CIS Benchmarks

CIS Cisco Firewall v8.x Benchmark

v4.2.0 - 04-01-2021

Terms of Use

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

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

Table of Contents

Overview

This is an END OF LIFE document tickets and discussions have been addressed. This document, Security Configuration Benchmark for Cisco Firewall Appliances, provides prescriptive guidance for establishing a secure configuration posture for Cisco Firewall Appliances versions 8.x. This guide was tested against Cisco ASA 8.0(5). To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This 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 a Cisco Firewall Appliance.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Assessment Status

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

Automated

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

Manual

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Cisco ASA 8.x**

  Items in this profile intend to:

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

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:

Contributor
Adam Montville
Jordan Rakoske GSEC, GCWN
Bill Munyan GSEC, GCWN, Center for Internet Security
Mike Wicks GCIH, GSEC, GSLC, GCFE, GISP
Piyush Sharma
Darren Freidel

Editor
Brigitte Afoumbom CISM, CISSP, CCNA SECURITY, CCNP, ITIL, MBA (PM)

Recommendations

1 Management Plane

The management plane deals with services, settings and data streams related to the configuration of the security appliance. Examples of management plane services include: administrative device access (telnet, ssh, http, and https), SNMP, and security protocols like RADIUS and TACACS+, the authentication and authorization of firewall administrators.

1.1 Password Management

Sets the rules for password enforcement

1.1.1 Ensure 'Logon Password' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Changes the default login password.

Rationale:

The login password is used for Telnet and SSH connections. The default device configuration does not require any strong user authentication enabling unfettered access to an attacker that can reach the device. A user can enter the default password and just press the Enter key at the Password prompt to login to the device. Setting the login password causes the device to enforce use of a strong password to access user mode. Using default or well-known passwords makes it easier for an attacker to gain entry to a device.

Audit:

- Step 1: Run the following to determine whether the login password is set

```
hostname# show running-config passwd
```

The output should look like

```
passwd xxxxxx encrypted
```

Example:

```
Asa#show running-config passwd
passwd 8Ry2YjIyt7RRXU24 encrypted
```

Here 8Ry2YjIyt7RRXU24 is the encrypted format of the plain-text password used as login password

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to set the login password.

```
hostname(config)#passwd <login_password>
```

The login_password parameter should be the plain-text password used to log into the system

Default Value:

The default password is "cisco".

8.4(2)

The SSH default username is no longer supported; you can no longer connect to the ASA using SSH with the pix or asa username and the login password.

9.0(2), 9.1(2)

The default password, “cisco,” has been removed; you must actively set a login password. Using the no passwd or clear configure passwd command removes the password; formerly, it reset it to the default of “cisco.”

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/p1.html#wp2130703

CIS Controls:

Version 7

4.2 Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

1.1.2 Ensure 'Enable Password' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the password for users accessing privileged EXEC mode when they run the enable command.

Rationale:

The default device configuration does not require any strong user authentication enabling unfettered access to an attacker that can reach the device. A user can enter the default password and just press the Enter key at the Password prompt to login to the device. Setting the enable password causes the device to enforce use of a strong password to access privileged EXEC mode. Using default or well-known passwords makes it easier for an attacker to gain entry to a device.

Audit:

- Step 1: Run the following to determine whether the login password is set

```
hostname#show run | inc enable
```

The output should look like

```
enable password xxxxxxx encrypted
```

Example:

```
Asa#show run enable
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Here 8Ry2YjIyt7RRXU24 is the encrypted format of the plain-text password used as enable password

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to set the enable password.

```
hostname(config)#enable password <enable_password> level <privilege_level>
```

The enable_password parameter should be the plain-text password used to log into the enable mode
If the privilege level is not configured, the default one is 15

Default Value:

By default, the enable password is blank.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/basic.html

CIS Controls:

Version 7

18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms
Use only standardized and extensively reviewed encryption algorithms.

1.1.3 Ensure 'Master Key Passphrase' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Defines the master key passphrase used for to encrypt the application secret-keys contained in the configuration file for software releases from 8.3(1) and above.

Rationale:

For ASA software releases from 8.3 and below, the VPN preshared keys, Tacacs+/Radius shared keys or Routing protocols authentication passwords are encrypted in the running-configuration once generated. They can be viewed in plain-text when the file is transferred through TFTP or FTP to be stored out of the device. Therefore, if the stored file falls into the hands on an attacker, he/she will have all the passwords and application encryption keys.

From version 8.3(1) and above, the master key passphrase helps to generate the AES encryption key used to encrypt secret-keys both in the running configuration and when the file is exported through TFTP or FTP to be stored in a different location.

It improves the security because the master key is never displayed in the running-configuration.

Audit:

- Step 1: Run the following to find whether the software version of the security appliance is from 8.3(1) and above

```
hostname# sh version | i Software_Version_8.[3-9] hostname# sh version | i
Software_Version_9.[0-9]
```

Example:

```
asa-dmz# sh version | i Software_Version_8.[3-9]
Cisco Adaptive Security Appliance Software Version 8.4(2)
asa-dmz# sh version | i Software_Version_9.[0-9]
```

In this example, the software version is 8.4(2

```
Datacenter-fw-01# sh version | i Software_Version_8.[3-9]
Datacenter-fw-01# sh version | i Software_Version_9.[0-9]
Cisco Adaptive Security Appliance Software Version 9.5(2) <system>
```

In this example, the software version is 9.5(2)

- Step 2: If an output is displayed, go to the step 3. If not, the release is not from 8.3(1) and above and the recommendation is not applicable.
- Step 3: Run the following to find whether the existing keys are type 6 encrypted

```
hostname# sh run | in key.6
```

Example:

```
cis-asa-1/admin# sh run | in key.6
key 6 "JDYkW0hEIquGiXMdznN2
```

Here the Tacacs+ key is encrypted using AES encryption and master key. If it was not the case, the key would be displayed with stars only as follows: **key ********

- Step 4: If an output is displayed, the system is compliant, if not it is a finding.

Remediation:

- Step 1: Set the master key passphrase with the following command:

```
hostname (config)# key config-key password-encryption <passphrase>
```

The passphrase is between 8 and 128 characters long

- Step 2: Enable the AES encryption of existing keys of the running-configuration

```
hostname(config)# password encryption aes
```

- Step 3: Run the following for the encryption of keys in the startup-configuration

```
hostname(config)# write memory
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/basic.html

CIS Controls:

Version 7

18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms
Use only standardized and extensively reviewed encryption algorithms.

1.1.4 Ensure 'Password Recovery' is disabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the password recovery

Rationale:

Disabling the password recovery is an additional physical control. It will prevent an attacker that will have circumvented all the physical safeguards and being in contact with the security appliance to change the existing login password, enable password and local user password and then hack the system.

Audit:

- Step 1: Run the following to determine if the password recovery has been disabled

```
hostname#sh run | in no.service.password-recovery
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to disable the password recovery:

```
hostname (config)# no service password-recovery
```

Default Value:

The password recovery is enabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/admin_trouble.html#wp1243707

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.5 Ensure 'Password Policy' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enforces the Enterprise Password Policy by setting compliant local password requirements for the security appliance

Rationale:

The password policy helps to prevent unauthorized accesses by enforcing the password for more complexity and making them difficult to be guessed. This applies to the local database.

Audit:

- Step 1: Run the following to determine whether the password-policy is set

```
hostname#show run password-policy
```

Example:

```
Asa#sh run password-policy
password-policy minimum-length 8
password-policy minimum-numeric 1
```

Here the password-policy is configured for the passwords to have at least 8 characters and to contain at least a number

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Run the following to set the password lifetime in days to less than or equal to 180

```
hostname(config)#password-policy lifetime 30
```

- Step 2: Run the following to set the minimum number of characters that must be changed between the old and the new passwords, to be to be greater than or equal to 14

```
hostname(config)#password-policy minimum-changes 14
```

- Step 3: Run the following to set the minimum number of upper case characters in the password, to be to be greater than or equal to 1

```
hostname(config)#password-policy minimum-uppercase 1
```

- Step 4: Run the following to set the minimum number of lower case characters in the password, to be to be greater than or equal to 1

```
hostname(config)#password-policy minimum-lowercase 1
```

- Step 5: Run the following to set the minimum number of numeric characters in the password, to be greater than or equal to 1

```
hostname(config)#password-policy minimum-numeric 1
```

- Step 6: Run the following to set the minimum number of special characters in the password, to be greater than or equal to 1

```
hostname(config)#password-policy minimum-special 1
```

- Step 7: Run the following to set the password minimum length, to be greater than or equal to 14

```
hostname(config)#password-policy minimum-length 14
```

Default Value:

Password policy is disabled by default.

The following are default values:

password-policy lifetime 0 password-policy minimum-changes 0 password-policy minimum-length 3 password-policy minimum-uppercase 0 password-policy minimum-lowercase 0 password-policy minimum-numeric 0 password-policy minimum-special 0

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.2 Device Management

Sets the security appliance device name

1.2.1 Ensure 'Domain Name' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the domain name for the security appliance

Rationale:

The domain name is important during the deployment of RSA keys and certificates used by the appliance.

Audit:

- Step 1: Acquire the enterprise domain name <enterprise_domain>
- Step 2: Run the following to check whether it is configured

```
hostname#sh run | inc domain-name
```

The output should be the domain.
Example:

```
asa_internet#sh run domain-name | in example.com
example.com
```

- Step 3: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the enterprise domain name (enterprise_domain)
- Step 2: Run the following to configure the domain name

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

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_hostname_pw.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2 Ensure 'Host Name' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Changes the device default hostname

Rationale:

The device hostname plays an important role in asset inventory and identification as a security requirement, but also in the public keys and certificate deployments as well as when correlating logs from different systems during an incident handling.

Audit:

- Step 1: Run the following to check whether the default name is changed

```
hostname# sh run hostname | e _ciscoasa_|_asa
```

The output should look like:

```
hostnamem name_of_device
```

where the name_of_device is not the default one.
Example:

```
Datacenter-asa-1# sh run hostname | e _ciscoasa_|_asa_
hostname Datacenter-asa-1
```

Here the hostname is Datacenter-asa-1

- Step 2: If an output is displayed, the system is compliant. If not it is a finding.

Remediation:

- Step 1: Acquire the enterprise naming convention to build the name_of_device
- Step 2: Run the following to configure the device hostname

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

Default Value:

The default value depends on the platform, but generally is ciscoasa

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_hostname_pw.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.2.3 Ensure 'Failover' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables failover between the security appliance and another security appliance in order to achieve high availability

Rationale:

Enabling failover helps to meet the availability requirement of the security CIA (Confidentiality - Integrity - Availability) triad, ensuring a physical and logical redundancy of firewalls in order to avoid service disruption should the security appliance or its component fails. It requires to identical systems in hardware and software version connected through a failover and a state links.

Audit:

- Step 1: Run the following to check if failover is enabled

```
hostname#sh run failover | grep -v no
```

Example:

```
Asa-fw# sh run failover | grep -v no
failover
failover lan unit secondary
failover lan interface fointerface GigabitEthernet0/0
failover link fointerface GigabitEthernet0/0
failover interface ip fointerface 10.0.0.1 255.0.0.0 standby 10.0.0.2
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Follow the steps below to enable active/standby failover. The commands are run in the system execution space

- Step 1: For each appliance, identify the failover link physical interface <failover_interface_physical> and assign it a name <failover_interface_name> and IP address <failover_interface_ip> and subnet mask <failover_interface_mask>. Identify the other device IP address for each appliance as <peer_failover_ip>

- Step 2: For each appliance, identify the state link physical interface <state_interface_physical> and assign it a name <state_interface_name> and IP address <state_interface_ip> and subnet mask <state_interface_mask>. Identify the other device IP address for each appliance as <peer_state_ip>
- Step 3: Run the following on the Active device to set it as primary node

```
hostname(config)#failover lan unit primary
```

- Step 4: Run the following on the Standby device to set it as secondary node

```
hostname(config)#failover lan unit secondary
```

- Step 5: Run the following on both security appliances

```
hostname(config)#failover lan interface <failover_interface_name>
<failover_interface_physical>
hostname(config)#failover interface ip <failover_interface_name>
<failover_interface_ip> <failover_interface_mask> standby <peer_failover_ip>
hostname(config)#interface <failover_interface_physical>
hostname(config-if)#no shutdown
hostname(config)#failover link <state_interface_name>
<state_interface_physical>
hostname(config)#failover interface ip <state_interface_name>
<state_interface_ip> <state_interface_mask> standby  <peer_state_ip>
hostname(config)#interface <state_interface_physical>
hostname(config-if)#no shutdown
hostname(config)#failover
hostname(config)#write memory
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/ha_failover.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.2.4 Ensure 'Unused Interfaces' is disable (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the unused interfaces

Rationale:

Shutting down the unused interfaces is a complement to physical security. In fact, an attacker connecting physically to an unused port of the security appliance can use the interface to gain access to the device if the relevant interface has not been disabled and the source restriction to management access is not enabled.

Audit:

- Step 1: Run the following command to check if there are unsused ports that have not been disabled.

