the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Cisco IOS

Version 3.0.0-A2
August 2011

http://cisecurity.org
feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Cisco IOS*, provides prescriptive guidance for establishing a secure configuration posture for *Cisco Router running Cisco IOS* version *15.0M*. This guide was tested against *Cisco IOS IP Advanced IP Servoces v15.0.1* as installed by c880data-universalk9-mz.150-1.M4.bin. 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.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract 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 released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate *Cisco IOS* on a Cisco routing and switching platforms.

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:

Authors **Justin Opatrny**

Maintainers **Justin Opatrny**

Editors

Testers

Contributors and Reviewers **TBD**

Typographic 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

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

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-II Benchmark settings/actions

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

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1. Level-1 Benchmark

Description:

The Level-1 Benchmark for Cisco IOS represents a prudent level of minimum due care. These settings:

- Can be easily understood and performed by system administrators with any level of security knowledge and experience
- Are unlikely to cause an interruption of service to the operating system or the applications that run on it

1.1 Management Plane Level 1

Description:
Services, settings, and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative SSH, SNMP, TFTP for image file upload, and security protocols such as RADIUS and TACACS+.

1.1.1 Local Authentication, Authorization and Accounting (AAA) Rules (Level 1, Scorable)

Description: Rules in the Local authentication, authorization, and accounting (AAA) configuration class enforce device access control, provide a mechanism for tracking configuration changes, and enforcing security policy.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control. The services are only accessible once authenticated and accounting tracking services accessed. In addition, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

Warning:
Only "the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list." (1)

1.1.1.1 Require AAA Service

Description:
Verify centralized authentication, authorization, and accounting (AAA) service (new-model) is enabled.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Globally enable authentication, authorization and accounting (AAA) using new-model command

IOS:

```
hostname(config)#aaa new-model
```

Audit:
Perform the following to determine if AAA services are enabled:

IOS:

1. If the result includes a "no", the feature is not enabled

```
hostname#show run | incl aaa new-model
```

Default Value:
AAA is disabled by default.

References:

1. Cisco IOS Security Configuration Guide: Securing User Services, Release 15.0
2. Cisco IOS Security Command Reference, Release 15.0
3. NSA Router Security Configuration Guide

1.1.1.2 Require AAA Authentication for Login (Level 1, Scorable)

Description:

Verify authentication, authorization, and accounting (AAA) method(s) configuration for case-sensitive, local user login authentication.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

NOTE:
Only "the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list." (1)

Remediation:
Configure AAA authentication method(s) for login authentication.

IOS:

```
hostname(config)#aaa authentication login {default | aaa_list_name}
local-case
```

Audit:
Perform the following to determine if AAA authentication for login is enabled:

IOS:

1. If a result does not return, the feature is not enabled

```
hostname#show run | incl aaa authentication login
```

Default Value: AAA is disabled by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

1.1.1.3 Require AAA Authentication for Enable Mode (Level 1, Scorable)

Description:
Verify authentication, authorization, and accounting (AAA) methods for enable mode authentication.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control. The services are only accessible once authenticated and accounting tracking services accessed. In addition, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

Platform: IOS

Dependencies:

IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA authentication method(s) for enable authentication.

IOS:

```
hostname(config)#aaa authentication enable default {method} enable
```

Audit:
Perform the following to determine if AAA authentication for enable mode is enabled:

IOS:

1. If a result does not return, the feature is not enabled

```
hostname#show run | incl aaa authentication enable
```

Default Value:
AAA is disabled by default.

References:
1. Cisco IOS Security Command Reference
2. NSA Router Security Configuration Guide

1.1.1.4 Require AAA Authentication for Local Console and VTY Lines (Level 1, Scorable)

Description:

Verify configurations for all management lines require login using the default or a named authentication, authorization and accounting (AAA) method list. If selected, this rule applies for both local and network AAA.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure management lines to require login using the default or a named AAA authentication list. This configuration must be set individually for all lines (e.g. console, etc.)

IOS:

```
hostname(config)#line {aux | console | tty | vty} {line-number}
[ending-line-number]

hostname(config-line)#login authentication {default | aaa_list_name}
```

Audit:
Perform the following to determine if AAA authentication for line login is enabled:

IOS:

1. If the command does not return a results for each management access method, the feature is not enabled

```
hostname#sh run | sec line | incl login authentication
```

Default Value:
AAA login is disabled by default.

References:
1. Cisco IOS Security Command Reference
2. NSA Router Security Configuration Guide

3. Cisco AutoSecure

1.1.2 Access Rules

Description:
Rules in the access class enforce controls for device administrative connections.

1.1.2.1 Require Privilege Level 1 for Local Users (Level 1, Scorable)

Description:
Verify all locally defined users are set to the lowest level permissions as possible.

Rationale:
Default device configuration does not require strong user authentication potentially enabling unfettered access to an attacker that is able to reach the device. Creating a local account with privilege level 1 permissions only allows the local user to access the device with EXEC-level permissions and will be unable to modify the device without using the enable password. In addition, require the use of an encrypted password as well (see Section 1.1.4.4 - Require Encrypted User Passwords).

Platform: IOS

Dependencies:
IOS: None

Remediation:
Set the local user to privilege level 1.

IOS:

```
hostname(config)#username <LOCAL_USERNAME> privilege 1
```

Audit:
Perform the following to determine if a user with an encrypted password is enabled:

IOS:

1. Verify all username results return "privilege 1"

```
hostname#show run | incl privilege
```

Default Value:
Username-based authentication system is disabled.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.2.2 Require VTY Transport SSH (Level 1, Scorable)

Description:
Verify secure shell (SSH) access is configured on all vty management lines.

Rationale:
Configuring VTY access control restricts remote access to only those authorized to manage the device and prevents unauthorized users from accessing the system.

Platform: IOS

Dependencies:
IOS: 1.1.2.3Require SSH version 2

Remediation:
Apply VTY transport SSH on all management lines

IOS:

```
hostname(config)#line vty <line-number> <ending-line-number>

hostname(config-line)#transport input ssh
```

Audit:
Perform the following to determine if SSH is the only transport method for incoming VTY logins:

IOS:

1. The result should show only "ssh" for "transport input"

```
hostname#sh run | sec vty
```

Default Value:

No transport input is defined.

References:

1. Cisco IOS Terminal Services Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

1.1.2.3 Require Timeout for Login Sessions (Level 1, Scorable)

Description:
Verify device is configured to automatically disconnect sessions after a fixed idle time.

Rationale:
This prevents unauthorized users from misusing abandoned sessions. For example, if the network administrator leaves for the day and leaves a computer open with an enabled login session accessible. There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Review your local policies and operational needs to determine the best timeout value. In most cases, this should be no more than 10 minutes.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure device timeout (10 minutes) to disconnect sessions after a fixed idle time.

IOS:

```
hostname(config)#line {aux | console | tty | vty} {line-number}
[ending-line-number]

hostname(config-line)#exec-timeout <timeout_in_minutes>
<timeout_in_seconds>
```

Audit:

Perform the following to determine if the timeout is configured:

IOS:

1. Verify you return a result
   NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname# sh line vty 0 | begin Timeout
hostname# sh line vty 5 | begin Timeout
```

Default Value:

IOS: This is disabled by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco AutoSecure

1.1.2.4 Forbid Auxillary Port (Level 1, Scorable)

Description:
Verify that the EXEC process is disabled on the auxiliary (aux) port.

Rationale:
Unused ports should be disabled, if not required, since they provide a potential access path for attackers. Some devices include both an auxiliary and console port that can be used to locally connect to and configure the device. The console port is normally the primary port used to configure the device; even when remote, backup administration is required via console server or Keyboard, Video, Mouse (KVM) hardware. The auxiliary port is primarily used for dial-up administration via an external modem; instead, use other available methods.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable the EXEC process on the auxiliary port.

IOS:

```
hostname(config)# line aux 0
hostname(config-line)# no exec
hostname(config-line)# transport input none
```

Audit:

Perform the following to determine if the EXEC process for the aux port is disabled:

IOS:

1. Verify `no exec`

```
hostname#sh run | sec aux
```

2. Verify you see the following "Allowed input transports are none"

```
hostname#sh line aux 0 | incl input transports
```

Default Value:

The EXEC process is enabled by default on all lines.

References:

1. NSA Router Security Configuration Guide

1.1.2.5 Require VTY ACL (Level 1, Scorable)

Description:
Verify that the required VTY access control list (ACL) exists to restrict inbound management sessions for all VTY lines.

Rationale:
VTY ACLs control what addresses may attempt to log in to the router. Configuring VTY lines to use an ACL, restricts the sources a user can manage the device from. You should limit the specific host(s) and or network(s) authorized to connect to and configure the device, via an approved protocol, to those individuals or systems authorized to administrate the device. For example, you could limit access to specific hosts, so that only network managers can configure the devices only by using specific network management workstations. Make sure you configure all VTY lines to use the same ACL.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the VTY ACL that will be used to restrict management access to the device.

IOS:

```
hostname(config)#access-list <vty_acl_number> permit tcp
<vty_acl_block_with_mask> any
hostname(config)#access-list <vty_acl_number> permit tcp host
<vty_acl_host> any
hostname(config)#deny ip any any log
```

Audit:
Perform the following to determine if the ACL is created:

IOS:

1. Verify the appropriate access-list definitions

```
hostname#sh ip access-list <vty_acl_number>
```

Default Value:

No access lists are defined.

References:

1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.2.6 Require SSH Access Control (Level 1, Scorable)

Description:
Verify that management access to the device is restricted to appropriate management subnets.

Rationale:
Configuring access control to restrict remote access to those systems authorized to manage the device prevents unauthorized users from accessing the system.

Platform: IOS

Dependencies:
IOS: 1.1.2.5 Require VTY ACL

Remediation:
Configure remote management access control restrictions for all VTY lines.

IOS:

```
hostname(config)#line {aux | console | tty | vty} <line-number>
<ending-line-number>
hostname(config-line)# access-class <vty_acl_number> in
```

Configure remote management restrictions for SSH.

Audit:
Perform the following to determine if the ACL is set:

IOS:

1. Verify you see the access-class defined

```
hostname#sh run | sec {aux | console | tty | vty} <line-number>
<ending-line-number>
```

Default Value:

SSH access is not enabled by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.3 Banner Rules

Description:

Rules in the banner class communicate legal rights to users.

Rationale:

"Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

1. Banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of networks
2. Banners may be used to generate consent to real-time monitoring under Title III
3. Banners may be used to generate consent to the retrieval of stored files and records pursuant to the SCA
4. In the case of a non-government network, banners may establish the network owner's common authority to consent to a law enforcement search" (17)

References:

1. US Department of Justice – Cybercrime – Sample Network Login Banner

1.1.3.1 Require EXEC Banner (Level 1, Scorable)

Description:
Verify an authorized EXEC banner is defined.

Rationale:
Presentation of an EXEC banner occurs before displaying the enable prompt, after starting an EXEC process, normally after displaying the message of the day and login banners and after the user logs into the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the EXEC banner presented to a user when accessing the devices enable prompt.

IOS:

```
hostname(config)#banner exec c
Enter TEXT message.  End with the character 'c'.

