the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Cisco Firewall

Version 2.2.0
December 30, 2010

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

Background.

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

No representations, warranties and covenants.

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

User agreements.

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

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

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

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

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

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

Grant of limited rights.

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

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

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

Retention of intellectual property rights; limitations on distribution.

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

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

Special rules.

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

Choice of law; jurisdiction; venue.

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

Table of Contents

Overview

This document, *Security Configuration Benchmark for Cisco Firewall Appliances*, provides prescriptive guidance for establishing a secure configuration posture for *Cisco Firewall Appliances* versions *7.1 – 8.2.3* This guide was tested against *Cisco ASA 8.2* as installed by ASA823-k8.bin To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

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

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

Intended Audience

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

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:

Author
Chris Jackson, *Cisco Systems, Inc., CCIE #6256 SEC & R&S, CISA, GSNA, GCIH, GCIA, GCFW, CISSP, MCSE*

Maintainers
Chris Jackson, *Cisco Systems, Inc., CCIE #6256 SEC & R&S, CISA, GSNA, GCIH, GCIA, GCFW, CISSP, MCSE*
Justin Opatrny

Editors
Steven Piliero, *Center for Internet Security*

Testers
Chris Jackson, *Cisco Systems, Inc., CCIE #6256 SEC & R&S, CISA, GSNA, GCIH, GCIA, GCFW, CISSP, MCSE*
Jeff Weekes, *Terra Verde, LLC*

Contributors and Reviewers
Ahmed Adel
Adam Baines
Blake Frantz, *Center for Internet Security*
Ashwin Kohli
Tim Muniz, *Tenable Network Security, Inc.*
Jason Nehrboss, *Computer Sciences Corporation*
Justin Opatrny
Jeff Weekes, *Terra Verde, LLC*

Typographic Conventions

The following typographical conventions are used throughout this guide:

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

Configuration Levels

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

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

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

Level-II Benchmark settings/actions

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

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

Scoring Status

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

Scorable

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

Not Scorable

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

1 Level-1 Benchmark Profile

Description:
This benchmark for Cisco firewall appliances represents a prudent level of minimum due care. These settings:

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

1.1 Management Plane Level 1

Description:
Services, settings and data streams related to setting up and examining the static configuration of the firewall, and the authentication and authorization of firewall administrators. Examples of management plane services include administrative device access (telnet, ssh, http, and https), SNMP, and security protocols like RADIUS and TACACS+.

1.1.1 Local Authentication, Authorization and Accounting (AAA) Rules

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

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

Description:
Verify authentication, authorization and accounting (AAA) method(s) configuration for enable mode authentication.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access to devices. Centralizing control provides a repository for access control rules and authentication privileges while maintaining accountability through logging of firewall device access and configuration commands enters at the user level. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. 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.

Platform(s):
ASA, FWSM, PIX

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

```
hostname(config)#aaa authentication enable console {server-tag [LOCAL] | LOCAL}
```

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

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

```
hostname#show run aaa authentication
```

Default Value:
The default value for `aaa` is disabled.

References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.1.2 Require AAA Authentication for Console and Other Interactive Management Protocols (Level 1, Scorable)

Description:
Verify configurations for management lines require login using the default authentication, authorization and accounting (AAA) method list.

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.

Platform(s):
ASA, FWSM, PIX

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

```
hostname(config)#aaa authentication {serial | telnet | ssh | http | secure-http-client) console {server-tag [LOCAL] | LOCAL}
```

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

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

```
hostname#show run aaa authentication
```

Default Value:
The default value for `aaa authentication` is disabled.

References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.1.3 Require Defined AAA Servers and Protocols (Level 1, Scorable)

Description:
Verify that authentication, authorization and accounting (AAA) configuration uses required servers and protocols.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure designated security protocol, server, key and timeout used for authenticating users.

```
hostname(config)#aaa-server {server-tag} protocol {
Kerberos | ldap | nt | radius | sdi |tacacs+ }

hostname(config)#aaa-server {server-tag} host {aaa_server-
ip} [key] [timeout seconds]
```

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

1. If the command does not return a result for each AAA server group, the feature is not enabled

```
hostname#show run aaa-server
```

Default Value:
The default value for `aaa-server` is disabled.