```
hostname#sh int ip brief | in __down
```

Example:
This first command lists all the interfaces

```
Corp-FW# show int ip brief
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/1         unassigned      YES unset  up
up
GigabitEthernet0/1.201     172.16.61.1     YES CONFIG up
up
GigabitEthernet0/1.202     172.16.62.171   YES CONFIG up
up
GigabitEthernet1/0         unassigned      YES unset  administratively down
down
GigabitEthernet1/1         unassigned      YES unset  administratively down
down
GigabitEthernet1/2         unassigned      YES unset  down
down
GigabitEthernet1/3         192.168.1.11    YES manual up
up
```

This second command is the audit command which looks for unused interfaces that are not disabled

```
Corp-FW#sh int ip brief | in __down
GigabitEthernet1/2         unassigned      YES unset  down
down
```

Here, the interface GigabitEthernet1/2 is unused but not shutdown since the status is 'down' instead of being 'administratively down'

- Step 2: If there is no output displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Identify the physical name <interface_physical_name> of the unused interfaces that are not disabled
- Step 2: For each of the identified interfaces, run the following command

```
Hostname(config)#interface <interface_physical_name>
Hostname(config-if)#shutdown
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/int5505.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.3 Image security

Verifies the integrity and authenticity of the image

1.3.1 Ensure 'Image Integrity' is correct (Manual)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Verifies integrity of an uploaded software before upgrading the system

Rationale:

Sometimes, manipulating software from downloading them from the Cisco.com website to uploading them in the security appliance can modify the software, mostly when the copy has not been properly performed or the software has transited into malware infected machines. For an upgrade to be performed without downtime, the image integrity should be verified.

Audit:

- Step 1: Acquire the location in the security appliance of the new image <new_image_location> and the MD5 checksum <md5_checksum> from the Cisco.com Website
- Step 2: Run the following command to verify that the MD5 checksum value of the new image matches the one provided on the Cisco.com Website

```
hostname#verify <new_image_location> <md5_checksum>
```

Example:

```
Asa-fw# verify disk0:asa803-6-k8.bin 76b5448039e642099334abbfec5a8705
Verifying file integrity of disk0:/asa803-6-k8.bin!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<lines omitted> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Verified (disk0:/asa803-6-k8.bin) = 76b5448039e642099334abbfec5a8705
```

The new image location is disk0:asa803-6-k8.bin

- Step 3: If the message '**Verified**' appears at the end of the output, the new image is valid. If instead the message '**%Error verifying**' is displayed, the image is not valid. It is a finding.

Remediation:

Download a new image from the Cisco.com website and apply the audit procedure until obtaining the message '**Verified**' at the end of the output.

CIS Controls:

Version 7

11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices

Install the latest stable version of any security-related updates on all network devices.

1.3.2 Ensure 'Image Authenticity' is correct (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Verifies for digitally signed images that the running image is from a trusted source

Rationale:

The software image being a code can be vulnerable to many attacks such as malicious code injection in the software, the modification of the code installed in the ROM. In order to ensure that the image running is from a trusted source, the image is digitally signed and its certificate should be verified.

Audit:

- Step 1: Run the following command to verify the authenticity of the image currently running on the security appliance

```
hostname#show software authenticity running | in CiscoSystems$
```

Example:

```
Asa-fw# show software authenticity running
Image type                   : Release
    Signer Information
        Common Name          : abraxas
        Organization Unit    : ASAv
        Organization Name    : CiscoSystems
    Certificate Serial Number : 565963AF
    Hash Algorithm           : SHA2 512
    Signature Algorithm      : 2048-bit RSA
    Key Version              : A
Asa-fw# show software authenticity running | in CiscoSystems$
        Organization Name    : CiscoSystems
```

- Step 2: If an output is displayed, the image is sourced from Cisco. The system is compliant. If there is no output displayed, the image is not from a trusted source. It is a finding.

Remediation:

- Step 1: Correct the errors on the hardware and software
- Step 2: Run the audit procedure until the system is compliant

- Step 3: Implement secure delivery of hardware and harden the software distribution server

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s12.html

CIS Controls:

Version 7

11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices

Install the latest stable version of any security-related updates on all network devices.

1.4 Authentication, Authorization and Accounting (AAA)

The AAA (authentication, authorization, and accounting) scheme implements the security requirements relevant to access control, mainly in providing the mechanisms to authenticate the users, controlling their privileges and tracking their actions on the system. AAA provides a primary method for authenticating users (a username/password database stored on a TACACS+ or RADIUS server or group of servers) and then specifies a backup method (a locally stored username/password database). The backup method is used if the primary method's database cannot be accessed by the networking device.

1.4.1 Local AAA rules

Sets the AAA (Authentication, Authorization, Accounting) requirements for the local database of users

1.4.1.1 Ensure 'aaa local authentication max failed attempts' is set to less than or equal to '3' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Limits the maximum number of times a local user can enter a wrong password before being locked out

Rationale:

Limiting the number of failed authentication attempts is a prevention and safeguard against brute force and dictionary attacks on systems. The implementation of the aaa local authentication max failed attempts helps to limit the number of consecutive failed login attempts when the AAA authentication scheme through the local database is used as method.

Audit:

- Step 1: Acquire the enterprise standard maximum value (enterprise_max_value) for local authentication failed attempts
- Step 2: Run the following to determine whether the standard value is configured.

```
hostname#sh run aaa | in max-fail 3
```

The output should look like

```
aaa local authentication attempts max-fail 3
```

Example:

```
Asa#sh run aaa | in max-fail.3
aaa local authentication attempts max-fail 3
```

Here the max-fail attempts is 3 and it is configured

- Step 3: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to configure the maximum number of consecutive local login failures to be less than or equal to 3

```
hostname(config)# aaa local authentication attempts max-fail 3
```

Default Value:

The aaa local authentication max login attempts is disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/a1.html#wp1557629

Additional Information:

The feature does not affect the privilege level 15 users.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

1.4.1.2 Ensure 'local username and password' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets a local username and password

Rationale:

Default device configuration does not require strong user authentication enabling unfettered access to an attacker that can reach the device. Creating a local account with a strong password enforces login authentication and provides a fallback authentication mechanism in case remote centralized authentication, authorization and accounting services are unavailable

Audit:

- Step 1: Run the following to determine whether a local username password is set

```
hostname#show running-config username
```

The output should look like

```
username <username> password xxxxxxx encrypted
```

Example:

```
Asa#show running-config username
username cisuser password 3USUcOPFUiMCO4Jk encrypted
```

Here the username is cisuser and 3USUcOPFUiMCO4Jk is the encrypted format of the plain-text password that has been configured

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to set a local username and password.

```
hostname(config)#username <local_username> password <local_password>
privilege <level>
```

The privilege level is chosen between 0 and 15. If the privilege is not configured, the default one is 2.

Default Value:

The default username used for the first SSH connection or aaa authentication telnet console is asa but for versions from 8.4(2) and above, there is no default username

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_local.html

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.4.1.3 Ensure known default accounts do not exist (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Deletes the known default accounts configured

Rationale:

In order to attempt access to known devices' platforms, attackers use the available database of the known default accounts for each platform or Operating System. The known default accounts are often (without limiting to) the following: 'root', 'asa', 'admin', 'cisco', 'pix'. When the attacker has discovered that a default account is enabled on a system, the work of attempting to access to the device will be half done given that the remaining part will be on guessing the password and risks for devices to be intruded are very high. It is a best practice to use Enterprise customized administrative accounts.

Audit:

- Step 1: Run the following to determine whether a known default account is available.

```
hostname#show running-config username | in _admin_|_asa_|_cisco_|_pix_|_root_
```

The output should look like:

```
username <known_default_account> password xxxxxxx encrypted
```

Example:

```
Asa-fw-1#show running-config username | in _admin_|_asa_|_cisco_|_pix_|_root_
username admin password 3USUcOPFUiMCO4Jk encrypted privilege 15
```

Here the known default account is admin.

- Step 2: If there is no output displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the Enterprise customized administrative account `<customized\_admin\_account>` and password `<admin\_password>`

- Step 2: Run the following to create the customized administrative account as well as the required privilege level `<privilege\_level>`

```
hostname(config)#username <customized_admin_account> password
<admin_password> privilege <privilege_level>
```

- Step 3: Run the following to delete the known default accounts identified during the audit

```
hostname(config)# no username <known_default_account>
```

Default Value:

The default username used for the first SSH connection or aaa authentication telnet console is asa but for versions from 8.4(2) and above, there is no default username

References:

1. http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html

CIS Controls:

Version 7

4.2 Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

1.4.2 Remote AAA servers

Sets the AAA servers for remote authentication

1.4.2.1 Ensure 'TACACS+/RADIUS' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Specifies the AAA server-group and each individual server using the TACACS+ or RADIUS protocol

Rationale:

Authentication, authorization and accounting (AAA) scheme provide an authoritative source for managing and monitoring access for devices. Many protocols are supported for the communication between the systems and the AAA servers: http-form, kerberos, ldap, nt, radius, sdi, tacacs+.

Audit:

- Step 1: Acquire the enterprise standard protocol (protocol_name) for authentication (TACACS+ or RADIUS)
- Step 2: Perform the following to determine if the AAA server-group is configured with the required protocol

```
hostname#sh run aaa-server | i protocol.<protocol_name>
```

The output should look like:

```
aaa-server server_group_name protocol protocol_name
```

Example:

```
Asa#sh run aaa-server | i protocol.tacacs+
aaa-server cisco_tacacs protocol tacacs+
```

Here the the protocol_name is tacacs+ and server_group_name is cisco_tacacs

- Step 3: If an output is displayed, go to the step 4. If not, it is a finding and the remediation procedure should be applied.

- Step 4: Perform the following to determine if there is at least an AAA server configured for the server group <server_group_name> identified in step 2

```
hostname#sh run aaa-server <server_group_name> | i host
```

The output should look like:

```
aaa-server server_group_name (interface_name) host server_ip_address
```

Example:

```
Asa#sh run aaa-server cisco_tacacs | i host
aaa-server cisco_tacacs (MGMT) host 192.16.0.223
```

Here the server_group_name is cisco_tacacs, the interface_name is MGMT and the server_ip_address is 192.168.0.223

- Step 5: If an output is displayed, the system is compliant. If not, it is a finding and the remediation procedure should be applied.

Remediation:

- Step 1: Acquire the enterprise standard protocol (protocol_name) for authentication (TACACS+ or RADIUS)
- Step 2: Run the following to configure the AAA server-group for the required protocol

```
hostname(config)#aaa-server <server-group_name> protocol <protocol_name>
```

- Step 3: Run the following to configure the AAA server:

```
hostname(config)#aaa-server <server-group_name> (<interface_name>) host <aaa-
server_ip> <shared_key>
```

server-group_name: the above server-group configured
interface_name: the network interface from which the AAA server will be accessed
aaa-server_ip: the IP address of the AAA server
shared_key: the TACACS+ or RADIUS shared key

Default Value:

The AAA server configuraton is by default disabled

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1596656

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3 AAA authentication

Defines the AAA authentication rules

1.4.3.1 Ensure 'aaa authentication enable console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Authenticates users trying to access the Enable mode (privileged EXEC mode) through the 'enable' command.

Rationale:

The default access to enable mode is done through a password. AAA provides a primary method for authenticating users (a username/password database stored on a TACACS+ or RADIUS server or group of servers) and then specifies backup method (a locally stored username/password database). The backup method is used if the primary method's database cannot be accessed by the networking device.

Audit:

- Step 1: Perform the following to determine if the aaa authentication is configured for the access to the enable mode (privileged EXEC mode)

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

The output should look like

```
aaa authentication enable console server_group_name
```

Example:

```
Asa#sh run | i aaa authentication enable console
aaa authentication enable console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the aaa authentication for enable access using the TACACS+ server-group as primary method and the local database as backup method

```
hostname(config)# aaa authentication enable console <server-group_name> local
```

Default Value:

The aaa authentication is disabled by default for the enable mode

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa84/command/reference/a1.html#wp1593705
2. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1594161

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3.2 Ensure 'aaa authentication http console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Authenticates ASDM users who access the security appliance over HTTP

Rationale:

By default, the enable password is used in combination with no username for http access. The aaa command is used to define the TACACS+/RADIUS authentication method. The local database can be mentioned as backup method to this primary method, failing that the ASDM will use the default administrator username and enabled password for authentication.

Audit:

- Step 1: Perform the following to determine if aaa authentication http is configured.

```
hostname#sh run aaa authentication | i http.console
```

The output should look like

```
aaa authentication http console server_group_name
```

Example:

```
Asa#sh run aaa authentication | i http.console
aaa authentication http console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the aaa authentication for http using the TACACS+ server-group as primary method and the local database as backup method.

```
hostname(config)#aaa authentication http console <server-group_name> local
```

Default Value:

The http aaa authentication is disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/command/reference/cmd_ref/a1.html

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3.3 Ensure 'aaa authentication secure-http-client' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Provides a secure method, SSL, to protect username and password to be sent in clear text

Rationale:

If HTTP authentication is used without the command aaa authentication secure-http-client, the username and password are sent from the client to the security appliance in clear text.