<banner-text>

c
```

Audit:
Perform the following to determine if the exec banner is set:

IOS:

1. If the command does not return a result, the banner is not enabled

```
hostname#sh run | beg banner exec
```

Default Value:
There is no default EXEC banner.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.3.2 Require Login Banner (Level 1, Scorable)

Description:
Verify an authorized login banner is defined.

Rationale:
Presentation of a login banner, to a user attempting to access the device, occurs before the display of login prompts and usually appears after the message of the day banner.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the login banner presented to a user attempting to access the device.

IOS:

```
hostname(config)#banner login c
Enter TEXT message.  End with the character 'c'.
```

```
<banner-text>

c
```

Audit:
Perform the following to determine if the login banner is set:

1. If the command does not return a result, the banner is not enabled

IOS:

```
hostname#sh run | beg banner login
```

Default Value:
There is no default login banner.

References:

1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.3.3 Require MOTD Banner (Level 1, Scorable)

Description:
Verify an authorized message of the day (MOTD) banner is defined.

Rationale:
Presentation of a MOTD banner occurs when a user first connects to the device, normally before displaying the login banner and login prompts.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the message of the day (MOTD) banner presented when a user first connects to the device.

IOS:

```
hostname(config)#banner motd c
Enter TEXT message.  End with the character 'c'.

<banner-text>

c
```

Audit:
Perform the following to determine if the login banner is set:

1. If the command does not return a result, the banner is not enabled

IOS:

```
hostname#sh run | beg banner motd
```

Default Value:
There is no default MOTD banner.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.4 Password Rules

Description:

Rules in the password class enforce secure, local device authentication credentials.

Refrain from using common usernames such as admin, administrator, cisco, etc. Instead, use a more difficult to guess username. In addition, follow password complexity rules of having a password of at least eight characters, using upper and lower case letters, numbers, and/or special characters.

1.1.4.1 Require Enable Secret (Level 1, Scorable)

Description:
Verify an enable secret password is defined using strong encryption to protect access to privileged EXEC mode (enable mode) which is used to configure the device.

Rationale:
Requiring the enable secret setting protects privileged EXEC mode. By default, a strong password is not required, a user can just press the Enter key at the Password prompt to start privileged mode. The enable password command causes the device to enforce use of a password to access privileged mode. Enable secrets use a one-way cryptographic hash (MD5). This is preferred to Level 7 enable passwords that use a weak, well-known, and easily reversible encryption algorithm.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure a strong, enable secret password.

IOS:

```
hostname(config)#enable secret <ENABLE_SECRET>
```

Audit:
Perform the following to determine enable secret is set:

1. If the command does not return a result, the enable password is not set.

IOS:

```
hostname#sh run | incl enable secret
```

Default Value:
An enable password is not configured by default.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.4.2 Require Password Encryption Service (Level 1, Scorable)

Description:
Verify encryption of passwords in device configuration is enabled.

Rationale:
This requires passwords to be encrypted in the configuration file to prevent unauthorized users from learning the passwords just by reading the configuration. When not enabled, many of the device's passwords will be rendered in plain text in the configuration file. This service ensures passwords are rendered as encrypted strings preventing an attacker from easily determining the configured value.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Enable password encryption service to protect sensitive access passwords in the device configuration.

```
hostname(config)#service password-encryption
```

Audit:
Perform the following to determine if a user with an encrypted password is enabled:

1. Ensure a result that matches the command return

```
hostname#sh run | incl service password-encryption
```

Default Value:
There no passwords are encrypted.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.1.4.3 Require Encrypted Line Passwords (Level 1, Scorable)

Description:
Verify an access password with encryption is configured on all management lines.

Rationale:
This requires a password to be set on each line. Note, that given the use of local usernames (level 1) or TACACS+ (level 2) line passwords will not be used for authentication. There they are included as a fail-safe to ensure that some password is required for access to the router in case other AAA options are not configured. Low quality passwords are easily guessed possibly providing unauthorized access to the router.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure each line with an encrypted password

```
hostname(config)# line {aux | console | tty | vty} <line-number>
<ending-line-number>
hostname(config-line)#password <LINE_PASSWORD>
```

Audit:
Perform the following to determine a line password is set:

1. Verify you see the line password set

```
hostname#sh run | sec aux | console | tty | vty} <line-number> <ending-
line-number>
```

Default Value:
There is no default line password.

References:
1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.4.4 Require Encrypted User Passwords (Level 1, Scorable)

Description:
Verify at least one local user exists and ensure all have encrypted passwords.

Rationale:
Default device configuration does not require strong user authentication potentially enabling unfettered access to an attacker that is able to reach the device. Creating a local

account with an encrypted password enforces login authentication and provides a fallback authentication mechanism for configuration in a named method list in a situation where centralized authentication, authorization, and accounting services are unavailable.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Create a local user with an encrypted, complex (not easily guessed) password.

IOS:

```
hostname(config)#username <LOCAL_USERNAME> secret <LOCAL_PASSWORD>
```

Audit:
Perform the following to determine if a user with an encrypted password is enabled:

1. If a result does not return a result, the feature is not enabled

IOS:

```
hostname#show run | incl username
```

Default Value:
Username-based authentication system is disabled.

References:

1. Cisco IOS Security Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.1.5 SNMP Rules

Description:

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.

Rationale:
SNMP allows management and monitoring of networked devices. SNMP should be disabled unless you absolutely require it for network management purposes.

If you require SNMP, use SNMPv3 which uses authentication, authorization, and data privatization (encryption). Be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the enable password, line password, or other authentication credentials.

1.1.5.1 Forbid SNMP Read and Write Access (Level 1, Scorable)

Description:

If not in use, disable simple network management protocol (SNMP), read and write access.

Rationale:
SNMP read access allows remote monitoring and management of the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable SNMP read and write access if not in used to monitor and/or manage device.

IOS:

```
hostname(config)#no snmp-server
```

Audit:

IOS:

1. Verify the result reads "SNMP agent not enabled"

```
hostname# show snmp community
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.2 Forbid SNMP Community String private (Level 1, Scorable)

Description:
Verify configuration does not contain default simple network management protocol (SNMP) community strings. The configuration cannot include snmp-server community commands with prohibited community strings.

Rationale:
The default community string "private" is well known. Using easy to guess, well known community string poses a threat that an attacker can effortlessly gain unauthorized access to the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:

Disable the default SNMP community string "private"

IOS:

```
hostname(config)#no snmp-server community {private}
```

Audit:
Perform the following to determine if the private community string is enabled:

IOS:

1. Ensure `private` does not show as a result

```
hostname# show snmp community
```

Default Value:

SNMP is disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.3 Forbid SNMP Community String public (Level 1, Scorable)

Description:
Verify configuration does not contain default simple network management protocol (SNMP) community strings. The configuration cannot include snmp-server community commands with prohibited community strings.

Rationale:
The default community string "public" is well known. Using easy to guess, well known community string poses a threat that an attacker can effortlessly gain unauthorized access to the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable the default SNMP community string "public"

IOS:

```
hostname(config)#no snmp-server community {public}
```

Audit:
Perform the following to determine if the public community string is enabled:

IOS:

1. Ensure `public` does not show as a result

```
hostname# show snmp community
```

Default Value:

SNMP is disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.4 Forbid SNMP Write Access (Level 1, Scorable)

Description:
Unless absolutely necessary, verify the device does not allow simple network management protocol (SNMP) write access.

Rationale:
Enabling SNMP read-write enables remote management of the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable SNMP write access.

IOS:

```
hostname(config)#no snmp-server community {write_community_string}
```

Audit:
Perform the following to determine if a read/write community string is enabled:

IOS:

1. Verify the result does not show a community string with a "RW"

```
hostname#show run | incl snmp-server community
```

Default Value:

SNMP is disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.5 Forbid SNMP without ACL (Level 1, Scorable)

Description:
Verify all simple network management protocol (SNMP) access is restricted using an access control list (ACL).

Rationale:
If ACLs are not applied, then anyone with a valid SNMP community string can potentially monitor and manage the router. An ACL should be defined and applied for all SNMP access to limit access to a small number of authorized management stations segmented in a trusted management zone. If possible, use SNMPv3 which uses authentication, authorization, and data privatization (encryption).

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure authorized SNMP community string and restrict access to authorized management systems.

IOS:

```
hostname(config)#snmp-server community <community_string>  {ro | rw}
<snmp_access-list_number>
```

Audit:
Perform the following to determine if an ACL is enabled:

IOS:

1. Verify the result shows a number after the community string

```
hostname#show run | incl snmp-server community
```

Default Value:

SNMP does not have an access list.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.6 Require a Defined SNMP ACL (Level 1, Scorable)

Description:
Verify a defined simple network management protocol (SNMP) access control list (ACL) exists with rules for restricting SNMP access to the device.

