Set with Any/Info (Automated)	□	□
6.12.3	Ensure Local Logging is Set for Firewall Events (Automated)	□	□
6.12.4	Ensure Local Logging is Set for Authentication and Authorization Events (Automated)	□	□
6.12.5	Ensure Local Logging is Set for Interactive-Commands (Automated)	□	□
6.12.6	Ensure Local Logging is Set to Messages File (Automated)	□	□
6.13	Ensure Autoinstallation is Set to Disabled (Automated)	□	□
6.14	Ensure Configuration File Encryption is Set (Automated)	□	□
6.15	Ensure Multicast Echo is Set to Disabled (Automated)	□	□
6.16	Ensure Ping Record Route is Set to Disabled (Automated)	□	□
6.17	Ensure Ping Timestamps are Set to Disabled (Automated)	□	□
6.18	Ensure Time-Zone is Set to UTC (Automated)	□	□
6.19	Ensure Hostname is Not Set to Device Make or Model (Automated)	□	□
6.20	Ensure Default Address Selection is Set (Automated)	□	□
6.21	Ensure ICMP Redirects are Disabled for IPv4 (Automated)	□	□
6.22	Ensure ICMP Redirects are Disabled for IPv6 (Automated)	□	□
6.23	Ensure Password is Set for PIC-Console-Authentication (Automated)	□	□

Appendix: Change History

Date	Version	Changes for this version
Oct 11, 2017		_Audit Procedure, Remediation Procedure, Rationale Statement, Description_ on **[Recommendation] 2.4 Forbid Internal Source from External Networks** were updated.
Oct 18, 2017		_references, Notes, Default Value, Impact Statement, Audit Procedure, Remediation Procedure, Artifact Equation_ on **[Recommendation] 6.8.2 Require Shared Secret for External Authentication Servers** were updated.
Dec 4, 2018	1.1.0	_Listing Order_ on **[recommendation] 5.5P Ensure SHA1 is set for SNMPv3 authentication** was updated.
Dec 4, 2018	1.1.0	_Listing Order_ on **[recommendation] 5.5P Ensure SNMP is set to OOB management only** was updated.
Jan 11, 2019	1.1.0	_Listing Order_ on **[section] 8PP General Recommendations** was updated.
Jan 23, 2019	1.1.0	**[recommendation] 4.2.4P Ensure IS-IS Hello authentication check is not suppressed** was created.