References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.1.4 Require AAA Command Authorization (Level 1, Scorable)

Description:
Verify that command authorization is preformed locally based on privilege level and/or through Tacacs+ for per command access control with local authorization for fallback.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. Requiring authorization for commands enforces segmentation of duties and provides least privilege access for specific job roles.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure AAA authorization for local commands entered through CLI, ASDM, or Enable mode. AAA authorization can be conducted against locally configured users with assigned privilege levels or Radius through user privilege levels assigned through attributes. The following commands enable command authorization for these configured authentication sources:

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

hostname(config)# aaa authorization command LOCAL
```

For local and Radius authorization there are 16 privilege levels that range from 0-15. Level 1 is the default level that a user is placed in when they authenticate to the FW. Level 15 is granted once the enable password has been verified. Through local command authorization each command level can be attributed to different roles, reducing the commands that they can enter to only those required preforming their job. A user can access any commands that are at or lower than their current privilege level. To set command privilege levels, the following commands are used to modify the default privilege levels for each command:

```
hostname(config)# privilege [show | clear | cmd] level level
[mode {enable | cmd}] command command
```

The following commands by default are at privilege level 0, all others are at level 15 (enable mode).

```
show checksum, show curpriv, enable, help, show history, login, logout,
pager, show pager, clear pager, quit, show version
```

Tacacs+ Authorization operates though validating each command entered against an approved list configured within the TACACS+ server. The command to enable TACACS+ with LOCAL database fallback is as follows and requires a preconfigured TACACS+ server_group to send command authorization to:

```
hostname(config)# aaa authorization command
tacacs+_server_group [LOCAL]
```

For detailed configuration instructions, refer to the Cisco ASA 8.2 configuration guide.

Audit:
Perform the following to determine if AAA authorization is configured:

1. If the command does not return a result for each AAA server group, the feature is not enabled.

```
hostname#show run aaa authorization
```

2. Review the custom privilege level by user role to ensure that commands are mapped appropriately.

```
!--- List ALL commands
hostname(config)# show running-config all privilege all

!--- List ALL commands at a privilege level
hostname(config)# show running-config privilege level level

!--- List ALL commands at a privilege level
hostname(config)# show running-config privilege command
command
```

Default Value:
The default value for `aaa authorization` is disabled.

References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.1.5 Require AAA Accounting (Level 1, Scorable)

Description:
Verify that authentication, authorization and accounting (AAA) configuration uses required servers and protocols.

Rationale:
Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. AAA Accounting provides a management and audit trail for user and administrative sessions through RADIUS and TACACS+. If TACACS+ is used all commands entered by users and administrators of the firewall are logged.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure the firewall to implement AAA accounting for user access through RADIUS or TACACS+.

```
hostname(config)# aaa accounting {serial | telnet | ssh |
enable} console server-tag
```

Command accounting can be configured through Tacacs+ through the following command:

```
hostname(config)# aaa accounting command [privilege level]
server-tag
```

Audit:
Perform the following to determine if AAA accounting is enabled:

1. If the command does not return a result for AAA accounting, the feature is not enabled.

```
hostname#show run aaa accounting
```

Default Value:
The default value for `aaa accounting` is disabled.

References:
1. NSA Router Security Configuration Guide
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.2 Access Rules

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

1.1.2.1 Require Local Password (Level 1, Scorable)

Description:
Verify a local login password is configured to restrict access to the device via Telnet or SSH.

Rationale:
Default device configuration does not require any strong user authentication enabling unfettered access to an attacker that can reach the device. Requiring a unique local login password protects user EXEC mode. A user can enter the default password and just press the Enter key at the Password prompt to login to the device. The passwd command 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.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure a strong login password.