Rationale:

SNMP ACLs control what addresses are authorized to manage and monitor the device via SNMP. If ACLs are not applied, then anyone with a valid SNMP community string may monitor and manage the router. An ACL should be defined and applied for all SNMP community strings to limit access to a small number of authorized management stations segmented in a trusted management zone.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure SNMP ACL for restricting access to the device from authorized management stations segmented in a trusted management zone.

IOS:

```
hostname(config)#access-list <snmp_acl_number> permit <snmp_access-list>
hostname(config)#access-list deny any log
```

Audit:
Perform the following to determine if the ACL is created:

IOS:

1. Verify you the appropriate access-list definitions

```
hostname#sh ip access-list <snmp_acl_number>
```

Default Value:

SNMP does not have an access list.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.1.5.7 Forbid SNMP Traps (Level 1, Scorable)

Description:
Verify the device is not configured to send SNMP traps.

Rationale:
SNMP has the ability to submit traps.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable SNMP traps.

IOS:

```
hostname(config)#no snmp-server enable traps [notification-type]
```

Audit:
Perform the following to determine if SNMP traps are enabled:

IOS:

1. If the command returns configuration values, then SNMP is enabled.

```
hostname# show run snmp-server
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M

1.1.5.8 Require SNMP Trap Server When Using SNMP (Level 1, Scorable)

Description:
Verify the device is configured to submit SNMP traps only to authorized systems required to manage the device.

Rationale:
If SNMP is enabled for device management and device alerts are required, then ensure the device is configured to submit traps to authorize management systems.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure authorized SNMP trap community string and restrict sending messages to authorized management systems.

IOS:

```
hostname(config)#snmp-server host {ip_address} {trap_community_string}
snmp
```

Audit:
Perform the following to determine if SNMP traps are enabled:

IOS:

1. If the command returns configuration values, then SNMP is enabled.

```
hostname# show run snmp-server
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M

1.1.1.1 Allow SNMP Traps on When SNMP Trap Server Defined (Level 1, Scorable)

Description:
Verify the device is not configured to send SNMP traps.

Rationale:
SNMP has the ability to submit traps.

Platform: IOS

Dependencies:
IOS: 1.1.5.7 Require SNMP Trap Server When Using SNMP

Remediation:
Disable SNMP traps.

IOS:

```
hostname(config)#snmp-server enable traps snmp authentication linkup
linkdown coldstart
```

Audit:
Perform the following to determine if SNMP traps are enabled:

IOS:

1. If the command returns configuration values, then SNMP is enabled.

```
hostname# show run snmp-server
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M

1.1.1.2 Require Group for SNMPv3 Access (Level 2, Scorable) (Level 1, Scorable)

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. AES128 is the minimum strength encryption method that should be deployed.

AES Encryption is only available in IOS versions that support encryption algorithms.

Platform: IOS

Dependencies:
IOS: None

Remediation:
For each SNMPv3 group created on your router add privacy options by issuing the following command...

IOS:

```
hostname(config)#snmp-server group <group_name> v3 priv
```

Audit:

IOS:

1. Verify the result show the appropriate group name and security model

```
hostname# show snmp groups
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.1.1.3 Require AES128 or Better Encryption for SNMPv3 Access (Level 2, Scorable) (Level 1, Scorable)

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. AES128 is the minimum strength encryption method that should be deployed.

AES Encryption is only available in IOS versions that support encryption algorithms.

Platform: IOS

Dependencies:
IOS: 1.1.5.6 Forbid SNMP without ACL
1.1.5.8 Require Group for SNMPv3 Access

Remediation:
For each SNMPv3 user created on your router add privacy options by issuing the following command...

IOS:

```
hostname(config)#snmp-server user <user_name> <group_name> v3 auth sha
<auth_password> priv aes 256 <priv_password> <acl_name_or_number>
```

Audit:

IOS:

1. Verify the result show the appropriate user name and security settings

```
hostname# show snmp user
```

Default Value:

SNMP is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.2 Control Plane Level 1

Description:
The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

1.2.1 Clock Rules

Description:

Rules in the clock class enforce device time and timestamp settings.

1.2.1.1 Require Clock Timezone – UTC (Level 1, Scorable)

Description:
Verify the time zone for the device clock is configured to coordinated universal time (UTC) explicitly.

Rationale:
Configuring devices with a universal time zone eliminates difficulty troubleshooting issues across different time zones and correlating time stamps for disparate log files across multiple devices. Set the clock to UTC 0 (no offset) to aid in root cause analysis of attacks and network issues.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the devices clock time zone to coordinated universal time (UTC) explicitly.

IOS:

```
hostname(config)#clock timezone UTC 0
```

Audit:
Perform the following to determine if the time zone is set:

IOS:

1. Verify the result shows UTC

```
hostname#show clock
```

Default Value:

The default clock time zone is UTC.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.2.1.2 Forbid Daylight Savings Time Clock Adjustments (Level 1, Scorable)

Description:
Verify the clock is not configured to adjust the device clock for daylight saving time.

Rationale:
The difficulty of troubleshooting and correlating issues across different time zones increases if the time stamps of individual logs need to be adjusted for summer time clock settings. Timestamp adjustments can lead to errors when correlating logs across multiple devices. Employ coordinated universal time (UTC) instead of local time zones and do not use summer-time, daylight saving, clock adjustments.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable clock summer-time adjustments.

IOS:

```
hostname(config)#no clock summer-time
```

Audit:
Perform the following to determine if summer-time is not enabled:

IOS:

1. Verify no results return.

```
hostname#sh run | incl summer-time
```

Default Value:

Daylight savings time is disabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide
3. Cisco Guide to Harden Cisco IOS Devices

1.2.1.3 Require Daylight Savings Time Clock When Using Local Time Zone (Level 1, Scorable)

Description:
Verify the clock is configured to adjust the device clock for daylight saving time only when using a local time zone.

Rationale:
Only configure daylight savings time if your organization's policy requires configuring devices for local time. Time zone and daylight savings adjustment settings should be consistent across all devices to eliminate difficulty troubleshooting issues and correlating time stamps for disparate log files across multiple devices.

1.2.1.3.1 Setup Local Time Zone (Level 1, Scorable)

Description:
Verify the clock is configured for the local time zone.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the local time zone.

IOS:

```
hostname(config)#clock timezone [-]hours [minutes]
```

Audit:
Perform the following to determine if the local time zone is configured:

IOS:

1. Verify the result shows configured local time zone.

```
hostname#sh clock
```

Default Value:

Daylight savings time is disabled.

References:

1. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M

1.2.1.3.2 Set Daylight Savings Dates (Level 1, Scorable)

Description:
Verify the clock is configured for the appropriate daylight savings dates for the local time zone.

Platform: IOS

Dependencies:
IOS: 1.2.1.3.1 Setup Local Time Zone

Remediation:
Configure the appropriate daylight savings dates for the local time zone.

IOS:

```
hostname(config)#clock summer-time zone date {day month | month day}
year hh:mm {day month | month day} yy:mm [offset]
```

Audit:
Perform the following to determine if the local time zone is configured:

IOS:

1. Verify the result shows the summer-time dates are configured properly.

```
hostname#sh run | incl summer-time
```

Default Value:

Daylight savings time is disabled.

References:

1. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M

1.2.1.3.3 Setup Daylight Savings Recurrence (Level 1, Scorable)

Description:
Verify the clock is configured for the appropriate daylight savings recurrence for the local time zone.

Platform: IOS

Dependencies:
IOS: 1.2.1.3.2 Set Daylight Savings Dates

Remediation:
Configure the appropriate daylight savings recurrence for the local time zone.

IOS:

```
hostname(config)#clock summer-time zone recurring {week weekday month
hh:mm week weekday month hh:mm [offset]
```

Audit:
Perform the following to determine if the local time zone is configured:

IOS:

1. Verify the result shows the summer-time recurrence is configured properly.

```
hostname#sh run | incl summer-time
```

Default Value:

Daylight savings time is disabled.

References:

1. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M

1.2.2 Global Service Rules

Description:

Rules in the global service class enforce server and service controls that protect against attacks or expose the device to exploitation.

Rationale:
Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.

1.2.2.1 SSH

Description:
Ensure use of SSH remote console sessions to Cisco 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.

Due to this extra protection, all remote console sessions should use SSH.

1.2.2.2 Configure Prerequisites for the SSH Service (Level 1, Scorable)

1.2.2.2.1 Configure the Host Name (Level 1, Scorable)

Description:
Configure the router's domain name

Rationale:
The domain name is prerequisite for setting up SSH.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure an appropriate host name for the router.

IOS:

```
hostname(config)#hostname <router_name>
```

Audit:
Perform the following to determine if the local time zone is configured:

IOS:

1. Verify the result shows the summer-time recurrence is configured properly.

```
hostname#sh run | incl summer-time
```

Default Value:

The default hostname is Router.

References:

1. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M

1.2.2.2.2 Configure the Domain Name (Level 1, Scorable)

Description:
Configure the router's host name

Rationale:
The host name is prerequisite for setting up SSH.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure an appropriate domain name for the router.

IOS:

```
hostname (config)#ip domain name <domain-name>
```

Audit:
Perform the following to determine if the local time zone is configured:

IOS:

1. Verify the host name is configured properly.

```
hostname#sh run | incl domain name
```

Default Value:

No domain name is setup.

References:

1. Cisco IOS IP Addressing Services Command Reference, Release 15.0M

1.2.2.2.3 Generate the RSA Key Pair (Level 1, Scorable)

Description:

Generate an RSA key pair

Rationale:

An RSA key pair is prerequisite for setting up SSH and should be at least 2048 bits

Platform: IOS

Dependencies:
IOS: None

Remediation:
Generate an RSA key pair for the router.