Audit:

- Step 1: Perform the following command to determine if the secure communication is enabled.

```
hostname#sh run | i aaa authentication secure-http-client
```

The output should be:

```
aaa authentication secure-http-client
```

Example:

```
Asa#sh run | i aaa authentication secure-http-client
aaa authentication secure-http-client
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the secure aaa authentication for http

```
hostname(config)#aaa authentication secure-http-client
```

Default Value:

The secure aaa authentication for http is disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/command/reference/cmd_ref/a1.html

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3.4 Ensure 'aaa authentication serial console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Authenticates users who access the security appliance using the serial Console port.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA. Fallback mode should also be enabled to allow emergency access to the firewall in the event that the AAA server was unreachable, by utilizing the LOCAL keyword after the AAA server-tag.

Audit:

Step 1: Perform the following to determine if aaa authentication serial is configured.

```
hostname#sh run aaa authentication | i serial.console
```

The output should look like

```
aaa authentication serial console server_group_name
```

Example:

```
Asa#sh run aaa authentication | i serial.console
aaa authentication serial console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the aaa authentication serial using the TACACS+ server-group as primary method and the local database as backup method.

```
hostname(config)#aaa authentication serial console <server-group_name> local
```

Default Value:

The aaa authentication serial console is disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/a1.html#wp1555384

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3.5 Ensure 'aaa authentication ssh console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Authenticates users who access the device using SSH.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA. Fallback mode should also be enabled to allow emergency access to the firewall in the event that the AAA server was unreachable, by utilizing the LOCAL keyword after the AAA server-tag.

Audit:

- Step 1: Perform the following to determine if aaa authentication ssh is configured.

```
hostname#sh run aaa authentication | i ssh.console
```

The output should look like

```
aaa authentication ssh console server_group_name
```

Example:

```
Asa#sh run aaa authentication | i ssh.console
aaa authentication ssh console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the aaa authentication ssh using the TACACS+ server-group as primary method and the local database as backup method.

```
hostname(config)#aaa authentication ssh console <server-group_name> local
```

Default Value:

The aaa authentication ssh console is disabled by default.

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1594161

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.3.6 Ensure 'aaa authentication telnet console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Authenticates users who access the security appliance using Telnet.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA. Fallback mode should also be enabled to allow emergency access to the firewall in the event that the AAA server was unreachable, by utilizing the LOCAL keyword after the AAA server-tag.

Audit:

- Step 1: Perform the following to determine if aaa authentication Telnet is configured.

```
hostname#sh run aaa authentication | i telnet.console
```

The output should look like

```
aaa authentication telnet console server_group_name
```

Example:

```
Asa#sh run aaa authentication | i telnet.console
aaa authentication telnet console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Configure the aaa authentication Telnet using the TACACS+ server-group as primary method and the local database as backup method.

```
hostname(config)#aaa authentication telnet console <server-group_name> local
```

Default Value:

The aaa authentication telnet console is disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/a1.html

Additional Information:

By default, fallback to the local database is disabled.

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.4 AAA Authorization

Defines the AAA authorization rules

1.4.4.1 Ensure 'aaa command authorization' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Defines the source of authorization for the commands entered by an administrator/user

Rationale:

Requiring authorization for commands enforces separation of duties and provides least privilege access for specific job roles.

Audit:

- Step 1: Perform the following to determine if command authorization is enabled

```
hostname#sh run aaa authorization | i command
```

The output should look like

```
aaa authorization command server_group_name
```

Example:

```
Asa#sh run aaa authorization | in command
aaa authorization command cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to determine the remote the TACACS+/RADIUS servers (server_group_name) as source of authorization and the local database (LOCAL) as fallback method if the remote servers are not available.

```
hostname(config)# aaa authorization command <server-group_name> LOCAL
```

This implies that locally, each privilege has its sets of commands configured and username associated just in accordance with the privilege and command definition in the remote servers.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/a1.html

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.4.2 Ensure 'aaa authorization exec' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Limits the access to the privileged EXEC mode

Rationale:

When a user is placed in the privileged EXEC mode, valuable information can be obtained. The AAA authorization exec enforces the segregation of users rights so that only authorized users can get access to the privileged EXEC mode. Once this feature is enabled, the user rights are provided by the authentication servers mentioned in the AAA authentication console and AAA authentication enable schemes.

Audit:

- Step 1: Run the following to determine whether the AAA authentication exec is enabled.

```
hostname# sh run aaa authorization | in exec
```

Example:

```
datacenter-asa# sh run aaa authorization | in exec
aaa authorization exec authentication-server
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable the AAA authorization exec

```
hostname(config)# aaa authorization exec authentication-server
```

Default Value:

Not enabled

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/a1.html

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

1.4.5 AAA Accounting

Defines the AAA accounting rules

1.4.5.1 Ensure 'aaa command accounting' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables accounting of administrative access by specifying that each command, or commands of a specified privilege level or higher, entered by an administrator/user is recorded and sent to the accounting server or servers.

Rationale:

The AAA accounting feature enables to track the actions performed by users and to store the data collected into AAA serves for further audit or further analysis. While the aaa accounting serial, ssh, telnet and enable commands collect and sent the accounting records related to the start and end of sessions done on each access type, the aaa accounting command provides the accounting records related to each command entered by the users during the session and whatever the privilege level of the user.

Audit:

- Step 1: Perform the following to determine if command accounting is enabled.

```
hostname#sh run aaa accounting | in command
```

The output should look like

```
aaa accounting command server_group_name
```

Example:

```
Asa#sh run aaa accounting | in command
aaa accounting command cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding

Remediation:

Run the following in order to record all the commands entered at all the privilege levels and to send them to the AAA servers

```
hostname(config)# aaa accounting command <server-group_name>
```

Default Value:

By default, AAA accounting for administrative access is disabled.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/a1.html#pgfId-1593580

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

1.4.5.2 Ensure 'aaa accounting for SSH' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables accounting of administrative access by specifying the start and stop of SSH sessions

Rationale:

The AAA accounting feature enables to track the actions performed by users and to store the data collected into AAA serves for further audit or further analysis. While the aaa accounting serial, ssh, telnet and enable commands collect and sent the accounting records related to the start and end of sessions done on each access type, the aaa accounting command provides the accounting records related to each command entered by the users during the session and whatever the privilege level of the user.

Audit:

- Step 1: Perform the following to determine if ssh accounting is enabled.

```
hostname#sh run aaa accounting | in ssh
```

The output should look like

```
aaa accounting ssh console server_group_name
```

Example:

```
Asa#sh run aaa accounting | in ssh
aaa accounting ssh console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding

Remediation:

Run the following in order to record ssh session start and stop and to send them to the AAA servers

```
hostname(config)#aaa accounting ssh console <server-group_name>
```

Default Value:

By default, AAA accounting for administrative access is disabled.

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1593580

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

1.4.5.3 Ensure 'aaa accounting for Serial console' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables accounting of administrative access by specifying the start and stop of Serial console sessions

Rationale:

The AAA accounting feature enables to track the actions performed by users and to store the data collected into AAA serves for further audit or further analysis. While the aaa accounting serial, ssh, telnet and enable commands collect and sent the accounting records related to the start and end of sessions done on each access type, the aaa accounting command provides the accounting records related to each command entered by the users during the session and whatever the privilege level of the user.

Audit:

- Step 1: Perform the following to determine if the serial console accounting is enabled.

```
hostname#sh run aaa accounting | in serial
```

The output should look like

```
aaa accounting serial console server_group_name
```

Example:

```
Asa#sh run aaa accounting | in serial
aaa accounting serial console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding

Remediation:

Run the following in order to record serial console session start and stop and to send them to the AAA servers

```
hostname(config)#aaa accounting serial console <server-group_name>
```

Default Value:

By default, AAA accounting for administrative access is disabled.

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1593580

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

1.4.5.4 Ensure 'aaa accounting for EXEC mode' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables accounting of administrative access by specifying the start and stop of EXEC sessions

Rationale:

The AAA accounting feature enables to track the actions performed by users and to store the data collected into AAA serves for further audit or further analysis. While the aaa accounting serial, ssh, telnet and enable commands collect and sent the accounting records related to the start and end of sessions done on each access type, the aaa accounting command provides the accounting records related to each command entered by the users during the session and whatever the privilege level of the user.

Audit:

- Step 1: Perform the following to determine if exec mode accounting is enabled.

```
hostname#sh run aaa accounting | in enable
```

The output should look like

```
aaa accounting command server_group_name
```

Example:

```
Asa#sh run aaa accounting | in enable
aaa accounting enable console cisco_tacacs
```

Here the remote servers group name is cisco_tacacs

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding

Remediation:

Run the following in order to record exec mode session start and stop and to send them to the AAA servers

```
hostname(config)# aaa accounting enable console <server-group_name>
```

Default Value:

By default, AAA accounting for administrative access is disabled.

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a1.html#wp1593580

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

1.5 Banner Rules

Rules in the banner class communicate legal rights to users.

1.5.1 Ensure 'ASDM banner' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the banner message for the ASDM access

Rationale:

Configuring banner is an additional security safeguard to protect the device. In fact, banners are deterrent controls meant to discourage attackers by letting them know that their access is illegitimate and the possible consequences of going further.

Audit:

- Step 1: Run the following command to determine if the ASDM banner is set:

```
hostname#sh run banner asdm | i banner.asdm
```

Example:

```
Asa-fw# sh run banner asdm | in banner.asdm
banner asdm
banner asdm  -----------------"This is the property of CIS"------------------
-----
banner asdm  --------Unauthorized users may be subject to prosecution--------
-----
banner asdm
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to set the ASDM banner where <line_of_message> is a line of the banner text.

```
hostname(config)#banner asdm <line_of_message>
```

Repeat the command for each line if the banner text has several lines.

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/access_management.html

CIS Controls:

Version 7

17.3 Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

1.5.2 Ensure 'EXEC banner' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the banner message for the access to the privileged EXEC mode

Rationale:

Configuring banner is an additional security safeguard to protect the device. In fact, banners are deterrent controls meant to discourage attackers by letting them know that their access is illegitimate and the possible consequences of going further.

Audit:

- Step 1: Run the following command to determine if the EXEC banner is set:

```
hostname#sh run banner exec | i banner.exec
```

Example:

```
Asa-fw# sh run banner exec | in banner.exec
banner exec
banner exec  -----------------"This is the property of CIS"------------------
-----
banner exec  --------Unauthorized users may be subject to prosecution--------
-----
banner exec
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to set the EXEC banner where <line_of_message> is a line of the banner text.

```
hostname(config)#banner exec <line_of_message>
```

Repeat the command for each line if the banner text has several lines.

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/access_management.html

CIS Controls:

Version 7

17.3 Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

1.5.3 Ensure 'LOGIN banner' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the LOGIN banner for access to the Command Line Interface (CLI)

Rationale:

Configuring banner is an additional security safeguard to protect the device. In fact, banners are deterrent controls meant to discourage attackers by letting them know that their access is illegitimate and the possible consequences of going further.

Audit:

- Step 1: Run the following command to determine if the LOGIN banner is set:

```
hostname#sh run banner login | i banner.login
```

Example:

```
Asa-fw# sh run banner login | in banner.login
banner login
banner login  -----------------"This is the property of CIS"-----------------
------
banner login  --------Unauthorized users may be subject to prosecution-------
------
banner login
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to set the LOGIN banner where <line_of_message> is a line of the banner text.

```
hostname(config)#banner login <line_of_message>
```

Repeat the command for each line if the banner text has several lines.

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/access_management.html

CIS Controls:

Version 7

17.3 Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

1.5.4 Ensure 'MOTD banner' is set (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the message-of-the-day (MOTD) banner for first access to the Command Line Interface (CLI).

Rationale:

Configuring banner is an additional security safeguard to protect the device. In fact, banners are deterrent controls meant to discourage attackers by letting them know that their access is illegitimate and the possible consequences of going further.

Audit:

- Step 1: Run the following command to determine if the MOTD banner is set:

```
hostname#sh run banner motd | i banner.motd
```

Example:

```
Asa-fw# sh run banner motd | in banner.motd
banner motd
banner motd  -----------------"This is the property of CIS"------------------
-----
banner motd  --------Unauthorized users may be subject to prosecution--------
-----
banner motd
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to set the MOTD banner where <line_of_message> is a line of the banner text.

```
hostname(config)#banner motd <line_of_message>
```

Repeat the command for each line if the banner text has several lines.

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/access_management.html

CIS Controls:

Version 7

17.3 Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

1.6 SSH rules

Defines the SSH requirements

1.6.1 Ensure 'SSH source restriction' is set to an authorized IP address (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines the client IP addresses that are allowed to connect to the security appliance through SSH

Rationale:

One key element of securing the network is the security of management access to the infrastructure devices. It is critical to establish the appropriate controls in order to prevent unauthorized access to infrastructure devices. One of them is permitting only authorized originators to attempt device management access. This ensures that the processing of access requests is restricted to an authorized source IP address, thus reducing the risk of unauthorized access and the exposure to other attacks, such as brute force, dictionary, or DoS attacks.

Audit:

- Step 1: Run the following to verify if ssh access source restriction is enabled:

```
hostname# sh run ssh | i ssh_[0-9]|[0-9]|[0-9]
```

The output should look like

```
ssh source_ip source_netmask interface_name
```

Example:

```
Asa#sh run ssh | i ssh_[0-9]|[0-9]|[0-9]
ssh 192.168.0.0 255.255.255.0 mgmt
```

Here the source_ip value is 192.168.0.0, the source_netmask 255.255.255.0 and the interface_name is mgmt

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable SSH access source restriction

```
hostname(config)#ssh <source_ip> <source_netmask> <interface_name>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

11.6 Use Dedicated Machines For All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

1.6.2 Ensure 'SSH version 2' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SSH version to 2

Rationale:

SSH is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. The ASA allows SSH connections to the ASA for management purposes. The ASA supports the SSH remote shell functionality provided in SSH Versions 1 and 2. However, SSH version is known to be a vulnerable protocol that can be exploited by attackers.