```
hostname(config)#{passwd | password} {login_password}
encrypted
```

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

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

```
hostname#show run passwd
```

Default Value:
The default value for `passwd` is cisco.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.2.2 Require ASDM Management Access Control (Level 1, Scorable)

Description:
Verify the device configuration restricts remote management access via HTTPS for adaptive security device manager (ASDM) to authorized management subnets only.

Rationale:
Configuring access control to restrict remote administration to those network address ranges authorized to manage the device prevents unauthorized parts of the network from

accessing the system. Web-based, remote administration access should be restricted to authorized management systems to minimize the devices attack surface and avoid potential compromise. A valid and unique certificate should also be assigned to the FW instead of the self-signed certificate, which is installed by default, to provide device authentication. In addition, Web access should not be enabled on any public facing network connection. If remote management is necessary across the internet a VPN session should be required to the FW.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure remote administration access restrictions for HTTPS and ASDM.

```
hostname(config)#http {ip_address subnet_mask
interface_name}
```

Audit:
Perform the following to determine if ASDM access control is enabled:

1. If the command does not return a result, the feature is not enabled. Verify that only management subnets are allowed access to ASDM, and that no public facing network is allowed access to the ASDM.

```
hostname#show run http
```

Default Value:
No default value.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.2.3 Require SSHv2 for Remote Management Access (Level 1, Scorable)

Description:
Verify that SSHv2 is the only protocol allowed for remote management access to the device.

Rationale:
SSHv2 uses RSA public key cryptography to establish a secure connection between a client and a server. Because connections are encrypted, passwords and other sensitive information are not exposed in clear text between the administrator's host and the device. SSHv2 also prevents session hijacking and many other kinds of network attacks. SSHv2 should be employed to replace Telnet where available.

Platform(s):
ASA, PIX, FWSM

Remediation:

Disable remote administration access via Telnet for all hosts and enable SSHv2.

```
hostname(config)#no telnet {hostname | ip_address mask
interface_name}
hostname(config)#ssh {ip_address mask} interface
hostname(config)#ssh version 2
```

Audit:
Perform the following to determine if telnet is disabled and SSHv2 is enabled:

1. If the command does not return a result, the feature is not enabled. Verify that only management subnets are allowed access to ASDM

```
hostname#show run telnet
hostname#show run ssh
```

Default Value:
Neither SSH nor Telnet access are enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

Description:
Verify device is configured to automatically disconnect sessions after a fixed idle time.
Rationale:
This prevents unauthorized users from misusing abandoned sessions. Example, if the administrator goes on vacation and leaves an enabled login session active on his desktop system. There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Check your local policies and operational needs to determine the best value. In most cases, this should be no more than 10 minutes.
Platform(s):
ASA, FWSM, PIX
Remediation:
Configure device timeout 10 minutes) to disconnect sessions after a fixed idle time.

```
hostname(config)#console timeout {minutes}
hostname(config)#ssh timeout {minutes}
```

Audit:
Perform the following to determine if session timeout is no longer than 10 minutes:

1. Verify appropriate timeout values for management access

```
hostname#show run console timeout
```

```
hostname#show run ssh timeout
```

Default Value:
SSH timeout is 5 minutes by default and console timeout is disabled.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.2.5 Require SSH Access Control (Level 1, Scorable)

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

Rationale:
Configuring access control to restrict remote administration to those network address ranges authorized to manage the device prevents unauthorized parts of the network from accessing the system.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure remote management restrictions for SSH.

```
hostname(config)#ssh {ip_address mask} interface
```

Audit:
Perform the following to determine if SSH management access controls are configured:

1. If the command does not return a result, the feature is not enabled. Verify that only management subnets are allowed access to SSH.