IOS:

```
hostname (config)#crypto key generate rsa general-keys modulus {2048}
```

Audit:
Perform the following to determine if the RSA key pair is configured:

IOS:

1. Verify the host name is configured properly.

```
hostname#sh run | incl crypto key
```

Default Value:

RSA key pairs do not exist

References:

1. Cisco IOS Security Command Reference, Release 15.0

1.2.2.2.4 Configure the SSH Timeout (Level 1, Scorable)

Description:

Verify that an idle timeout has been configured for SSH sessions.

Rationale:
This reduces the risk of an administrator leaving an authenticated session logged in for an extended period of time.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the SSH timeout

IOS:

```
hostname(config)#ip ssh timeout [60]
```

Audit:
Perform the following to determine if the SSH timeout is configured:

IOS:

1. Verify the timeout is configured properly.

```
hostname#sh ip ssh
```

Default Value:

SSH timeouts are not setup by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0

1.2.2.2.5 Limit the number of SSH Authentication Tries (Level 1, Scorable)

Description:

Verify the device is configured to limit the number of SSH authentication attempts

Rationale:
This limits the number of times an unauthorized user can attempt a password without having to establish a new SSH login attempt.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the SSH timeout

IOS:

```
hostname(config)#ip ssh authentication-retries [3]
```

Audit:
Perform the following to determine if SSH authentication retries is configured:

IOS:

1. Verify the authentication retries is configured properly.

```
hostname#sh ip ssh
```

Default Value:

SSH authentication retries are not setup by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0

1.2.2.3 Require SSH version 2 (Level 1, Scorable)

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.

Cisco routers support both versions, but due to the weakness of SSH Version 1 only the later standard should be used.

Platform: IOS

Dependencies:
IOS: 1.1.2.2 Configure Prerequisites for the SSH Service

Remediation:
Configure the router to use SSH version 2

IOS:

```
hostname(config)#ip ssh version 2
```

Audit:
Perform the following to determine if SSH version 2 is configured:

IOS:

1. Verify that SSH version 2 is configured properly.

```
hostname#sh ip ssh
```

Default Value:

SSH is not setup by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0

1.2.2.4 Forbid CDP Run Globally (Level 1, Scorable)

Description:
Disable Cisco Discovery Protocol (CDP) service at device level.

Rationale:
The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in network monitoring and troubleshooting situations but is considered a security risk because of the amount of information provided

from queries. In addition, there have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless necessary.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable Cisco Discovery Protocol (CDP) service globally.

IOS:

```
hostname(config)#no cdp run
```

Audit:
Perform the following to determine if CDP is enabled:

IOS:

1. Verify the result shows "CDP is not enabled"

```
hostname#show cdp
```

Default Value:

CDP is enabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.5 Forbid Finger Service (Level 1, Scorable)

Description:
Disable the finger server.

Rationale:
Finger is used to find out which users are logged into a device. This service is rarely used in practical environments and can potentially provide an attacker with useful information.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable the finger server.

```
hostname(config)#no ip finger
```

Audit:
Perform the following to determine if Finger is enabled:

1. Verify the no result return

```
hostname#show run | incl finger
```

Default Value:

Finger is disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.6 Forbid IP BOOTP Server (Level 1, Scorable)

Description:
Disable bootstrap protocol (BOOTP) server.

Rationale:
BootP allows a router to issue IP addresses. This should be disabled unless there is a specific requirement.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable the bootp server.

IOS:

```
hostname(config)#no ip bootp server
```

Audit:
Perform the following to determine if bootp is enabled:

IOS:

1. Verify a "no ip bootp server" result returns

```
hostname#show run | incl bootp
```

Default Value:

bootp is enabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.7 Forbid DHCP Server Service (Level 1, Scorable)

Description:
Verify the device is not configured as a Dynamic Host Configuration Protocol (DHCP) server.

Rationale:
The DHCP server supplies automatic configuration parameters, such as dynamic IP address, to requesting systems. A dedicated server located in a secured management zone should be used to provide DHCP services instead. Attackers can potentially be used for denial-of-service (DoS) attacks.

Platform: IOS

Dependencies:
IOS: None

Remediation:

Disable the DHCP server.

IOS:

```
hostname(config)#no ip bootp server
```

Audit:
Perform the following to determine if the DHCP service is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl dhcp
```

Default Value:

DHCP is disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.8 Forbid Identification Server (Level 1, Scorable)

Description:
Disable the identification (identd) server.

Rationale:
Identification protocol enables identifying a users transmission control protocol (TCP) session. This information disclosure could potentially provide an attacker with information about users.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable the ident server.

IOS:

```
hostname(config)#no ip identd
```

Audit:
Perform the following to determine if identd is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl identd
```

Default Value:
Identd is disabled.

References:
1. NSA Router Security Configuration Guide
2. Cisco Guide to Harden Cisco IOS Devices

1.2.2.9 Forbid HTTP (to include ADSM) Services (Level 1, Scorable)

Description:
Disable the native HTTP services.

Rationale:
HTTP services allow remote management of routers. However, when using simple HTTP, authentication sends passwords in the clear. This could allow unauthorized access to and mis-management of the router. HTTP services should be disabled. If you require a web management interface, ensure use of the HTTPS server functionality.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Disable the HTTP services.

IOS:

```
hostname(config)#no ip http server
hostname(config)#no ip http secure-server
```

Audit:
Perform the following to determine if the HTTP services are enabled:

IOS:

1. Verify both "no ip http server" and "no ip http secure-server" results return

```
hostname#show run | incl http server
```

Default Value:

The HTTP and HTTPS servers are disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.10 Forbid Remote Startup Configuration (Level 1, Scorable)

Description:
Disable auto-loading of remote configuration files from a network server.

Rationale:
Service config allows the device to autoload its startup configuration from a remote device (e.g. a tftp server). The protocols used to transfer configurations files, such as trivial file transfer protocol (TFTP) and file transfer protocol (FTP), are not secure. Since these methods are insecure, an attacker could potentially compromise, collect, or spoof the remote configuration service enabling malicious reconfiguration of the device.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable auto loading of remote configurations files from a network server.

IOS:

```
hostname(config)#no boot network
```

```
hostname(config)#no service config
```

Audit:
Perform the following to determine if boot network is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl boot network
```

2. Verify no result returns

```
hostname#show run | incl service config
```

Default Value:

Boot network and service config are both disabled.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.2.11 Require TCP keepalives-in Service (Level 1, Scorable)

Description:
Verify transmission control protocol (TCP) keepalives-in service is enabled to kill abnormally terminated sessions.

Rationale:
Stale connections use resources and could potentially be hijacked to gain illegitimate access. The TCP keepalives-in service generates keepalive packets on idle incoming network connections (initiated by remote host). This service allows the device to detect when the remote host fails and drop the session. If enabled, keepalives are sent once per minute on idle connections. The closes connection is closed within five minutes if no keepalives are received or immediately if the host replies with a reset packet.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Enable TCP keepalives-in service to kill sessions where the remote side has died.

IOS:

```
hostname(config)#service tcp-keepalives-in
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify a command string result returns

```
hostname#show run | incl service tcp
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.12 Require TCP keepalives-out Service (Level 1, Scorable)

Description:
Use transmission control protocol (TCP) keepalives-out service to kill abnormally terminated sessions.

Rationale:
Stale connections use resources and could potentially be hijacked to gain illegitimate access. The TCP keepalives-out service generates keepalive packets on idle outgoing network connections (initiated by remote host). This service allows the device to detect when the remote host fails and drop the session. If enabled, keepalives are sent once per minute on idle connections. The connection is closed within five minutes if no keepalives are received or immediately if the host replies with a reset packet.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Enable TCP keepalives-out service to kill sessions where the remote side has died.

IOS:

```
hostname(config)#service tcp-keepalives-out
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify a command string result returns

```
hostname#show run | incl service tcp
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.13 Forbid tcp-small-servers (Level 1, Scorable)

Description:
Disable unnecessary services such as echo, discard, chargen, etc.

Rationale:
TCP small services: echo, chargen and daytime (including UDP versions) are rarely used. These services can be leveraged by attackers to launch denial-of-service (DoS) and other attacks that would be prevented by packet inspection filters provided these services are disabled. Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable unnecessary services such as echo, discard, chargen, etc.

IOS:

```
hostname(config)#no service tcp-small-servers
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl tcp-small-servers
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.14 Forbid udp-small-servers (Level 1, Scorable)

Description:
Disable unnecessary services such as echo, discard, chargen, etc.

Rationale:
TCP small services: echo, chargen and daytime (including UDP versions) are rarely used. These services can be leveraged by attackers to launch denial-of-service (DoS) and other attacks that would be prevented by packet inspection filters provided these services are disabled. Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable unnecessary services such as echo, discard, chargen, etc.

IOS:

```
hostname(config)#no service udp-small-servers
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl udp-small-servers
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.2.15 Forbid TFTP Server (Level 1, Scorable)

Description:
Disable trivial file transfer protocol (TFTP) server service.

Rationale:

Trivial file transfer protocol (TFTP) is not a secure service. It allows anyone who can connect to the device to transfer files, such as access control lists, router configurations and system images.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable tftp-server service.

IOS:

```
hostname(config)#no tftp-server flash:<name_of_ios>.bin
hostname(config)#no tftp-server flash:vlan.dat
hostname(config)#no tftp-server nvram:startup-config
hostname(config)#no tftp-server nvram:private-config
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl tftp-server
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.3 Logging Rules

Description:

Rules in the logging class enforce controls that provide a record of system activity and events.

Rationale:
Logging should be enabled to allow monitoring of both operational and security related events. Logs are critical for responding to general as well as security incidents. In addition, device logging is highly recommended or required by most security regulations.

1.2.3.1 Require System Logging (Level 1, Scorable)

Description:

Verify logging is enabled to allow monitoring of both operational and security related events.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Enable system logging.