Audit:

- Step 1: Run the following to determine whether SSH version 2 is enabled:

```
hostname#sh run ssh version | in 2
```

The output should be:

```
 ssh version 2
```

- Step 2: If this output is displayed, the system is compliant. If not, there is a finding.

Remediation:

Run the following to enable SSH version 2

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

Default Value:

By default, the security appliance allows both SSH Version 1 and Version 2

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_management.html

CIS Controls:

Version 7

11.6 Use Dedicated Machines For All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

1.6.3 Ensure 'RSA key pair' is greater than or equal to 2048 bits (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Generates an RSA key pair used by SSH protocol of at least 2048 bits

Rationale:

Secure Shell (SSH) is a secure remote-login protocol. The ASA allows SSH connections to the ASA for management purposes and supports the SSH DES and 3DES ciphers. SSH uses a key-exchange method based on Rivest-Shamir-Adleman (RSA) public-key. Since RSA 1024-bit keys are likely to become crackable, it is recommended to have RSA keys of at least 2048 bits.

Audit:

- Step 1: Run the following to determine whether the RSA key modulus size is equal or greater than 2048 bits.

```
hostname#sh crypto key mypubkey rsa | i _Modulus_Size_.bits.._[2-9][0-9][0-
9][0-9]
```

Ths is an example of output where the key pair modulus size is 2048 bits:

```
Asa# sh crypto key mypubkey rsa | i _Modulus_Size_.bits.._[2-9][0-9][0-9][0-
9]
 Modulus Size (bits): 2048
```

- Step 2: If this output is not displayed, either there is no key configured, either the available modulus size is less than 2048 bits. The system is not compliant. If is a finding.
- Step 3: Run the following to check if there is already an existing RSA key pair:

```
hostname# sh crypto key mypubkey rsa | i ^Key|^_Usage|^_Modulus
```

The example below shows that there are already created RSA key pairs but they are not compliant, since one is 1024 bits and the other 768 bits.

```
Asa# sh crypto key mypubkey rsa | i ^Key|^_Usage|^_Modulus
```

```
 Key pair was generated at: 13:54:47 UTC Sep 14 2008
 Key name: <Default-RSA-Key>
  Usage: General Purpose Key
  Modulus Size (bits): 1024

 Key pair was generated at: 06:43:39 UTC Mar 2 2003
 Key name: <Default-RSA-Key>.server
  Usage: Encryption Key
  Modulus Size (bits): 768
```

Remediation:

- Step 1: Acquire the enterprise standard RSA key size greater or equal than 2048 bits
- Step 2: If the audit procedure revealed existing non-compliant key pairs, run the following to remove them:

```
hostname(config)#crypto key zeroize rsa
```

- Step 3: Run the following to generate compliant RSA key pair:

```
hostname(config)# crypto key generate rsa modulus <enterprise_RSA_key_size>
```

- Step 4: Run the following to save the RSA keys to persistent Flash memory

```
hostname(config)#write memory
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.6.4 Ensure 'SCP protocol' is set to Enable for files transfers (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables Secure Copy protocol

Rationale:

FTP and TFTP are protocols that transfer data in clear text across the network and thus are vulnerable to packet sniffing. Files and mostly configuration files should be transferred using secure protocols such as HTTPS or SCP.

Audit:

- Step 1: Run the following command to determine

```
hostname# sh run ssh | grep scopy
```

Example:

```
Corp-FW# sh run ssh | grep scopy
ssh scopy enable
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to enable secure copy

```
hostname(config)# ssh scopy enable
```

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

1.6.5 Ensure 'Telnet' is disabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the telnet access to the security appliance in the case it has been configured

Rationale:

Telnet is an unsecure protocol as username and password are conveyed in clear text during the administrator authentication and can be retrieved through network sniffing.

Audit:

- Step 1: Run the following to verify if telnet access is enabled:

```
hostname# sh run telnet | i telnet_[0-9]|[0-9]|[0-9]
```

The output should look like

```
telnet source_ip source_netmask interface_name
```

Example:

```
Asa#sh run telnet | i telnet_[0-9]|[0-9]|[0-9]
telnet 192.168.0.0 255.255.255.0 mgmt
telnet timeout 15
```

Here the source_ip value is 192.168.0.0, the source_netmask 255.255.255.0 and the interface_name is mgmt

- Step 2: If this output is displayed, the system is not compliant. It is a finding.

Remediation:

Run the following to remove the telnet access

```
hostname(config)#no telnet 0.0.0.0 0.0.0.0 <interface_name>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_management.html#wp1054101

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.7 HTTP rules

Defines the HTTP requirements

1.7.1 Ensure 'HTTP source restriction' is set to an authorized IP address (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines the client IP addresses that are allowed to connect to the security appliance through HTTP

Rationale:

One key element of securing the network is the security of management access to the infrastructure devices. It is critical to establish the appropriate controls in order to prevent unauthorized access to infrastructure devices. One of them is permitting only authorized originators to attempt device management access. This ensures that the processing of access requests is restricted to an authorized source IP address, thus reducing the risk of unauthorized access and the exposure to other attacks, such as brute force, dictionary, or DoS attacks.

Audit:

- Step 1: Run the following to verify if http access source restriction is enabled:

```
hostname# sh run http | i http_[0-9]|[0-9]|[0-9]
```

The output should look like

```
http source_ip source_netmask interface_name
```

Example:

```
Asa#sh run http | i http_[0-9]|[0-9]|[0-9]
http 192.168.0.0 255.255.255.0 mgmt
```

Here the source_ip value is 192.168.0.0, the source_netmask 255.255.255.0 and the interface_name is mgmt

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable HTTP access source restriction

```
hostname(config)#http <source_ip> <source_netmask> <interface_name>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.7.2 Ensure 'TLS 1.2' is set for HTTPS access (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enable SSL server version to TLS 1.2

Rationale:

Given that the network may be prone to sniffing, the HTTP access to the security appliance must be secured with SSL or TLS protocols. The latest version of SSL that is SSL v3 is now inclined to many vulnerabilities and systems should use at least TLS 1.2 as SSL server version.

Audit:

- Step 1: For Software version 8.x, run the following to check that AES 256 algorithm is enabled

```
hostname#sh run ssl | in encryption.aes256-sha1$
```

Example:

```
Corp_fw#sh run ssl | in encryption.aes256-sha1$
ssl encryption aes256-sha1
```

For Software version 9.x, run the following to check that AES 256 algorithm is enabled

```
hostname#sh run ssl | in custom_"AES256-SHA"$
```

Example:

```
Corp_fw#sh run ssl | in custom_"AES256-SHA"$
ssl cipher tlsv1 custom "AES256-SHA"
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

For version 8.x, run the following command to enable AES 256 algorithm

```
hostname(config)# ssl encryption aes256-sha1
```

For version 9.x, run the following command to enable AES 256 algorithm

```
hostname(config)# ssl cipher tlsv1.2
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/ssl.html

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

1.7.3 Ensure 'SSL AES 256 encryption' is set for HTTPS access (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SSL encryption algorithm to AES 256

Rationale:

Given that the network may be prone to sniffing, the HTTP access to the security appliance must be secured with SSL or TLS protocols. A secure encryption algorithm must be used.

Audit:

- Step 1: For Software version 8.x, run the following to check that AES 256 algorithm is enabled

```
hostname#sh run ssl | in encryption.aes256-sha1$
```

Example:

```
Corp_fw#sh run ssl | in encryption.aes256-sha1$
ssl encryption aes256-sha1
```

For Software version 9.x, run the following to check that AES 256 algorithm is enabled

```
hostname#sh run ssl | in custom_"AES256-SHA"$
```

Example:

```
Corp_fw#sh run ssl | in custom_"AES256-SHA"$
ssl cipher tlsv1 custom "AES256-SHA"
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

For version 8.x, run the following command to enable AES 256 algorithm

```
hostname(config)# ssl encryption aes256-sha1
```

For version 9.x, run the following command to enable AES 256 algorithm

```
hostname(config)# ssl cipher tlsv1 custom AES256-SHA
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm/vpn-asdm-ssl.html

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

1.8 Session timeout

Sets the idle timeout values

1.8.1 Ensure 'console session timeout' is less than or equal to '5' minutes (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the idle timeout for a console session before the security appliance terminates it.

Rationale:

Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to set the console timeout to less than or equal to 5 minutes

```
hostname(config)# console timeout 5
```

Default Value:

The default timeout is 0, which means the console session will not time out.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.8.2 Ensure 'SSH session timeout' is less than or equal to '5' minutes (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the idle timeout for an SSH session before the security appliance terminates it.

Rationale:

Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

Audit:

- Step 1: Run the following to verify the required timeout is configured:

```
hostname#sh run ssh | in timeout.5
```

The output should look like

```
ssh timeout 5
```

Example:

```
Asa#sh run ssh | in timeout.5
ssh timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following to set the SSH timeout to 5 minutes

```
hostname(config)# ssh timeout 5
```

Default Value:

The default session timeout value is 5 minutes.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/admin_management.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

1.8.3 Ensure 'HTTP idle timeout' is less than or equal to '5' minutes (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the timeout for an HTTP session idle before the security appliance terminates it.

Rationale:

Limiting session idle timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

Audit:

- Step 1: Run the following to verify the required timeout is configured:

```
hostname#sh run http | in idle-timeout.5
```

The output should look like

```
http server idle-timeout 5
```

Example:

```
Asa#sh run http | in idle-timeout.5
http server idle-timeout 5
```

Here the session-timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following to set the HTTP timeout to less than or equal to 5 minutes

```
hostname(config)# http server idle-timeout 5
```

Default Value:

The default session timeout value is 20 minutes.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/intro.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

1.9 Clock rules

Sets the device time

1.9.1 NTP rules

Defines the NTP requirements

1.9.1.1 Ensure 'NTP authentication' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables NTP authentication in order to receive time information only from trusted sources

Rationale:

When authentication is not enabled, attackers can disguise as NTP servers and broadcast wrong time and it will be difficult to correlate events upon an incident. In some other cases, attackers can perform NTP DDoS attacks such as NTP Amplification.

Audit:

- Step 1: Run the following command to check whether NTP authentication is enabled

```
hostname#sh run ntp | in authenticate
```

Example:

```
Asa-fw#sh run ntp | in authenticate
ntp authenticate
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to enable NTP authentication

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

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/n.html#wp1814887

1.9.1.2 Ensure 'NTP authentication key' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the key used to authenticate NTP servers

Rationale:

When authentication is not enabled, attackers can disguise as NTP servers and broadcast wrong time and it will be difficult to correlate events upon an incident. In some other cases, attackers can perform NTP DDoS attacks such as NTP Amplification.

Audit:

- Step 1: Run the following command to check whether the NTP key is configured

```
hostname#sh run ntp | in authentication-key
```

Example

```
Asa-fw#sh run ntp | in authentication-key
ntp authentication-key 11 md5 *****
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Run the following to set the authentication key ID <key_id>

```
hostname(config)# ntp trusted-key <key_id>
```

- Step 2: Run the following to configure the authentication key <authentication_key>

```
hostname(config)# ntp authentication-key <key_id> md5 <authentication_key>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/n.html#wp1815345

1.9.1.3 Ensure 'trusted NTP server' exists (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets a NTP server for which authentication is enabled in order to receive time information

Rationale:

When authentication is not enabled, attackers can disguise as NTP servers and broadcast wrong time and it will be difficult to correlate events upon an incident. In some other cases, attackers can perform NTP DDoS attacks such as NTP Amplification. The trusted NTP server will be authenticated through the NTP authentication key.

Audit:

- Step 1: Run the following command to check whether a trusted NTP server is configured

```
hostname#sh run ntp | in [0-5]_key
```

Example

```
Asa-fw#sh run ntp | in [0-5]_key
ntp server 10.140.1.100 key 11 source mgmt
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the authentication key ID <key_id>, the IP address of the NTP server <ip_address> and the interface <interface_name> used by the appliance to communicate with the NTP server.
- Step 2: Run the following to configure the trusted NTP server

```
hostname(config)# ntp server <ip_address> key <key_id> source
<interface_name>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/n.html#wp1815345

1.9.2 Ensure 'local timezone' is properly configured (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the local time zone information so that the time displayed by the ASA is more relevant to those who are viewing it.

Rationale:

Having a correct time set on a Cisco ASA is important for two main reasons. The first reason is that digital certificates compare this time to the range defined by their Valid From and Valid To fields to define a specific validity period. The second reason is to have a relevant time stamps when logging information. Whether you are sending messages to a syslog server, sending messages to an SNMP monitoring station, or performing packet captures, time stamps have little usefulness if you cannot be certain of their accuracy.

Audit:

- Step 1: Acquire standard zone name (enterprise_zone_name) used by the enterprise (GMT, UTC, EDT, PST)
- Step 2: Run the following to check if the required value is configured

```
hostname#sh run clock | in <enterprise_zone_name>
```

The output should look like

```
clock timezone enterprise_zone_name local_offset
```

Example:

```
Asa# sh run clock | in EDT
clock timezone EDT 1
```

Here the enterprise_zone_name is `EDT` and the `local_offset` is `1`

- Step 3: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Acquire standard zone name (enterprise_zone_name) used by the enterprise (GMT, UTC, EDT, PST)

- Step 2: Run the following to configure the required value

```
hostname(config)# clock timezone <enterprise_zone_name> <local_offset>
```

Default Value:

By default, the time zone is UTC

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/basic.html#wp1071217

1.10 Logging Rules

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

1.10.1 Ensure 'logging' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables logging

Rationale:

Logging is fundamental for audit requirements and incident management and should be enabled on any business critical system storing or conveying information

Audit:

- Step 1: Run the following to check if logging is enabled

```
hostname# sh run logging | in enable
```

Example:

```
Dc-fw-01# sh run logging | in enable
logging enable
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable logging

```
hostname(config)#logging enable>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_syslog.html

1.10.2 Ensure 'logging to Serial console' is disabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the logging to the Serial console

Rationale:

Enabling the logs to be sent to the Serial console may negatively impact the logging to the buffer and remote syslog servers and to a certain extent the buffer and syslog servers may no longer receive logs because the logs generation will follow the Serial console speed.

Audit:

- Step 1: Run the following to check if the logging to console is enabled

```
hostname# sh run logging | grep console
```

Example:

```
asa-fw-2# sh run logging | grep console
logging console errors
```

- Step 2: If an output is displayed, the system is not compliant. It is a finding.

Remediation:

Run the following command to disable the logging to console

```
hostname(config)#no logging console
```

Default Value:

The logging to console is disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_syslog.html

1.10.3 Ensure 'logging to monitor' is disabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the logging to monitor

Rationale:

The ASA by default send logs to monitor for Telnet and SSH sessions. The logs messages will continuously scroll on the monitor after the "Terminal Monitor" command is issued. This consumes a lot of resources causing high CPU usage and should be avoided.

Audit:

- Step 1: Run the following to check if the logging monitor is enabled

```
hostname# sh run logging | grep monitor
```

Example:

```
asa-fw-2# sh run logging | grep monitor
logging monitor debugging
```

- Step 2: If an output is displayed, the system is not compliant. It is a finding.

Remediation:

Run the following command to disable the logging monitor

```
hostname(config)#no logging monitor
```

Default Value:

The logging monitor is disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_syslog.html

1.10.4 Ensure 'syslog hosts' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SNMP notification recipient or the NMS or SNMP manager that can connect to the ASA.

Rationale:

Syslog messages are an invaluable tool for accounting, monitoring, and routine troubleshooting. Logging to a central syslog server is a method of collecting messages from devices to a server running a syslog daemon. This helps in aggregation of logs and alerts. This form of logging provides protected long-term storage for logs, since are also useful in incident handling.

Audit:

- Step 1: Run the following to check whether the Syslog host is configured:

```
hostname#sh run logging | i host
```

The output should look like:

```
logging host interface_name host_ip_address
```

Example:

```
Asa#sh run logging | i host
logging host mgmt 10.7.26.5
```

Here the interface name is mgmt, the Syslog server IP address is 10.7.26.5

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

Run the following to configure the Syslog server

```
hostname(config)# logging host <interface_name> <host_ip_address>
```

Default Value:

The syslog server is not configured by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_syslog.html

1.10.5 Ensure 'logging with the device ID' is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Includes the device ID in the logs generated

Rationale:

In an environment where logs are collected from many different sources, identifying the logs from a specific device is alleviated by doing a query including the device's hostname included in the logs and helps to quickly gather the expected results.

Audit:

- Step 1: Run the following to check if logging is enabled with the device id.

```
hostname# sh run logging | in device-id
```

Example:

```
Dc-fw-01# sh run logging | in device-id
logging device-id hostname
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable logging with the device hostname:

```
hostname(config)#logging device-id hostname
```

In a multi-context security appliance, run the following command:

```
hostname(config)#logging device-id context-name
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_syslog.html

1.10.6 Ensure 'logging history severity level' is set to greater than or equal to '5' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines which syslog messages should be sent to the SNMP server.

Rationale:

Syslog messages are an invaluable tool for accounting, monitoring, and routine troubleshooting. They can be sent as SNMP traps to an SNMP server. This provides an additional method for the events to be viewed in real time and a backup method to Syslog servers in case there is an issue with the Syslog protocol.

Audit:

- Step 1: Run the following to verify the required severity level is configured:

```
hostname# sh run logging | in history.5
```

The output should look like

```
logging history 5
```

Example:

```
Asa-fw# sh run | in history.information
logging history informational
```

Here the level is set to notification

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to set the logging level to 5:

```
hostname(config)# logging history 5
```

The severity level can be chosen between 0 and 7

Default Value:

The device does not log to simple network management protocol (SNMP) servers by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_syslog.html

1.10.7 Ensure 'logging with timestamps' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Allows the timestamp to logs generated

Rationale:

Enabling timestamps, to mark the generation time of log messages, reduces the complexity of correlating events and tracing network attacks across multiple devices by providing a holistic view of events thus enabling faster troubleshooting of issues and analysis of incidents.

Audit:

- Step 1: Run the following to check if the timestamp is enabled

```
hostname# sh run logging | grep timestamp
```

Example:

```
asa-fw-2# sh run logging | grep timestamp
logging timestamp
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to enable the logging timestamp

```
hostname(config)#logging timestamp
```

Default Value:

By default, syslog messages do not include timestamp

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_syslog.html

1.10.8 Ensure 'syslog logging facility' is equal to '23' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the facility (location) on the syslog server for the log messages sent by the security appliance

Rationale:

Logs should be directed to a consistent and expected logging facility to ensure proper processing and storage by the remote system. There are eight possible logging facilities: 16 (LOCAL0) through 23 (LOCAL7) for the logs messages sent by the security appliance to the syslog server.

Audit:

- Step 1: Run the following to verify the required syslog facility is configured:

```
hostname#sh run logging | in facility.23
```

The output should look like

```
logging facility 23
```

Example:

```
Asa#sh run logging | in facility.23
logging facility 23
```

Here the facility is 23

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to set the logging facility to 23

```
hostname(config)# logging facility 23
```

Default Value:

The default logging facility value is 20

Additional Information:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_syslog.html

1.10.9 Ensure 'logging buffer size' is greater than or equal to '524288' bytes (512kb) (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines the size of the local buffer in which the logs are stored so that they can be checked by the administrator.

Rationale:

The internal log buffer serves as a temporary storage location. New messages are appended to the end of the list. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated. The internal log buffer allows the administrator performing a health check on the system to locally have the last logs generated.

Audit:

- Step 1: Run the following to verify the required buffer size is configured:

```
hostname# sh run logging | in buffer-size.524288
```

The output should look like

```
logging buffer-size 524288
```

Example:

```
Asa# sh run | in buffer-size.524288
logging buffer-size 524288
```

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to set the `logging buffer-size` to *524288*

The size is in bytes and is to be chosen between 4096 and 1048576 bytes

```
hostname(config)# logging buffer-size 524288
```

Default Value:

The default size is 4kB.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/l2.html#wp1770503

1.10.10 Ensure 'logging buffered severity level' is greater than or equal to '3' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines which syslog messages should be temporary stored in the local buffer so they can be checked by the administrator

Rationale:

The internal log buffer serves as a temporary storage location, thus allowing the administrator performing a health check on the system to locally have the last logs generated. Given that the size of the buffer is limited, it is better to have a specific set of syslog messages to be kept therein.

Audit:

- Step 1: Run the following to verify the required severity level is configured:

```
hostname# sh run logging | in buffered.3
```

The output should look like

```
logging buffered 3
```

Example:

```
Asa# sh run | in buffered.3
logging buffered 3
```

Here the level is notification

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to set the `Logging Buffered` to greater than or equal to `3`:

```
hostname(config)# logging buffered 3
```

The severity level can be chosen between 0 through 7

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_syslog.html

1.10.11 Ensure 'logging trap severity level' is greater than or equal to '5' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines which syslog messages should be sent to the syslog server.

Rationale:

Syslog messages are an invaluable tool for accounting, monitoring, and routine troubleshooting. Logging to a central syslog server is a method of collecting messages from devices to a server running a syslog daemon. This helps in aggregation of logs and alerts. This form of logging provides protected long-term storage for logs, since are also useful in incident handling.

Audit:

- Step 1: Run the following to verify the required severity level is configured:

```
hostname# sh run logging | in trap.5
```

The output should look like

```
logging trap 5
```

Example:

```
Asa# sh run | in trap.5
logging trap 5
```

Here the level is notification

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Run the following command to verify logging trap is equal to 5:

```
hostname(config)# logging trap 5
```

The severity level can be chosen between 0 and 7

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_syslog.html

1.10.12 Ensure email logging is configured for critical to emergency (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables logs to be sent to an email recipient for critical to emergency logs' severity levels

Rationale:

In some cases, the notifications of the Syslog server or the NMS system can be delayed by the time taken to process the logs and build the reports. Some system's events require an immediate intervention of the administrator and it in this case, the logs generated should be directly sent to the administrator email address.

Audit:

- Step 1: Run the following to check if the email logging is enabled.

```
hostname# sh run logging | in mail
```

Example:

```
Dc-fw-01# sh run logging | in mail
logging mail critical
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Run the following to enable email logging for logs with severity level from critical and above (critical, alert and emergency)

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

- Step 2: Obtain from the mail server administrator to create an firewall email account <firewall_email_account> and run the following to enable the account as email source address in the firewall

```
hostname(config)#logging from-address <firewall_email_account>
```

- Step 3: Acquire the firewall administrator email account <firewall_admin_email> and run the following for the security appliance to send logs to its administrator email account

```
hostname(config)#logging recipient-address <firewall_admin_email>
```

- Step 4: Obtain from the mail server administrator the mail server IP address <mail_server_ip> and run the following to configure it in the firewall

```
hostname(config)#smtp-server <mail_server_ip>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_syslog.html

1.11 SNMP Rules

Rules in the simple network management protocol class (SNMP) enforce secure network management and monitoring of the device.

1.11.1 Ensure 'snmp-server group' is set to 'v3 priv' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SNMP v3 group with authentication and privacy

Rationale:

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations.

For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, and are divided into the following three types:

• NoAuthPriv—No Authentication and No Privacy, which means that no security is applied to messages.

• AuthNoPriv—Authentication but No Privacy, which means that messages are authenticated.

• AuthPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.

It is recommended that packets should be authenticated and encrypted

Audit:

- Step 1: Run the following to check if the SNMP group includes packet authentication and encryption

```
hostname# sh run snmp-server group | i v3.priv
```

The output should look like:

```
snmp-server group <group_name> v3 priv
```

Example:

```
sa# sh run snmp-server group | i v3.priv
snmp-server group v3 asagroup priv
```

Here the SNMP v3 group name is asagroup. The keyword 'priv' ensures that the SNMP packets will be authenticated and encrypted

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

Run the following to configure the SNMP v3 group.

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

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/monitor_snmp.html#37189

1.11.2 Ensure 'snmp-server user' is set to 'v3 auth SHA' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SNMP v3 user with SHA authentication and AES-256 encryption

Rationale:

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, and AES (which is available in 128, 192, and 256 versions).

It is recommended to use SHA algorithm for authentication and AES-256 for encryption

Audit:

- Step 1: Run the following to check if there is an SNMP v3 user with SHA authentication

```
hostname#sh run snmp-server user | i auth.SHA
```

The output should look like:

```
snmp-server user XXXXX Authentication_Encryption v3 engineID YYYYY encrypted
auth sha ZZZZZ priv aes 256 WWWWW
```

Example:

```
sa#sh run snmp-server user | i auth.SHA
snmp-server user XXXXX Authentication_Encryption v3 engineID YYYYY encrypted
auth sha ZZZZZ priv aes 256 WWWWW
```

Here the SNMP v3 user is asauser in the group asagroup. The authentication algorithm is SHA and xxxxxxx is the authentication password.

- Step 2: If an output is displayed, go to the step 3. If not, there is a finding. The remediation procedure should be applied
- Step 3: Acquire the SNMP username identified in step 1 configured for SHA authentication
- Step 4: Run the following to check that the identified user is also configured for AES-256 encryption

```
hostname#sh run snmp-server user | i priv.AES.256
```

The output should look like:

```
snmp-server user snmp_user group-name v3 auth SHA authentication_password
priv AES 256 encryption_password
```

Example:

```
Asa#sh run snmp-server user | i priv.AES.256
snmp-server user asauser  asagroup v3 auth SHA xxxxxxx  priv AES 256
yyyyyyyyy
```

Here, for the SNMP v3 user 'asauser', the encryption algorithm is AES-256 and yyyyyyyyy is the encryption password.

- Step 5: If an output is displayed, the system is compliant. If not, there is a finding. The remediation procedure should be applied

Remediation:

Run the following:

```
hostname(config)#snmp-server user <snmp_username>  <group-name> v3 auth SHA
<authentication_password> priv AES 256 <encryption_password>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/monitor_snmp.html#56907

1.11.3 Ensure 'snmp-server host' is set to 'version 3' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the SNMP notification recipient or the NMS or SNMP manager that can connect to the ASA.