IOS:

```
hostname(config)#logging on
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify no result returns

```
hostname#show run | incl logging on
```

Default Value:

Logging is disabled by default.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.3.2 Require Logging Buffer (Level 1, Scorable)

Description:

Verify buffered logging (with minimum size) is configured to enable logging to internal device memory buffer.

Rationale:
The device can copy and store log messages to an internal memory buffer. The buffered data is available only from a router exec or enabled exec session. This form of logging is useful for debugging and monitoring when logged in to a router.

Platform: IOS

Dependencies:
IOS: 1.2.3.1 Require System Logging

Remediation:
Configure buffered logging (with minimum size). Recommended size is 16000.

IOS:

```
hostname(config)#logging buffered [log_buffer_size]
```

Audit:
Perform the following to determine if the feature is enabled:

IOS

1. Verify a command string result returns

```
hostname#show run | logging buffered
```

Default Value:

Logging is disabled by default.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco AutoSecure

1.2.3.3 Require Logging to Device Console (Level 1, Scorable)

Description:

Verify logging to device console is enabled and limited to a rational severity level to avoid impacting system performance and management.

Rationale:
This configuration determines the severity of messages that will generate console messages. Logging to console should be limited only to those messages required for immediate troubleshooting while logged into the device. This form of logging is not persistent; messages printed to the console are not stored by the router. Console logging is handy for operators when they use the console.

Warning: It is possible that misconfiguring the logging level to be excessively verbose or excessive log messages on the console could make it impossible to manage the device, even on the console.

Platform: IOS

Dependencies:
IOS: 1.2.3.1 Require System Logging

Remediation:
Configure console logging level.

IOS:

```
hostname(config)#logging console critical
```

Audit:
Perform the following to determine if the feature is enabled:

IOS:

1. Verify a command string result returns

```
hostname#show run | incl logging console
```

Default Value:

Log all messages when enabled.

References:

1. Cisco IOS Network Management Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

1.2.3.4 Require Logging to Syslog Server (Level 1, Scorable)

Description:

Designate one or more syslog servers to centrally record system logs.

Rationale:
Cisco routers can send their log messages to a Unix-style Syslog service. A syslog service simply accepts messages and stores them in files or prints them according to a simple configuration file. This form of logging is best because it can provide protected long-term storage for logs (the devices internal logging buffer has limited capacity to store events.) In addition, logging to an external system is highly recommended or required by most security standards. If desired or required by policy, law and/or regulation, enable a second syslog server for redundancy.

Platform: IOS

Dependencies:
IOS: 1.2.3.1 Require System Logging

Remediation:
Designate one or more syslog servers by IP address.

IOS:

```
hostname(config)#logging host syslog_server
```

Audit:
Perform the following to determine if a syslog server is enabled:

IOS:

1. Verify one or more IP address(es) returns

```
hostname#sh log | incl Logging to
```

Default Value:

Logs are not sent to any remote host.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.3.5 Require Logging Trap Severity Level (Level 1, Scorable)

Description:

Verify simple network management protocol (SNMP) trap and Syslog are set to required level.

Rationale:
This determines the severity of messages that will generate simple network management protocol (SNMP) trap and or syslog messages. This setting should be set to either "debugging" (7) or "informational" (6), but no lower.

Platform: IOS

Dependencies:
IOS: 1.2.3.1 Require System Logging

Remediation:
Configure SNMP trap and syslog logging level.

IOS:

```
hostname(config)#logging trap informational
```

Audit:
Perform the following to determine if a syslog server for SNMP traps is enabled:

IOS:

1. Verify "level informational" returns

```
hostname#sh log | incl Trap logging
```

Default Value:

Traps are not sent to remote hosts. When configured, **the default in IOS 11.3 and later is informational.**

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.3.6 Require Service Timestamps for Debug Messages (Level 1, Scorable)

Description:

Configure debug messages to include timestamps.

Rationale:
Including timestamps in log messages allows correlating events and tracing network attacks across multiple devices. Enabling service timestamp to mark the time log messages were generated simplifies obtaining a holistic view of events enabling faster troubleshooting of issues or attacks.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure debug messages to include timestamps.

IOS:

```
hostname(config)#service timestamps debug datetime {msec} {show-
timezone}
```

Audit:
Perform the following to determine if the additional detail is enabled:

IOS:

1. Verify a command string result returns

```
hostname#sh run | incl service timestamps
```

Default Value:

Basic time stamps are applied to debug messages

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.3.7 Require Service Timestamps in Log Messages (Level 1, Scorable)

Description:

Configure logging to include message timestamps.

Rationale:
Including timestamps in log messages allows correlating events and tracing network attacks across multiple devices. Enabling service timestamp to mark the time log messages

were generated simplifies obtaining a holistic view of events enabling faster troubleshooting of issues or attacks.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure logging to include message timestamps.

IOS:

```
hostname(config)#service timestamps log datetime {msec} {show-timezone}
```

Audit:
Perform the following to determine if the additional detail is enabled:

IOS:

1. Verify a command string result returns

```
hostname#sh run | incl service timestamps
```

Default Value:
Basic time stamps are applied to logging messages.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices
4. Cisco AutoSecure

1.2.4 NTP Rules

Description:

Network Time Protocol allows administrators to set the system time on all of their compatible systems from a single source, ensuring a consistent time stamp for logging and authentication protocols. NTP is an internet standard, defined in RFC1305.

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 vital to the operation of some network protocols and services such as IPSec and 802.1x which may be critical to many networks.

Using specified time sources allows you to better secure, monitor and manage your NTP implementation, simplifying debugging and allowing tighter control of NTP traffic.

Having multiple NTP servers ensures 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.

1.2.4.1 Require External Time Source(s) (Level 1, Scorable)

Description:
Verify configuration of at least two external (NTP) timeservers used to synchronize the device clock.

Rationale:

To ensure that the time on your Cisco router is consistent with other devices in your network, at least two (and preferably at least three) NTP Server/s external to the router should be configured.

Platform: IOS

Dependencies:
IOS: None

Remediation:

Configure at least one external NTP Server using the following commands

IOS:

```
hostname(config)#ntp server <ntp_server>
```

Audit:

From the command prompt, execute the following commands:

IOS:

```
hostname#sh ntp associations
```

You should see one or more NTP servers if configured correctly.

Default Value:

By default Cisco routers do not have NTP servers configured.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.4.2 Require Encryption Keys for NTP (Level 2, Scorable)

Description:

Encryption keys should be set for NTP Servers.

Rationale:

Having established the need for NTP, it is essential to ensure that the routers 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 allows for encryption keys to be set to allow systems to verify the identity of NTP servers and to protect communications between them from being altered. This functionality has been further enhanced in NTP 4 with PKI being supported on some platforms (but not Cisco at present).

Cisco IOS only supports use of an MD5 key, which is used to verify NTP packets by comparing the routers results to the hash provided by the server. This process confirms both that the server is authentic and that the NTP data has not been modified in transit.

Please note that NTP data itself is still sent in clear text on the network, however the data is not sensitive, the cryptographic protection is used simply to ensure identity and reliability as described above.

Default Value:
By default Cisco routers do not have NTP server authentication configured.

References:
1. NSA Router Security Configuration Guide
2. Cisco IOS Network Management Command Reference, Release 15.0M
3. Cisco Guide to Harden Cisco IOS Devices

1.2.4.2.1 Enable NTP Authentication (Level 2, Scorable)

Description:

Enable NTP authentication.

Platform: IOS

Dependencies:
IOS: None

Remediation:

IOS:

```
hostname(config)#ntp authenticate
```

Audit:

From the command prompt, execute the following commands:

IOS:

```
hostname#show run | include ntp
```

The above two commands should return any NTP server(s) configured with encryption keys. This value should be the same as the total number of servers configured as tested in

1.2.4.2.2 Define NTP Key Ring and Encryption Key (Level 2, Scorable)

Description:

Keys are configured on a key ring and identified by an ID number. To add a key enter the following command

Platform: IOS

Dependencies:
IOS: 1.2.4.2.1 Enable NTP Authentication

Remediation:

IOS:

```
hostname(config)#ntp authentication-key {ntp_key_id} md5 {ntp_key}
```

Audit:

From the command prompt, execute the following commands:

IOS:

```
hostname#show run | include ntp authentication-key
```

The above command should return any NTP server(s) configured with encryption keys. This value should be the same as the total number of servers configured as tested in

1.2.4.2.3 Define the NTP Trusted Key (Level 2, Scorable)

Description:

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

Platform: IOS

Dependencies:

IOS: 1.2.4.2.2 Define NTP Key Ring and Encryption Key

Remediation:

IOS:

```
hostname(config)#ntp trusted-key {ntp_key_id}
```

Audit:

From the command prompt, execute the following commands:

IOS:

```
hostname#show run | include ntp trusted-key
```

The above command should return any NTP server(s) configured with encryption keys. This value should be the same as the total number of servers configured as tested in

1.2.4.2.4 Bind the NTP Key Ring to each NTP server (Level 2, Scorable)

Description:

Set the keys for all configured NTP servers using the following commands under the [edit system] hierarchy, this sets the key that the router will use to encrypt and decrypt traffic for this server

Platform: IOS

Dependencies:
IOS: 1.2.4.2.3 Define the NTP Trusted Key

Remediation:

IOS:

```
hostname(config)#ntp server {ntp-server_ip_address}{key ntp_key_id}
[source interface_name] [prefer]
```

Audit:

From the command prompt, execute the following commands:

IOS:

```
hostname#show run | include ntp server
```

The above two commands should return any NTP server(s) configured with encryption keys. This value should be the same as the total number of servers configured as tested in

1.3 Data Plane Level 1

Description:

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

1.3.1 Routing Rules

Description:

Unneeded services should be disabled.

1.3.1.1 Forbid Directed Broadcast (Level 1, Scorable)

Description:
Disallow IP directed broadcast on each interface.

Rationale:
Directed broadcasts permit hosts to send broadcasts across local area network (LAN) segments. Device interfaces that allow directed broadcasts can be used for "smurf" denial-of-service (DoS) attacks.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable directed broadcast on each interface.

IOS:

```
hostname(config)#interface <interface>
hostname(config-if)#no ip directed-broadcast
```

Audit:
Perform the following to determine if directed broadcast is enabled:

IOS:

1. Verify directed broadcast shows as disabled for each active interface

```
hostname#sh ip interface <interface> | incl Directed broadcast
```

Default Value:

Disabled

References:

1. NSA Router Security Configuration Guide
2. Cisco Guide to Harden Cisco IOS Devices
3. Cisco AutoSecure

1.3.1.2 Forbid IP source-route (Level 1, Scorable)

Description:
Disable source routing.

Rationale:
Source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. Cisco routers normally accept and process source routes. Unless a network depends on source routing, it should be disabled.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Disable source routing.

IOS:

```
hostname(config)#no ip source-route
```

Audit:
Perform the following to determine if source routing is enabled:

IOS:

1. Verify a command string result returns

```
hostname#sh run | incl ip source-route
```

Default Value:

Enabled

References:

1. NSA Router Security Configuration Guide
2. Cisco Guide to Harden Cisco IOS Devices
3. Cisco AutoSecure

2. Level-2 Benchmark

Description:

The Level-2 Benchmark for Cisco IOS represents an enhanced level of due care for system security. These settings:

- Enhance security beyond the minimum due care level, based on specific network architectures and server function
- Contain some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and

applications running in their particular environments

2.1 Management Plane Level 1

Description:
Services, settings, and data streams related to setting up and examining the static configuration of the router and the authentication and authorization of router administrators. Examples of management plane services include: administrative telnet, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.

2.1.1 Local Authentication, Authorization and Accounting (r) Rules (Level 2, Scorable)

Description:
Rules in the Local authentication, authorization and accounting (AAA) configuration class enforce device access control, provide a mechanism for tracking configuration changes, and enforcing security policy.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control. The services are only accessible once authenticated and accounting tracking services accessed. In addition, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

2.1.1.1 Require AAA Authentication Enable (Level 2, Scorable)

Description:
Verify authentication, authorization, and accounting (AAA) methods for enable mode authentication (with fall-back) is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA authentication method(s) for enable authentication (with fall-back).

IOS:

```
hostname(config)#aaa authentication enable default group [enable ...]
```

Audit:
Perform the following to determine if aaa authentication enable is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa authentication enable
```

Default Value:

AAA login is disabled.

References:
1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.2 Require AAA Authentication Login (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) methods for enable mode authentication (with fall-back) is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA authentication method(s) for login authentication (with fall-back).

IOS:

```
hostname(config)#aaa authentication login {default | aaa_list_name}
{group group_name}
```

Audit:
Perform the following to determine if aaa authentication login is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa authentication login
```

Default Value:

AAA login is disabled.

References:
1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.3 Require AAA Accounting Commands (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) for commands is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA accounting for commands.

IOS:

```
hostname(config)#aaa accounting {commands 15} {default} {start-stop}
{group group-name}
```

Audit:
Perform the following to determine if aaa accounting for commands is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa accounting commands
```

Default Value:

AAA accounting is disabled.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.4 Require AAA Accounting Connection (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) for connections is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA accounting for connections.

IOS:

```
hostname(config)#aaa accounting {connection} {default} {start-stop}
{group group-name}
```

Audit:
Perform the following to determine if aaa accounting for connection is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa accounting connection
```

Default Value:

AAA accounting is disabled.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.5 Require AAA Accounting Exec (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) accounting for exec is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA accounting for exec.

IOS:

```
hostname(config)#aaa accounting {exec} {default} {start-stop} {group
group-name}
```

Audit:
Perform the following to determine if aaa accounting for exec is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa accounting exec
```

Default Value:
AAA accounting is disabled.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.6 Require AAA Accounting Network (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) accounting for network events is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:
Configure AAA accounting for network events.

IOS:

```
hostname(config)#aaa accounting {network} {default} {start-stop} {group
tacacs+} [local-case …]
```

Audit:
Perform the following to determine if aaa accounting for network is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa accounting network
```

Default Value:
AAA accounting is disabled.

References:
1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.1.1.7 Require AAA Accounting System (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) accounting for system events is configured.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service

Remediation:

Configure AAA accounting for system events.

IOS:

```
hostname(config)#aaa accounting {system} {default} {start-stop} {group
tacacs+} [local-case …]
```

Audit:
Perform the following to determine if aaa accounting for system is required:

IOS:

1. Verify a command string result returns

```
hostname#sh run | aaa accounting system
```

Default Value:
AAA accounting is disabled.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.2 Control Plane Level 1

Description:
Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

2.2.1 Loopback Rules

Description:

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.

2.2.1.1 Require Loopback Interface (Level 2, Scorable)

Description:
Configure a loopback interface.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Define and configure one loopback interface.

IOS:

```
hostname(config)#interface loopback <number>
hostname(config-if)#ip address <loopback_ip_address>
<loopback_subnet_mask>
```

Audit:
Perform the following to determine if a loopback interface is defined:

IOS:

1. Verify an IP address returns for the defined loopback interface

```
hostname#sh ip int brief | incl Loopback
```

Default Value:
The loopback interface is enabled without a configured IP address

References:
1. Cisco IOS Interface and Hardware Component Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.2.1.2 Forbid Multiple Loopback Interfaces (Level 2, Scorable)

Description:
Define no more than one loopback interface.

Rationale:
Alternate loopback addresses create a potential for abuse, mis-configuration, and inconsistencies. Additional loopback interfaces must be documented and approved prior to use by local security personnel.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Define no more than one loopback interface.

IOS:

```
hostname(config)#no loopback <instance>
```

Audit:
Perform the following to determine how many loopback interfaces are defined:

IOS:

1. Verify only one loopback interface is defined

```
hostname#sh ip int brief | incl Loopback
```

Default Value:
Only one loopback interface is enabled.

References:

1. Cisco IOS Interface and Hardware Component Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.2.1.3 Require Binding AAA Service to Loopback Interface (Level 2, Scorable)

Description:
Verify authentication, authorization and accounting (AAA) services are bound to the loopback interface.

Platform: IOS

Dependencies:
IOS: 1.1.1.1 Require AAA Service
2.2.1.1 Require Loopback Interface

Rationale:
This is required so that the AAA server (RADIUS or TACACS+) can easily identify routers and authenticate requests by their IP address.

Remediation:
Bind AAA services to the loopback interface.

IOS:

```
Hostname(config)#ip {tacacs|radius} source-interface loopback <0>
```

Audit:
Perform the following to determine if aaa services are bound to a source interface:

IOS:

1. Verify a command string result returns

```
hostname#sh run | incl tacacs source | radius source
```

Default Value:

Not configured

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

2.2.1.4 Require Binding the NTP Service to Loopback Interface (Level 2, Scorable)

Description:
Verify the network time protocol (NTP) service is bound to the loopback interface.

Rationale:
Set the source address to be used when sending NTP traffic. This may be required if the NTP servers you peer with filter based on IP address.

Platform: IOS

Dependencies:
IOS: 1.1.4.1 Require External Time Source(s)
2.2.1.1 Require Loopback Interface

Remediation:
Bind the NTP service to the loopback interface.

IOS:

```
hostname(config)#ntp source loopback <0>
```

Audit:
Perform the following to determine if NTP services are bound to a source interface:

IOS:

1. Verify a command string result returns

```
hostname#sh run | incl ntp source
```

Default Value:
The source address is determined by outgoing interface.

References:

1. Cisco IOS Network Management Command Reference, Release 12.4
2. NSA Router Security Configuration Guide

2.2.1.5 Require Binding TFTP Service to Loopback Interface (Level 2, Scorable)

Description:
Verify the trivial file transfer protocol (TFTP) client is bound to the loopback interface.

Rationale:
This is required so that the TFTP servers can easily identify routers and authenticate requests by their IP address.

Platform: IOS

Dependencies: IOS: 2.2.1.1 Require Loopback Interface

Remediation:
Bind the TFTP client to the loopback interface.

IOS:

```
hostname(config)#ip tftp source-interface loopback <0>
```

Audit:
Perform the following to determine if TFTP services are bound to a source interface:

IOS

1. Verify a command string result returns

```
hostname#sh run | incl tftp source-interface
```

Default Value:
Source address is determined by the closest interface to the destination.

References:

1. Cisco IOS Configuration Fundamentals Command Reference, Release 15.0M
2. NSA Router Security Configuration Guide

2.3 Data Plane Level 1

Description:
Services and settings related to the data passing through the router (as opposed to directed to it). Basically, the data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall function- ality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

2.3.1 Border Router Filtering

Description:
A border-filtering device connects "internal" networks such as desktop networks, DMZ networks, etc., to "external" networks such as the Internet. If this group is chosen, then ingress and egress filter rules will be required.

2.3.1.1 Forbid Private Source Addresses from External Networks (Level 2, Scorable)

Description:
Verify the device is configured to restrict access for traffic from external networks that have source address that should only appear from internal networks.

Rationale:
Configuring access controls can help prevent spoofing attacks. To reduce the effectiveness of IP spoofing, configure access control to deny any traffic from the external network that has a source address that should reside on the internal network. Include local host address or any reserved private addresses (RFC 1918).

Warning:
Verify IP multicast is not required or in use before blocking 224.0.0.0/3 address range.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure ACL for private source address restrictions from external networks.

IOS:

```
hostname(config)#access-list <access-list> deny ip <internal_networks>
any log
hostname(config)#access-list <access-list> deny ip 127.0.0.0
0.255.255.255 any log
hostname(config)#access-list <access-list> deny ip 10.0.0.0
0.255.255.255 any log
hostname(config)#access-list <access-list> deny ip 0.0.0.0
0.255.255.255 any log
hostname(config)#access-list <access-list> deny ip 172.16.0.0
0.15.255.255 any log
hostname(config)#access-list <access-list> deny ip 192.168.0.0
0.0.255.255 any log
hostname(config)#access-list <access-list> deny ip 192.0.2.0 0.0.0.255
any log
hostname(config)#access-list <access-list> deny ip 169.254.0.0
0.0.255.255 any log
hostname(config)#access-list <access-list> deny ip 224.0.0.0
31.255.255.255 any log
hostname(config)#access-list <access-list> deny ip host 255.255.255.255
any log
hostname(config)#interface <external_interface>
hostname(config-if)#access-group <access-list> in
```

Audit:
Perform the following to determine if the ACL is created:

IOS:

1. Verify you the appropriate access-list definitions

```
hostname#sh ip access-list <access-list>
```

Default Value:
No access lists are configured by default.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Security Command Reference, Release 15.0
3. RFC 3704 - Ingress Filtering for Multi-homed Networks

2.3.1.1.1 Apply Inbound Border ACL on External Interface (Level 2, Scorable)

Description:
Verify outbound traffic from your network includes only valid internal source addresses.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure ACL to only disallow non-routable unnecessary networks to ingress.

IOS:

```
hostname(config)#interface <external_interface>
hostname(config-if)#access-group <access-list> in
```

Audit:
Perform the following to determine if the outbound ACL is created:

IOS:

1. Verify you the appropriate access-list definitions

```
hostname#sh ip access-list <access-list>
```

Default Value:
No access lists are configured by default.

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS Security Command Reference, Release 15.0
3. RFC 3704 - Ingress Filtering for Multi-homed Networks
4. RFC 3300 - Special-Use IPv4 Addresses
5. RFC 3171 - IANA Guidelines for IPv4 Multicast Address Assignments
6. RFC 1918 - Address Allocation for Private Internets

2.3.1.2 Forbid External Source Addresses on Outbound Traffic (Level 2, Scorable)

Description:
Verify outbound traffic from your network includes only valid internal source addresses.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure ACL to only allow internal networks to egress.

IOS:

```
hostname(config)#interface <external_interface>
hostname(config-if)#access-group <access-list> out
```

Audit:
Perform the following to determine if the outbound ACL is created:

IOS:

1. Verify you the appropriate access-list definitions

```
hostname#sh ip access-list <access-list>
```

Default Value:
No access lists are configured by default.

References:
1. NSA Router Security Configuration Guide
2. **Cisco IOS Security Command Reference, Release 15.0**

2.3.1.2.1 Apply Outbound Border ACL on External Interface (Level 2, Scorable)

Description:
Apply inbound and outbound ACLs on your external interface.

Rationale:
You can prevent users from spoofing other networks by ensuring that any outbound traffic from your network uses only source IP addresses that are in your organization's IP addresses range. This filtering denies any traffic that does not have the source address that was expected on a particular interface.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure inbound and outbound ACL.

IOS:

```
hostname(config)#interface <external_interface>
hostname(config-if)#access-group <access-list> out
```

Audit:
Perform the following to determine if the ACL is created:

IOS:

1. Verify you the appropriate access-list definitions

```
hostname#sh ip access-list <access-list>
```

Default Value:
No access lists are configured by default.

References:
1. NSA Router Security Configuration Guide
2. Cisco IOS Security Command Reference, Release 15.0

2.3.2 Neighbor Authentication

Description:

Enable routing authentication.

Rationale:
Verifying routing update packets using neighbor authentication reduces the possibility of the device receiving false route updates that could potentially allow an attacker to corrupt route tables, compromise network availability, or redirect network traffic.

Warning:
If you configure the device for neighbor authentication, the neighbor device must be configured for neighbor authentication with compatible settings otherwise route update packets from the neighbor device will be rejected.

2.3.2.1 Establish the Key Chain (Level 2, Scorable)

Description:
Establish the key chain. This should be different for each routing protocol.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Establish the EIGRP key chain.

IOS:

```
hostname(config)#key chain <rip_key-chain_name>
```

Audit:
Perform the following to determine if the EIGRP key chain is setup:

IOS:

1. Verify the appropriate key chain is defined

```
hostname#sh run | sec key chain
```

2. Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.2.1.1 Configure the Key Number (Level 2, Scorable)

Description:
Configure the key number.

Platform: IOS

Dependencies:
IOS: 2.3.2.1 Establish the Key Chain

Remediation:
Configure the EIGRP key number.

IOS:

```
hostname(config-keychain)#key <key-number>
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

IOS:

1. Verify the appropriate key chain is defined

```
hostname#sh run | sec key chain
```

2. Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.2.1.2 Configure the Key String (Level 2, Scorable)

Description:
Configure the key string.

Platform: IOS

Dependencies:
IOS: 2.3.2.1 Establish the Key Chain

Remediation:
Configure the key string.

IOS:

```
hostname(config-keychain-key)#key-string <key-string>
```

Audit:
Perform the following to determine if the key string is enabled:

IOS:

1. Verify the appropriate key chain is defined

```
hostname#sh run | sec key chain
```

2. Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.2.2 Require BGP Authentication if Protocol is Used (Level 2, Scorable)

Description:

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.

Verify border gateway protocol (BGP) authentication is enabled, where feasible.

Note:
BGP routing support is not available in IP base.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure BGP neighbor authentication where feasible.

IOS:

```
hostname(config)#router bgp <bgp_as-number>
hostname(config-router)#neighbor <bgp_neighbor-ip | peer-group-name>
password <password>
```

Audit:
Perform the following to determine if BGP neighbor authentication is required:

IOS:

1. Verify you see the appropriate neighbor password is defined:

```
hostname#sh run | sec router bgp
```

Default Value:
BGP authentication is disabled by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. Cisco IOS IP Routing: BGP Configuration Guide, Release 15.0
3. Cisco IOS Security Configuration Guide: Securing the Control Plane, Release 15.0
4. NSA Router Security Configuration Guide

2.3.2.3 Require EIGRP Authentication if Protocol is Used (Level 2, Scorable)

Description:
Verify enhanced interior gateway routing protocol (EIGRP) authentication is enabled, if routing protocol is used, where feasible.

Default Value:
EIGRP authentication is disabled by default.

References:

1. Cisco IOS Security Command Reference, Release 15.0
2. Cisco IOS IP Routing: EIGRP Configuration Guide, Release 15.0
3. Cisco IOS Security Configuration Guide: Securing the Control Plane, Release 15.0
4. NSA Router Security Configuration Guide

Default Value:
EIGRP authentication is disabled by default.

2.3.2.3.1 Establish the EIGRP Address Family (Level 2, Scorable)

Description:
Configure the EIGRP address family.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the EIGRP address family.

IOS:

```
hostname(config)#router eigrp <virtual-instance-name>
hostname(config-router)#address-family ipv4 autonomous-system
{eigrp_as-number}
hostname(config-router-af)#af-interface default
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

IOS:

1. Verify the appropriate address family is set

```
hostname#sh run | sec router eigrp
```

2.3.2.3.2 Establish the EIGRP Address Family Key Chain (Level 2, Scorable)

Description:
Configure the EIGRP address family key chain.

Platform: IOS

Dependencies:
IOS: 2.3.2.2.4 Establish the EIGRP Address Family
2.3.1.2 Establish the Key Chain

Remediation:
Configure the EIGRP address family key chain.

IOS:

```
hostname(config-router-af-interface)#authentication key-chain
{eigrp_key-chain_name}
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

IOS:

1. Verify the appropriate address family is set

```
hostname#sh run | sec router eigrp
```

2.3.2.3.3 Establish the EIGRP Address Family Authentication Mode (Level 2, Scorable)

Description:
Configure the EIGRP address family authentication mode.

Platform: IOS

Dependencies:
IOS: 2.3.2.2.4 Establish the EIGRP Address Family
2.3.1.2 Establish the Key Chain

Remediation:
Configure the EIGRP address family authentication mode.

IOS:

```
hostname(config-router-af-interface)#authentication mode md5
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

IOS:

1. Verify the appropriate address family authentication mode is set

```
hostname#sh run | sec router eigrp
```

2.3.2.3.4 Configure the Interface with the EIGRP Key Chain (Level 2, Scorable)

Description:
Configure the interface with the EIGRP key chain.

Platform: IOS

Dependencies:
IOS: 2.3.1.2 Establish the Key Chain

Remediation:
Configure the interface with the EIGRP key chain.

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#ip authentication key-chain eigrp <eigrp_as-number>
<eigrp_key-chain_name>
```

Audit:
Perform the following to determine if the EIGRP key chain is enabled for the interface:

IOS:

1. Verify the appropriate key chain is set on the appropriate interface(s)

```
hostname#sh run int <interface> | incl key-chain
```

Default Value:

2.3.2.3.5 Configure the Interface with the EIGRP Authentication Mode (Level 2, Scorable)

Description:
Configure the interface with the EIGRP authentication mode.

Platform: IOS

Dependencies:
IOS: 2.3.2.2.6 Establish the EIGRP Address Family Authentication Mode

Remediation:
Configure the interface with the EIGRP authentication mode.

IOS:

```
hostname(config-if)#ip authentication mode eigrp <eigrp_as-number> md5
```

Audit:
Perform the following to determine if the EIGRP authentication is enabled:

IOS:

1. Verify the appropriate authentication mode is set on the appropriate interface(s)

```
hostname#sh run int <interface> | incl authentication mode
```

2.3.2.4 Require OSPF Authentication if Protocol is Used (Level 2, Scorable)

Description:
Verify open shortest path first (OSPF) authentication is enabled, where feasible.

Rationale:

Where it is deployed, OSPF routing is vital for normal operation of an organizations 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 Cisco routers (as well as routers from other manufacturers such as Juniper 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 an area by area basis.

Note:

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

Default Value:
OSPF authentication is disabled by default.