Rationale:

An SNMP host is an IP address to which SNMP notifications and traps are sent or which can send requests (polling) to the security appliance. To configure SNMP Version 3 hosts, along with the target IP address, the SNMP username must be provided, because traps are only sent to a configured user. It is an additional access control.

Audit:

- Step 1: Run the following to check whether the SNMP host is configured:

```
hostname#sh run snmp-server host | i version.3
```

The output should look like:

```
snmp-server host interface_name host_ip_address version 3 snmp_user
```

Example:

```
Asa#sh run snmp-server host | i version.3
snmp-server host mgmt 10.7.26.5 version 3 asauser
```

Here the interface name is mgmt, the host IP address is 10.7.26.5 and the SNMP user is asauser

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

Run the following to configure the SNMP v3 host

```
hostname(config)# snmp-server host <interface_name> <host_ip_address> version
3 <snmp_user>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_snmp.html#wp1092024

1.11.4 Ensure 'SNMP traps' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables SNMP traps to be sent to the NMS

Rationale:

The purpose of the SNMP service is to monitor in real time the events occurring on systems in order to meet the security requirement of availability of systems and services. The traps are SNMP notifications sent to the NMS and should be enabled in order to be sent and processed by the NMS. The NMS will then provide a comprehensive aggregation and reporting of events generated, thus helping administrator.

Audit:

- Step 1: Run the following command to determine if SNMP traps are enabled

```
hostname# sh run all | in traps.snmp
```

Example:

```
asa-dc# sh run all | in traps.snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following command to enable SNMP traps

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

Default Value:

By default, only syslog traps are enabled

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_snmp.html

1.11.5 Ensure 'SNMP community string' is not the default string (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets a SNMP community string different from the default one

Rationale:

The SNMP community string is a key used both by the security appliance and the NMS server. The security appliance accepts or rejects the requests from the NMS is a valid key is submitted.

From version 8.2(1) and above, for each community string, there are two SNMP server groups created, one for version 1 and another for version 2C. The default SNMP community string is public and can be used by an attacker to collect unauthorized information from the ASA and hence should be changed.

Audit:

- Step 1: Run the following command to check whether the default SNMP community string is configured

```
hostname# show snmp-server group | in _public
```

Example:

```
Corp-FW# show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview
specified>
notifyview: <no readview specified>
row status: active
groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview
specified>
notifyview: *<no readview specified>
row status: active
Corp-FW#show snmp-server group | in _public
groupname: public                              security model:v1
groupname: public                              security model:v2c
```

- Step 2: If an output is displayed, the system is not compliant, it is a finding.

Remediation:

Run the following command to configure the SNMP community string

```
hostname(config)#snmp-server community <snmp_community_string>
```

In a multi-context environment, run the same command in the context.

Default Value:

The default community string is public.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_snmp.html#wp1042029

2 Control Plane

The control plane covers routing table updates, the traffic directed to the security appliance and generally the dynamic operation of the firewall. Network control protocols like ICMP, ARP, IGMP directed to or sent by the firewall itself also fall into this area.

2.1 Routing protocols authentication

Defines the routing protocols security requirement

2.1.1 Ensure 'RIP authentication' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the authentication of RIPv2 neighbor before routing information is received from the neighbor

Rationale:

Enabling the routing protocol authentication prevents against attackers who can send wrong routing information in order to redirect traffic to their network or send malformed packets in order to saturate and to exhaust the control plane.

Audit:

- Step 1: Run the following command to check if the RIP protocol is enabled

```
hostname#sh run | in router.rip
```

Example:

```
Asa-fw#sh run | in router.rip
router rip
```

- Step 2: If an output is displayed, RIP is enabled. Go to Step 3. If there is no output, RIP is not enabled and the recommendation is not applicable.
- Step 3: Run the following to check whether RIP authentication is enabled

```
hostname#sh run | in rip.authentication.key
```

Example:

```
Asa-fw#sh run | in rip.authentication.key
  rip authentication key ***** key_id 11
```

- Step 4: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the interface <interface_name> used by the firewall to receive RIP routing updates
- Step 2: Agree with the neighbor device on the authencation key <key_value> and determine an authentication key ID <key_id>
- Step 3: Run the following to enable RIP authentication

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

Default Value:

Disabled by default

References:

1. https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/107255-asa-8x-rip-config-ex.html

2.1.2 Ensure 'OSPF authentication' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the authentication of OSPF neighbor before routing information is received from the neighbor

Rationale:

Enabling the routing protocol authentication prevents against attackers who can send wrong routing information in order to redirect traffic to their network or send malformed packets in order to saturate and to exhaust the control plane.

Audit:

- Step 1: Run the following command to check if the OSPF protocol is enabled

```
hostname#sh run | in router.ospf
```

Example:

```
Asa-fw#sh run | in router.ospf
router ospf 5
```

- Step 2: If an output is displayed, OSPF is enabled. Go to Step 3. If there is no output, OSPF is not enabled and the recommendation is not applicable.
- Step 3: Run the following to check whether OSPF authentication is enabled

```
hostname#sh run | in ospf.message-digest-key
```

Example:

```
Asa-fw#sh run | in ospf.message-digest-key
  ospf message-digest-key ******
```

- Step 4: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the interface <interface_name> used by the firewall to receive OSPF routing updates and the area ID <area_id>

- Step 2: Agree with the neighbor device on the authencation key <key_value> and determine an authentication key ID <key_id>
- Step 3: Run the following to enable OSPF authentication

```
hostname(config)#interface <interface_name>
hostname(config-if)#ospf authentication message-digest
hostname(config-if)#ospf message-digest-key <key_id> md5 <key_value>
hostname(config-if)#exit
hostname(config)#area <area_id> authentication message-digest
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/o.html#wp1816505

2.1.3 Ensure 'EIGRP authentication' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the authentication of EIGRP neighbor before routing information is received from the neighbor

Rationale:

Enabling the routing protocol authentication prevents against attackers who can send wrong routing information in order to redirect traffic to their network or send malformed packets in order to saturate and to exhaust the control plane.

Audit:

- Step 1: Run the following command to check if the EIGRP protocol is enabled

```
hostname#sh run | in router.eigrp
```

Example:

```
Asa-fw#sh run | in router.eigrp
router eigrp 200
```

- Step 2: If an output is displayed, EIGRP is enabled. Go to Step 3. If there is no output, EIGRP is not enabled and the recommendation is not applicable.
- Step 3: Run the following to check whether EIGRP authentication is enabled

```
hostname#sh run | in authentication.key.eigrp
```

Example:

```
Asa-fw#sh run | in authentication.key.eigrp
  authentication key eigrp 200 ***** key-id 11
```

- Step 4: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the interface <interface_name> used by the firewall to receive EIGRP routing updates and the EIGRP Autonomous System number <as_number>

- Step 2: Agree with the neighbor device on the authencation key <key_value> and determine an authentication key ID <key_id>
- Step 3: Run the following to enable RIP authentication

```
hostname(config)#interface <interface_name>
hostname(config-if)#authentication mode eigrp <as_number> md5
hostname(config-if)#authentication key eigrp <as_number> <key_value> key-id
<key_id>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/a3.html#wp1718640

2.2 Ensure 'noproxyarp' is enabled for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the Proxy-ARP function on untrusted interfaces

Rationale:

The ASA replies to ARP requests performed to IP addresses belonging to its interfaces' subnets and also to global IP addresses in some NAT configurations. Where the appliance is not asked to be a proxy for ARP requests, the Proxy-ARP function should be disabled especially on untrusted interfaces since attackers can act as legitimate devices by spoofing their IP addresses, perform ARP requests thus receiving packets intended to them.

Audit:

- Step 1: Acquire the name of the untrusted interface <untrusted_interface_name>
- Step 2: Run the following to check whether the Proxy-ARP is disabled on the interface

```
hostname# sh run sysopt | grep proxyarp.<untrusted_interface_name>
```

Example:

```
asa_fw_1# sh run sysopt | grep proxyarp.DMZ
sysopt noproxyarp DMZ
```

Here the untrusted interface name is DMZ

- Step 3: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the name of the untrusted interface <untrusted_interface_name>
- Step 2: Run the following command to disable the Proxy-ARP on the untrusted interface.

```
hostname(config)# sysopt noproxyarp <untrusted_interface_name>
```

Default Value:

Proxy-ARP is enabled by default

References:

1. https://supportforums.cisco.com/discussion/9867551/sysopt-noproxyarp

2.3 Ensure 'DNS Guard' is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the protection against DNS cache poisoning attacks

Rationale:

A DNS cache is poisoned when it contains incorrect entries that redirect traffic to an attacker website. When the DNS queries performed towards legitimate DNS servers, attackers can spoof the Identifier of the DNS header along with the DNS caching server UDP port in order to provide a reply as from an authoritative DNS server. The DNS Guard function helps eliminating subsequent replies coming after the authoritative server reply.

Audit:

- Step 1: Run the following to determine if the DNS Guard is enabled.

```
hostname# show running-config dns-guard
```

Example:

```
asa-dmz1# show running-config dns-guard
dns-guard
```

- Step 2: If an output is displayed, the system is compliant. If not it is a finding.

Remediation:

Run the following command to enable the DNS Guard function.

```
hostname(config)# dns-guard
```

Default Value:

The function is disabled for the related software versions

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/d3.html

2.4 Ensure DHCP services are disabled for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Disables the DHCP service

Rationale:

The ASA can act as a DHCP or DHCP Relay server. However, on untrusted interface, attacker can get the opportunity of the availability of the service to perform DoS attacks such as DHCP starvation that will exhaust not only the IP addresses' space but also the memory and CPU resources of the security appliance and bring it down.

Audit:

- Step 1: Acquire the name of the untrusted interface <untrusted_interface_name>
- Step 2: Run the following command to check if the DHCP service is enabled on the untrusted interface

```
hostname# sh run | in dhcpd.enable.<untrusted_interface_name>
```

Example:

```
Extrnl-FW# sh run | in dhcpd.enable.outside
dhcpd enable outside
```

Here outside is the name of the untrusted interface.

- Step 3: If there is no output displayed, go to the step 4. If not, it is a finding and the remediation procedure should be applied.
- Step 4: Run the following command to check if the DHCP Relay service is enabled on the untrusted interface

```
hostname# sh run | in dhcprelay.enable.<untrusted_interface_name>
```

Example:

```
Extrnl-FW# sh run | in dhcprelay.enable.outside
dhcprelay enable outside
```

- Step 5: If there is no output displayed, the system is compliant. If not, it is a finding and the remediation procedure should be applied.

Remediation:

- Step 1: Acquire the name of the untrusted interface <untrusted_interface_name>
- Step 2: Run the following command to disable DHCP service on the untrusted interface

```
hostname(config)# no dhcpd enable <untrusted_interface_name>
```

- Step 3: Run the following command to disable DHCP Relay service on the untrusted interface

```
hostname(config)# no dhcprelay enable <untrusted_interface_name>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/basic_dhcp.html

2.5 Ensure ICMP is restricted for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Allows ICMP traffic for specific hosts or subnets and denies ICMP traffic for all other sources

Rationale:

ICMP is an important troubleshooting tool that can also be used to perform ICMP attacks on untrusted interfaces. For these interfaces, the ICMP traffic should be allowed only for specific hosts or subnets that are trusted by the Enterprise and should be denied for all other sources.

Audit:

- Step 1: Acquire the untrusted interface name <untrusted_interface_name>
- Step 2: Run the following command to determine whether ICMP is denied on the interface

```
hostname#sh run icmp | in deny.any.<untrusted_interface_name>
```

Example:

```
Corp-FW# sh run icmp | in deny.any.Outside
icmp deny any Outside
```

Here the untrusted interface name is Outside.

- Step 3: If there is an output to this command that is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the untrusted interface name <untrusted_interface_name>, the trusted subnet and corresponding subnet mask
- Step 2: Run the following command to allow ICMP from the trusted subnet to the untrusted interface. Repeat the command if there are more than one trusted subnets identified.

```
hostname(config)# icmp permit <subnet> <mask> <untrusted_interface_name>
```

- Step 3: Run the following command to deny ICMP from all other sources to the untrusted interface.

```
hostname(config)# icmp deny any<untrusted_interface_name>
```

Default Value:

ICMP is enabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/i1.html

3 Data Plane

The data plane is for services and settings related to the data passing through the security appliance (as opposed to the traffic directed to it). It includes interface access lists, firewall functionality, traffic inspection, NAT, and IPSec.

3.1 Ensure DNS services are configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets DNS server(s) to be used by the appliance to perform DNS queries

Rationale:

The security appliance may perform DNS queries in order to achieve URL filtering or threat protection against Botnet traffic.

Audit:

- Step 1: Run the following to determine whether DNS lookup is enabled.

```
hostname#sh run all | in domain-lookup
```

The output should look like:

```
hostname#dns domain-lookup <interface_name>
```

where interface_name is the name of the interface connected to the DNS server
Example:

```
asa_dmz#sh run all | in domain-lookup
dns domain-lookup outside
```

Here the dns lookup is enabled and outside interface connects to DNS server

- Step 2: If an output is displayed, go to step 3. If not, it is a finding and the remediation procedure should be applied.
- Step 3: Acquire the enterprise authorized DNS servers' IP addresses <dns_ip_address> and for each of them, run the following command to determine if the DNS server has been configured.

```
hostname#sh run all | i name-server_<dns_ip_address>
```

The output should look like:

```
dns name-server <em><dns_ip_address></em>
```

Example:

```
asa_dmz#sh run all | in name-server_8.8.8.8
dns name-server 8.8.8.8
asa_dmz#sh run all| in name-server_10.1.1.254
dns name-server 10.1.1.254
```

Here the configured DNS servers are 8.8.8.8 and 10.1.1.254

- Step 4: If an output is displayed, the system is compliant. If not it is a finding.

Remediation:

- Step 1: Run the following to enable the DNS lookup

```
hostname(config)# dns domain-lookup <interface_name>
```

<interface_name> is the name of the interface connected to the DNS server

- Step 2: Configure the group of DNS servers

```
hostname(config)# dns server-group DefaultDNS
```

- Step 3: Acquire the enterprise authorized DNS servers' IP addresses <dns_ip_address> and for each of them, run the following command to configure the DNS server in the DNS server group

```
hostname(config-dns-server-group)#name-server <dns_ip_address>
```

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_hostname_pw.pdf

3.2 Ensure intrusion prevention is enabled for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the intrusion prevention with the IP audit feature on untrusted interfaces

Rationale:

The intrusion prevention is an additional feature for which the security appliance audits the traffic in order to identify vulnerability exploits. This is achieved because specific signatures are matched in the traffic. There are two types of signatures, attack signature for which the traffic is intended to harm the internal resource and informational signature for which the traffic is to gather information on internal resources through port scans, ping sweeps, DNS zone transfers and many others. The possible actions to prevent the intrusion are to drop the traffic, to reset the connection or to send an alarm.

Audit:

- Step 1: Acquire the name of the untrusted interface <interface_name>
- Step 2: Run the following to determine if there is a configured audit policy to prevent against attack signatures

```
hostname# sh run ip audit name | in _attack_
```

Example:

```
Asa-fw# sh run ip audit name | in _attack_
ip audit name ips-fw attack action alarm reset
```

Here the audit policy name is ips-fw

- Step 3: If there is an output displayed, collect the audit policy name <audit_name> and go to Step 4. If there is no output, the system is not compliant. It is a finding. The remediation procedure should be applied.
- Step 4: Run the following to determine if the identified audit policy is enabled on the untrusted interface

```
hostname#sh run ip audit interface <interface_name> | in <audit_name>
```

Example:

```
Asa-fw# sh run ip audit interface outside | in ips-fw
ip audit interface outside ips-fw
```

Here, the audit policy ips-fw is applied to the untrusted interface named outside

- Step 5: If there is an output, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the Enterprise standard action <prevention_action> to be performed when an attack signature is matched. It is to be chosen between 'drop' (The packet is dropped) and 'reset' (The packet is dropped and the connection closed)
- Step 2: Run the following to enable the audit policy against the attack signatures with the Enterprise standard action

```
hostname(config)# ip audit name <audit_name> attack action alarm
<prevention_action>
```

- Step 3: Identify the untrusted interface <interface_name>
- Step 4: Run the following to enable the intrusion prevention on the untrusted interface

```
hostname(config)# ip audit interface <interface_name> <audit_name>
```

Default Value:

Disabled

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/i3.html#wp1913566

3.3 Ensure packet fragments are restricted for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the security appliance to drop fragmented packets received on the untrusted interface.

Rationale:

Attackers use fragmentation to evade security systems such as firewalls or IPS because the checks are usually performed on the first fragment. They can then put malicious payload in the other fragments to perform DoS against internal systems. Disabling the fragmentation on the security appliance implies changing its default behavior from accepting up to 24 fragments in a packet to accepting only 1 fragment in a packet. In other words, it implies accepting only non fragmented packets.

Audit:

- Step 1: Acquire the name of the untrusted interface <interface_name>
- Step 2: Run the following to check if fragmentation is disabled on the interface

```
hostname# sh run fragment <interface_name> | in chain_1_
```

Example:

```
Asa-fw#sh run fragment Outside | in chain_1_
fragment chain 1 Outside
```

The Outside interface is configured to deny fragments.

- Step 3: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the name of the untrusted interface <interface_name>
- Step 2: Run the following command to deny fragments on the interface.

```
hostname(config)#fragment chain 1 <interface_name>
```

Default Value:

The default value for the fragment chain is 24.

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/f2.html#wp2019322

3.4 Ensure non-default application inspection is configured correctly (Manual)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the inspection of an application that is not in the default global policy application inspection

Rationale:

By default, the ASA configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (global policy). Not all inspections are enabled by default. The default policy can be edited in order to enable inspection for a specific application that is not by default included in it.

Audit:

Step 1: Run the following to determine whether the protocol <protocol_name> to be inspected is included in the default policy

```
hostname#sh run policy-map | in __inspect.<protocol_name>
```

The output should look like:

```
  inspect protocol_name
```

The example below confirms that the FTP protocol is inspected

```
Asa# sh run policy-map | in __inspect.ftp
  inspect ftp
```

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

Run the following to enable the inspection of the protocol:

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect <protocol_name>
hostname(config-pmap-c)# exit
```

```
hostname(config-pmap)# exit
hostname(config)#service-policy global_policy global
```

Default Value:

The default policy configuration includes the following commands to inspect applications: class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect ip-options inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp service-policy global_policy global

References:

1. http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113069-asa-disgi-enai-asdm-00.html
2. https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113499-asa-ip-options-00.html

3.5 Ensure DOS protection is enabled for untrusted interfaces (Manual)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Determines the maximum connections, maximum embryonic connections, maximum connections per client and maximum embryonic connections per client that can be accepted on the outside interface

Rationale:

Limiting the number of connections protects from a DoS attack. The ASA uses the per-client limits and the embryonic connection limits to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests.

Audit:

- Step 1: Run the following to determine whether the DOS protection is enabled

```
hostname#sh run policy-map | i set.connection
```

The output should look like:

```
  set connection connection_type max_value
```

The example below gives the values for maximum connections, maximum embryonic connections, maximum connections per client and maximum embryonic connections per client

```
Asa#sh run policy-map | i set.connection
    set connection conn-max 9500
    set connection embryonic-conn-max 5000
    set connection per-client-embryonic-max 100
    set connection per-client-max 75
```

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

Remediation:

- Step 1: Acquire the enterprise standard values for maximum connections, maximum embryonic connections, maximum connections per client and maximum embryonic connections per client
- Step 2: Run the following to configure the class to identify the traffic on which DOS protection should be performed.

```
hostname(config)# class-map <class_name>
hostname(config-cmap)# match any
```

Step 3: Run the following to configure the policy that will determine the maximum connections to be applied on the class previously configured

```
hostname(config)# policy-map <policy_name>
hostname(config-pmap)# class <class_name>
hostname(config-pmap-c)# set connection conn-max <enterprise_max_number>
hostname(config-pmap-c)# set connection embryonic-conn-max
<enterprise_max_number>
hostname(config-pmap-c)# set connection  per-client-embryonic-max
<enterprise_max_number>
hostname(config-pmap-c)# set connection per-client-max
<enterprise_max_number>
```

The enterprise_max_number parameter is to be taken between 0 and 65535.

- Step 4: Run the following to apply the policy previously configured on the untrusted

```
hostname(config-pmap-c)# service-policy <policy_name> interface
<untrusted_interface_name>
```

Default Value:

The default maximum value is 0 meaning there is no limitation

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_connlimits.html

3.6 Ensure 'threat-detection statistics' is set to 'tcp-intercept' (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables threat detection statistics for attacks blocked by the TCP Intercept function

Rationale:

The TCP Intercept function helps protecting the network and particularly servers against DOS attacks. When the maximum count of allowed connections is reached, through the TCP Intercept function, the firewall will no longer allow connection to the impacted server and will act as a proxy to the attack server until a valid traffic is received.

Enabling statistics can help to prevent the attacks at the earliest stage possible upstream.

Audit:

- Step 1: Run the following to check whether TCP Intercept threat detection statistics is enabled

```
hostname# sh run all threat-detection | in tcp-intercept
```

Example:

```
fw-4-dmz# sh run all threat-detection | in tcp-intercept
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400
average-rate 200
```

- Step 2: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

Run the following to enable threat detection statistics for TCP Intercept

```
hostname(config)# threat-detection statistics tcp-intercept
```

Default Value:

Not enable by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_threat.html#wp1094068

3.7 Ensure 'ip verify' is set to 'reverse-path' for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Enables the unicast Reverse-Path Forwarding (uRPF) on untrusted interfaces.

Rationale:

The unicast Reverse-Path Forwarding(uRPF) enabled on an interface ensures that for a packet received on an interface, the security appliance checks the routing table to make sure that the same interface is used to get back to the source IP address. If it is not the case, the packet will be dropped. This should be enabled by default on untrusted interfaces in order to prevent attackers from spoofing internal IP addresses. For the other internal interfaces, the uRPF should be enabled if there is no case of asymmetric routing for which the path to send a packet to the source IP address is different of the path from which the packet is received.

Audit:

- Step 1: Acquire the name of the untrusted interface <interface_name>
- Step 2: Run the following command to check if the uRPF is enabled on the interface

```
hostname# sh run ip verify reverse-path interface <interface_name>
```

Example:

```
Asa-fw#sh run ip verify reverse-path interface Outside
ip verify reverse-path interface Outside
```

- Step 3: If there is no output displayed, the system is not compliant. It is a finding.

Remediation:

- Step 1: Acquire the name of the untrusted interface <interface_name>
- Step 2: Run the following command to enable protection against IP spoofing

```
hostname(config)# ip verify reverse-path interface <interface_name>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/security/asa/asa90/command/reference/i3.html#wp1915749

3.8 Ensure 'security-level' is set to '0' for Internet-facing interface (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Sets the security level of the Internet facing interface to 0

Rationale:

Where security zones are not configured, the Internet facing interface is the most untrusted interface and must have the lowest security-level that is 0. Therefore, any traffic initiated from this interface to the other interfaces of the security appliance must be checked by a specific access-control list rule in order to be permitted.

Audit:

- Step 1: Acquire the physical name of the Internet facing interface <interface_physical_name>
- Step 2: Run the following command to check if its assigned security-level is 0

```
hostname#sh run interface <interface_physical_name> | in security-level.0
```

Example:

```
sh run interface GigabitEthernet 0/3.202 | in security-level.0
security-level 0
```

Here GigabitEthernet 0/3.202 is the physical name of the Internet facing interface

- Step 3: If an output is displayed, the system is compliant. If not, it is a finding.

Remediation:

- Step 1: Acquire the physical name of the Internet facing interface <interface_physical_name>
- Step 2: Run the following command assigned the security-level 0

```
hostname(config)#interface <interface_physical_name>
hostname(config-if)#security-level 0
```

Default Value:

Security level is not assigned by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/int5505.html

3.9 Ensure Botnet protection is enabled for untrusted interfaces (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Filters Botnet traffic on the untrusted interface

Rationale:

In a Botnet condition, many computers in the Enterprise network after being infected with malware and mostly trojans will collect data without the knowledge of the users owning them and send it to the attacker network. In other cases, the infected computers are remotely controlled to forward the same viruses that infected them to many other computers on the Internet. The Botnet protection enables the security appliance to filter and drop the botnet traffic

Audit:

- Step 1: Run the following command to check whether botnet traffic filter is enabled

```
hostname#sh run dynamic-filter | in enable
```

Example:

```
Corp-FW#sh run dynamic-filter | in enable
dynamic-filter enable interface outside
```

Here the Botnet traffic filter is enabled on the outside interface

- Step 2: If there is an output displayed, go to step 3. If there is no output displayed, the system is not compliant. It is a finding.
- Step 3: Run the following command to check whether the botnet malware traffic is dropped.

```
hostname#sh run dynamic-filter | in drop
```

Example:

```
Corp-FW#sh run dynamic-filter | in drop
dynamic-filter drop blacklist interface outside
```

Here the Botnet traffic on the outside interface is dropped

- Step 4: If there is an output displayed, the system is compliant. If there is no output displayed, the system is not compliant. It is a finding.

Remediation:

- Step 1: Run the following command to ensure that the DNS server is available.

```
hostname#sh run | i name-server
```

If there is no DNS server, configure the DNS server according to the related recommendation.

- Step 2: Run the following commands to enable the security appliance to download and use for inspection the lists of known malware websites

```
hostname(config)#dynamic-filter updater-client enable
hostname(config)#dynamic-filter use-database
```

- Step 3: Run the following command to create a class map for the security appliance to match the DNS traffic

```
hostname(config)#class-map <dns_class_map_name>
hostname(config-cmap)#match port udp eq domain
```

- Step 4: Run the following to create the policy-map in order to ask the appliance to inspect the matched DNS traffic and to compare the domain name in the DNS traffic with the list of known malware related domain names.

```
hostname(config)#policy-map <dns_policy_map_name>
hostname(config-pmap)# class <dns_class_map_name>
hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
```

- Step 5: Run the following for the inspection to be applied on the untrusted interface

```
hostname(config)# service-policy <dns_policy_map_name> interface
<untrusted_interface_name>
```

- Step 6: Run the following to monitor the Botnet traffic crossing the untrusted interface

```
hostname(config)# dynamic-filter enable interface <untrusted_interface_name>
```

- Step 7: Run the following to drop any identified Botnet traffic on the untrusted interface

```
hostname(config)# dynamic-filter drop blacklist interface
<untrusted_interface_name>
```

Default Value:

Disabled by default

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_botnet.html

3.10 Ensure ActiveX filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Removes ActiveX controls from the HTTP reply traffic received on the security appliance.

Rationale:

ActiveX controls are used to provide a rich users' browsing experience. Because the ActiveX control is a written program that is executed in the users' computers, it can be used by attackers to perform malicious tasks on the machines of their victims.

Audit:

- Step 1: Run the following command to check whether ActiveX filtering is enabled.