References:
1. Cisco IOS IP Routing: OSPF Configuration Guide, Release 15.0
2. Cisco IOS Security Configuration Guide: Securing the Control Plane, Release 15.0
3. NSA Router Security Configuration Guide

2.3.2.4.1 Require the Message Digest for OSPF (Level 2, Scorable)

Description:
Configure the message Digest option for OSPF

Platform: IOS

Dependencies:
IOS: None

Remediation:
Configure the message Digest option for OSPF

IOS:

```
hostname(config)#router ospf <ospf_process-id>
hostname(config-router)#area <ospf_area-id> authentication message-
digest
```

Audit:
Perform the following to determine if the OSPF authentication is enabled:

IOS:

1. Verify message digest for OSPF is defined

```
hostname#sh run | sec router ospf
```

2.3.2.4.2 Configure the Interface for Message Digest Authentication (Level 2, Scorable)

Description:
Configure the appropriate interface(s) for Message Digest authentication

Platform: IOS

Dependencies:
IOS: 2.3.2.4.1 Require Message Digest for OSPF

Remediation:
Configure the appropriate interface(s) for Message Digest authentication

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#ip ospf message-digest-key <ospf_md5_key-id> md5
<ospf_md5_key>
```

Audit:
Perform the following to determine if the OSPF authentication is enabled:

IOS:

1. Verify the appropriate md5 key is defined on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.2.5 Require RIPv2 Authentication if Protocol is Used (Level 2, Scorable)

Description:

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.

Verify routing information protocol (RIP) version two authentication is enabled, if routing protocol is used, where feasible.

Default Value:
RIPv2 authentication is disabled by default.

References:

1. Cisco IOS IP Routing: RIP Configuration Guide, Release 15.0
2. Cisco IOS Security Configuration Guide: Securing the Control Plane, Release 15.0
3. NSA Router Security Configuration Guide

2.3.2.5.1 Configure the Interface with the RIPv2 Key Chain (Level 2, Scorable)

Description:

Configure the Interface with the RIPv2 key chain.

Platform: IOS

Dependencies:
IOS: 2.3.1.2 Establish the Key Chain

Remediation:

Configure the Interface with the RIPv2 key chain.

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#ip rip authentication key-chain <rip_key-
chain_name>
```

Audit:
Perform the following to determine if the RIPv2 authentication is enabled:

IOS:

1. Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.2.5.2 Configure the Interface with the RIPv2 Authentication Mode (Level 2, Scorable)

Description:
Configure the Interface with the RIPv2 key chain.

Platform: IOS

Dependencies:
IOS: 2.3.1.2 Establish the Key Chain

Remediation:
Configure RIPv2 neighbor authentication where feasible.

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#ip rip authentication mode md5
```

Audit:
Perform the following to determine if the RIPv2 authentication mode is enabled:

1. Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
hostname#sh run int <interface>
```

2.3.3 Routing Rules

Description:
Unneeded services should be disabled.

2.3.3.1 Require Unicast Reverse-Path Forwarding (uRPF) (Level 2, Scorable)

Description:
Verify unicast reverse-path forwarding (uRPF) is enabled on all external or high risk interfaces.

Rationale:
Verifying the source address of IP traffic against routing rules reduces the possibility that an attacker can spoof the source of an attack. A number of attacks methods rely on falsifying the traffic source to create a denial-of-service (DoS) or make it harder to trace the source of an attack. When enabled, the device checks the source address of the packet against the interface through which the packet arrived. Packets are dropped if the device determines, by verifying routing tables, there is no feasible path through the interface for the source address. Enabling reverse-path verification in environments with asymmetric routes can adversely affect network traffic.

2.3.3.1.1 Enable Cisco Express Forwarding (CEF) (Level 2, Scorable)

Description:
Enable Cisco Express Forwarding

Rationale:
This is a requirement to enable uRPF.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Configure CEF.

IOS:

```
hostname(config)#ip cef
```

Audit:
Perform the following to determine if uRPF is enabled:

IOS:

1. Verify CEF is enabled

```
hostname#sh ip cef
```

Default Value:

CEF is enabled.

References:
1. Cisco IOS IP Switching Configuration Guide, Release 15.0

2.3.3.1.2 Enable Unicast Reverse-Path Forwarding (uRPF) (Level 2, Scorable)

Description:
Configure unicast reverse-path forwarding (uRPF) on all external or high risk interfaces.

Platform: IOS

Dependencies:
IOS: 2.3.3.1.1 Enable Cisco Express Forwarding (CEF)

Remediation:
Configure uRPF.

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#ip verify unicast source reachable-via rx
```

Audit:
Perform the following to determine if uRPF is enabled:

IOS:

1. Verify uRPF is running on the appropriate interface(s)

```
hostname#sh ip int <interface> | incl verify source
```

Default Value:

uRPF is disabled.

References:

1. NSA Router Security Configuration Guide
2. RFC 2267 - Network Ingress Filtering
3. Cisco IOS Security Configuration Guide: Securing the Control Plane, Release 15.0
4. Cisco IOS Security Command Reference, Release 15.0
5. Cisco IOS IP Switching Configuration Guide, Release 15.0
6. Cisco AutoSecure

2.3.3.2 Forbid IP Proxy ARP (Level 2, Scorable)

Description:
Verify proxy ARP is disabled on all interfaces.

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 Cisco 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.

Remediation:
Disable proxy ARP on all interfaces.

IOS:

```
hostname(config)#interface <interface_name>
hostname(config-if)#no ip proxy-arp
```

Audit:
Perform the following to determine if proxy ARP is enabled:

IOS:

1. Verify the proxy ARP status

```
hostname#sh ip int <interface> | incl proxy-arp
```

Default Value:

Enabled

References:

1. NSA Router Security Configuration Guide
2. Cisco IOS IP Addressing Services Command Reference
3. Cisco AutoSecure

2.3.3.3 Forbid Tunnel Interfaces (Level 2, Scorable)

Description:
Verify no tunnel interfaces are defined.

Rationale:
Tunnel interfaces should not exist in general. They can be used for malicious purposes. If they do exist, the network admins should be well aware of them and their purpose.

Remediation:
Do not define any tunnel interfaces.

IOS:

```
hostname(config)#no interface tunnel <instance>
```

Audit:
Perform the following to determine if a tunnel interface is defined:

IOS:

1. Verify no tunnel interfaces are defined

```
hostname#sh ip int brief | incl Tunnel
```

Default Value:
No tunnel interfaces are enabled.

References:

1. Cisco IOS Interface and Hardware Component Command Reference, Release 15.0
2. NSA Router Security Configuration Guide

Appendix A: References

1. Cisco Systems, Inc. (2010). Cisco IOS Security Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. Last accessed June 28, 2011.
2. Cisco Systems, Inc. (2010). Cisco IOS Terminal Services Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/termserv/command/reference/tsv_book.html. Last accessed June 28, 2011.
3. Cisco Systems, Inc. (2010). Cisco IOS Configuration Fundamentals Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/cf-cr-book.html. Last accessed June 28, 2011.
4. Cisco Systems, Inc. (2010). Cisco IOS Network Management Command Reference, Release 15.0 http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html. Last accessed June 28, 2011.
5. Cisco Systems, Inc. (2010). Cisco IOS Interface and Hardware Component Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_book.html. Last accessed June 28, 2011.
6. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: BGP Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html. Last accessed June 28, 2011.
7. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: EIGRP Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-cr-book.html. Last accessed June 28, 2011.
8. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: OSPF Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_ospf/command/reference/iro_book.html. Last accessed June 28, 2011.
9. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: RIP Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_rip/command/reference/irr_book.html. Last accessed June 28, 2011.
10. Cisco Systems, Inc. (2010). Cisco IOS IP Routing: Protocol Independent Command Reference, Release 15.0. http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_book.html. Last accessed June 28, 2011.
11. Cisco Systems, Inc. (2010). Cisco IOS Switching Command Reference, Release 12.4. http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html. Last accessed June 28, 2011.
12. Cisco Systems, Inc. (2005). Cisco AutoSecure White Paper. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper09186a00801dbf61.pdf. Last accessed June 28, 2011.

13. Cisco Systems, Inc. (2011). Cisco Guide to Harden Cisco IOS Devices. http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml. Last accessed June 28, 2011.
14. National Security Agency (2009). NSA Router Security Configuration Guide. http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf. Last accessed June 28, 2011.
15. United States Department of Justice (2009). US Department of Justice – Cybercrime – Appendix A - Sample Network Login Banner. http://www.cybercrime.gov/ssmanual/06ssma.html#AppA. Last accessed June 28, 2011.
16. Center for Information Security (2010). Cisco IOS Benchmark v2.4. http://benchmarks.cisecurity.org/tools2/cisco/CIS_Cisco_IOS_Benchmark_v2.4.0.pdf. Last accessed June 28, 2011.

Appendix B: Change History

Date	Version	Changes for this version
June 20, 2011	2.9.1	Created atomic recommendations for Sections 1 – 2.3.1.2.1
June 20, 2011	2.9.1	Added SNMP Trap sections for IOS
June 20, 2011	2.9.1	Added IOS to local time zone sections
June 20, 2011	2.9.1	Modified external interface ACL section to include atomic checks for application to interface
June 24, 2011	2.9.2	Created atomic recommendations for remainder of the document
June 24, 2011	2.9.2	Correct issue with Loopback syntax
June 24, 2011	2.9.2	Migrated SSH prerequisites into the main document and removed duplicate section from section 1
June 27, 2011	2.9.3	Updated PCI references
June 27, 2011	2.9.3	Re-ordered VTY ACL section before SSH for VTY
June 27, 2011	2.9.3	Added SNMPv3 sections
June 27, 2011	2.9.3	Corrected section numbering issues
June 27, 2011	2.9.4	Corrected formatting issues
June 27, 2011	2.9.4	Updated reference section
July 8, 2011	2.9.5	Updated SNMPv3 AES encryption information
July 8, 2011	2.9.5	Update SSH timeout wording