```
hostname#sh run filter | i activex
```

Example:

```
Corp-FW#sh run filter | i activex
filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

- Step 2: If an output is displayed, the system is compliant. If not it is a finding.

Remediation:

- Step 1: Acquire the TCP port used for the HTTP traffic containing ActiveX objects, the IP address <internal_users_ip> and mask <internal_users_mask> of internal users generating the HTTP traffic, and the IP address <external_servers_ip> and mask <external_servers_mask> of the external servers to which the internal users connect and that are source of ActiveX objects.
- Step 2: Run the following command to filter ActiveX applets.

```
hostname(config)# filter activex <port> <internal_users_ip>
<internal_users_mask> <external_servers_ip> <external_servers_mask>
```

Default Value:

ActiveX control filtering is disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa81/config/guide/config/filter.html

3.11 Ensure Java applet filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Removes Java applets from the HTTP reply traffic crossing the security appliance.

Rationale:

Java applets enhance users' Web experience with more interactivity. Because the applet is a code that is downloaded and executed on the users' machines, it can be used by attackers to perform malicious activities on the systems visiting untrusted websites.

Audit:

- Step 1: Run the following command to check whether Java filtering is enabled.

```
<strong>hostname#sh run filter | i java</strong>
```

Example:

```
Corp-FW#sh run filter | i java
filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

- Step 2: If an output is displayed, the system is compliant. If not it is a finding.

Remediation:

- Step 1: Acquire the TCP port used for the HTTP traffic containing Java objects, the IP address <internal_users_ip> and mask <internal_users_mask> of internal users generating the HTTP traffic, and the IP address <external_servers_ip> and mask <external_servers_mask> of the external servers to which the internal users connect and that are source of Java objects.
- Step 2: Run the following command to filter Java applets.

```
hostname(config)# filter java <port> <internal_users_ip>
<internal_users_mask> <external_servers_ip> <external_servers_mask>
```

Default Value:

Java applet filtering is disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa81/config/guide/config/filter.html

3.12 Ensure explicit deny in access lists is configured correctly (Automated)

Profile Applicability:

- Level 1 - Cisco ASA 8.x

Description:

Ensures that each access-list has an explicit deny statement

Rationale:

Configuring an explicit deny entry, with log option, at the end of access control lists enables monitoring and troubleshooting traffic flows that have been denied. Logging these events can provide an effective record to troubleshoot issues and attacks.

Audit:

- Step 1: Run the following command to determine the access-list that are applied to interfaces

```
hostname# sh run access-group
```

Example:

```
Asa-fw#sh run access-group
access-group inside_acl in interface Inside
access-group web_acl in interface Web
access-group dmz1_acl in interface Dmz1
access-group outside_acl in interface Outside
access-group finance_acl in interface Finance
```

- Step 2: Run the following to check if explicit deny is configured

```
hostname#sh run access-list | in deny.ip.any.any
```

Example:

```
Asa-fw#sh run access-list | in deny.ip.any.any
access-list outside_acl extended deny ip any any log
access-list web_acl extended deny ip any any log
access-list finance_acl extended deny ip any any log
```

- Step 3: If all the access-lists listed in step 1 are present in step 2, the system is compliant. If not it is a finding.

Remediation:

- Step 1: Acquire the name <access-list_name> of the access-list that is not compliant from the audit procedure
- Step 2: Run the following to configure the explicit deny.

```
hostname(config)#<access-list_name> extended deny ip any any log
```

The statement will be placed at the end of the access-list

Default Value:

Disabled by default.

References:

1. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/acl_overview.html

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Management Plane**		
1.1	**Password Management**		
1.1.1	Ensure 'Logon Password' is set (Automated)	☐	☐
1.1.2	Ensure 'Enable Password' is set (Automated)	☐	☐
1.1.3	Ensure 'Master Key Passphrase' is set (Automated)	☐	☐
1.1.4	Ensure 'Password Recovery' is disabled (Automated)	☐	☐
1.1.5	Ensure 'Password Policy' is enabled (Automated)	☐	☐
1.2	**Device Management**		
1.2.1	Ensure 'Domain Name' is set (Automated)	☐	☐
1.2.2	Ensure 'Host Name' is set (Automated)	☐	☐
1.2.3	Ensure 'Failover' is enabled (Automated)	☐	☐
1.2.4	Ensure 'Unused Interfaces' is disable (Automated)	☐	☐
1.3	**Image security**		
1.3.1	Ensure 'Image Integrity' is correct (Manual)	☐	☐
1.3.2	Ensure 'Image Authenticity' is correct (Automated)	☐	☐
1.4	**Authentication, Authorization and Accounting (AAA)**		
1.4.1	**Local AAA rules**		
1.4.1.1	Ensure 'aaa local authentication max failed attempts' is set to less than or equal to '3' (Automated)	☐	☐
1.4.1.2	Ensure 'local username and password' is set (Automated)	☐	☐
1.4.1.3	Ensure known default accounts do not exist (Automated)	☐	☐
1.4.2	**Remote AAA servers**		
1.4.2.1	Ensure 'TACACS+/RADIUS' is configured correctly (Automated)	☐	☐
1.4.3	**AAA authentication**		
1.4.3.1	Ensure 'aaa authentication enable console' is configured correctly (Automated)	☐	☐
1.4.3.2	Ensure 'aaa authentication http console' is configured correctly (Automated)	☐	☐
1.4.3.3	Ensure 'aaa authentication secure-http-client' is configured correctly (Automated)	☐	☐
1.4.3.4	Ensure 'aaa authentication serial console' is configured correctly (Automated)	☐	☐
1.4.3.5	Ensure 'aaa authentication ssh console' is configured correctly (Automated)	☐	☐
1.4.3.6	Ensure 'aaa authentication telnet console' is configured correctly (Automated)	☐	☐

1.4.4	**AAA Authorization**		
1.4.4.1	Ensure 'aaa command authorization' is configured correctly (Automated)	☐	☐
1.4.4.2	Ensure 'aaa authorization exec' is configured correctly (Automated)	☐	☐
1.4.5	**AAA Accounting**		
1.4.5.1	Ensure 'aaa command accounting' is configured correctly (Automated)	☐	☐
1.4.5.2	Ensure 'aaa accounting for SSH' is configured correctly (Automated)	☐	☐
1.4.5.3	Ensure 'aaa accounting for Serial console' is configured correctly (Automated)	☐	☐
1.4.5.4	Ensure 'aaa accounting for EXEC mode' is configured correctly (Automated)	☐	☐
1.5	**Banner Rules**		
1.5.1	Ensure 'ASDM banner' is set (Automated)	☐	☐
1.5.2	Ensure 'EXEC banner' is set (Automated)	☐	☐
1.5.3	Ensure 'LOGIN banner' is set (Automated)	☐	☐
1.5.4	Ensure 'MOTD banner' is set (Automated)	☐	☐
1.6	**SSH rules**		
1.6.1	Ensure 'SSH source restriction' is set to an authorized IP address (Automated)	☐	☐
1.6.2	Ensure 'SSH version 2' is enabled (Automated)	☐	☐
1.6.3	Ensure 'RSA key pair' is greater than or equal to 2048 bits (Automated)	☐	☐
1.6.4	Ensure 'SCP protocol' is set to Enable for files transfers (Automated)	☐	☐
1.6.5	Ensure 'Telnet' is disabled (Automated)	☐	☐
1.7	**HTTP rules**		
1.7.1	Ensure 'HTTP source restriction' is set to an authorized IP address (Automated)	☐	☐
1.7.2	Ensure 'TLS 1.2' is set for HTTPS access (Automated)	☐	☐
1.7.3	Ensure 'SSL AES 256 encryption' is set for HTTPS access (Automated)	☐	☐
1.8	**Session timeout**		
1.8.1	Ensure 'console session timeout' is less than or equal to '5' minutes (Automated)	☐	☐
1.8.2	Ensure 'SSH session timeout' is less than or equal to '5' minutes (Automated)	☐	☐
1.8.3	Ensure 'HTTP idle timeout' is less than or equal to '5' minutes (Automated)	☐	☐
1.9	**Clock rules**		
1.9.1	**NTP rules**		

1.9.1.1	Ensure 'NTP authentication' is enabled (Automated)	☐	☐
1.9.1.2	Ensure 'NTP authentication key' is configured correctly (Automated)	☐	☐
1.9.1.3	Ensure 'trusted NTP server' exists (Automated)	☐	☐
1.9.2	Ensure 'local timezone' is properly configured (Automated)	☐	☐
1.10	**Logging Rules**		
1.10.1	Ensure 'logging' is enabled (Automated)	☐	☐
1.10.2	Ensure 'logging to Serial console' is disabled (Automated)	☐	☐
1.10.3	Ensure 'logging to monitor' is disabled (Automated)	☐	☐
1.10.4	Ensure 'syslog hosts' is configured correctly (Automated)	☐	☐
1.10.5	Ensure 'logging with the device ID' is configured correctly (Automated)	☐	☐
1.10.6	Ensure 'logging history severity level' is set to greater than or equal to '5' (Automated)	☐	☐
1.10.7	Ensure 'logging with timestamps' is enabled (Automated)	☐	☐
1.10.8	Ensure 'syslog logging facility' is equal to '23' (Automated)	☐	☐
1.10.9	Ensure 'logging buffer size' is greater than or equal to '524288' bytes (512kb) (Automated)	☐	☐
1.10.10	Ensure 'logging buffered severity level' is greater than or equal to '3' (Automated)	☐	☐
1.10.11	Ensure 'logging trap severity level' is greater than or equal to '5' (Automated)	☐	☐
1.10.12	Ensure email logging is configured for critical to emergency (Automated)	☐	☐
1.11	**SNMP Rules**		
1.11.1	Ensure 'snmp-server group' is set to 'v3 priv' (Automated)	☐	☐
1.11.2	Ensure 'snmp-server user' is set to 'v3 auth SHA' (Automated)	☐	☐
1.11.3	Ensure 'snmp-server host' is set to 'version 3' (Automated)	☐	☐
1.11.4	Ensure 'SNMP traps' is enabled (Automated)	☐	☐
1.11.5	Ensure 'SNMP community string' is not the default string (Automated)	☐	☐
2	**Control Plane**		
2.1	**Routing protocols authentication**		
2.1.1	Ensure 'RIP authentication' is enabled (Automated)	☐	☐
2.1.2	Ensure 'OSPF authentication' is enabled (Automated)	☐	☐
2.1.3	Ensure 'EIGRP authentication' is enabled (Automated)	☐	☐
2.2	Ensure 'noproxyarp' is enabled for untrusted interfaces (Automated)	☐	☐
2.3	Ensure 'DNS Guard' is enabled (Automated)	☐	☐
2.4	Ensure DHCP services are disabled for untrusted interfaces (Automated)	☐	☐

2.5	Ensure ICMP is restricted for untrusted interfaces (Automated)	☐	☐
3	**Data Plane**		
3.1	Ensure DNS services are configured correctly (Automated)	☐	☐
3.2	Ensure intrusion prevention is enabled for untrusted interfaces (Automated)	☐	☐
3.3	Ensure packet fragments are restricted for untrusted interfaces (Automated)	☐	☐
3.4	Ensure non-default application inspection is configured correctly (Manual)	☐	☐
3.5	Ensure DOS protection is enabled for untrusted interfaces (Manual)	☐	☐
3.6	Ensure 'threat-detection statistics' is set to 'tcp-intercept' (Automated)	☐	☐
3.7	Ensure 'ip verify' is set to 'reverse-path' for untrusted interfaces (Automated)	☐	☐
3.8	Ensure 'security-level' is set to '0' for Internet-facing interface (Automated)	☐	☐
3.9	Ensure Botnet protection is enabled for untrusted interfaces (Automated)	☐	☐
3.10	Ensure ActiveX filtering is enabled (Automated)	☐	☐
3.11	Ensure Java applet filtering is enabled (Automated)	☐	☐
3.12	Ensure explicit deny in access lists is configured correctly (Automated)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Jan 15, 2021	4.2.0	Update control to align with Command History updates (Ticket 9381)
Jan 15, 2021	4.2.0	proposed reference link revision for this section (Ticket 9887)
Jan 15, 2021	4.2.0	Default Inspection application list (Ticket 8276)
Jan 15, 2021	4.2.0	Context is not clear (Ticket 8277)
Mar 3, 2021	4.2.0	The CIS check 1.4.5.. 1.4.5.3, 1.4.54 and 1.8.1 are applicabel ond Cisco ASA 8.x also (Ticket 6125)
Mar 3, 2021	4.2.0	Control "1.7.2 – Ensure 'TLS 1.0' is set for HTTPS access" has the incorrect remediation and audit steps (Ticket 5019)
Mar 3, 2021	4.2.0	Context is not clear (Ticket 8274)