```
hostname#show run ssh
```

Default Value:
SSH access is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.3 Banner Rules

Description:
Rules in the banner class communicate legal rights to users.

1.1.3.1 Require EXEC Banner (Level 1, Scorable)

Description:
Verify an authorized EXEC banner is defined.

Rationale:
Presentation of an EXEC banner occurs before displaying the enable prompt, after starting an EXEC process, normally after displaying the message of the day and login banners and after the user logs into the device. "Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language).

Platform(s):
ASA, FWSM, PIX

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

```
hostname(config)#banner {exec banner-text}
```

Audit:
Perform the following to determine if an EXEC banner is configured:

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

```
hostname#show run banner exec
```

Default Value:
An EXEC banner is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.3.2 Require Login Banner (Level 1, Scorable)

Description:
Verify an authorized login banner is defined.

Rationale:
Presentation of a login banner, to a user attempting to access the device, occurs before the display of login prompts and usually appears after the message of the day banner. "Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language).

Platform(s):
ASA, FWSM, PIX

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

```
hostname(config)#banner {login banner-text}
```

Audit:
Perform the following to determine if a login banner is configured:

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

```
hostname#show run banner login
```

Default Value:
A login banner is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.3.3 Require MOTD Banner (Level 1, Scorable)

Description:

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

Rationale:
Presentation of a MOTD banner occurs when a user first connects to the device, normally before displaying the login banner and login prompts. "Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language).

Platform(s):
ASA, FWSM, PIX

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

```
hostname(config)#banner {motd banner-text}
```

Audit:
Perform the following to determine if a MOTD banner is configured:

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

```
hostname#show run banner motd
```

Default Value:
A MOTD banner is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.3.4 Require ASDM Banner (Level 1, Scorable)

Description:
Verify an authorized ASDM banner is defined.

Rationale:
Presentation of an ASDM banner occurs after a user logins in to the ASDM. "Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language).

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure the ASDM banner presented when a user authenticates to the device for web administration.

```
hostname(config)#banner {ASDM banner-text}
```

Audit:
Perform the following to determine if an ASDM banner is configured:

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

```
hostname#show run banner asdm
```

Default Value:
An ASDM banner is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.4 Password Rules

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

1.1.4.1 Require Local User and Encrypted Password (Level 1, Scorable)

Description:

Verify at least one local user exists with a defined 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 for configuration in a named method list in case centralized authentication, authorization and accounting services are unavailable.

Platform(s):
ASA, FWSM, PIX

Remediation:
Create a local user with strong password.

```
hostname(config)#username {local_username} password
{local_password} encrypted
```

Audit:
Perform the following to determine if a local user account is configured for fallback authentication:

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

```
hostname#show run username
```

Default Value:
A local user is not configured by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.4.2 Require Enable Password (Level 1, Scorable)

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

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

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure a strong, enable secret password.

```
hostname(config)#enable password {enable_password}
encrypted
```

Audit:
Perform the following to determine if an enable password is configured:

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

```
hostname#show run enable
```

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

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.5 SNMP Rules

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

1.1.5.1 Forbid SNMP Read Access (Level 1, Scorable)

Description:
Verify simple network management protocol (SNMP) read access to the device is disabled.

Rationale:
SNMP read access allows remote monitoring and management of the device. Older version of the protocol, such as SNMP versions 1 and 2, do not use any encryption to protect community strings (passwords). SNMP should be disabled unless you absolutely require it for network management purposes. If you require SNMP, be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the device (e.g. enable password, line password, etc.) or other authentication credentials. Consider utilizing SNMPv3, which utilizes authentication and data privatization (encryption), when available. SNMP versions 1 and 2 use clear-text community strings, which are considered a weak security implementation.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable SNMP read access to the device.

```
hostname(config)#clear configure snmp-server
```

```
hostname(config)#no snmp-server host  (PIX 6.x)
```

Audit:
Perform the following to determine if SNMP is configured:

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

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

Default Value:
SNMP is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.5.2 Forbid SNMP Traps (Level 1, Scorable)

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

Rationale:
SNMP should be disabled unless you absolutely require them for network management purposes.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable SNMP traps.

```
hostname (config)#no snmp-server enable traps {all}
```

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

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

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

Default Value:
SNMP is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.5.3 Require SNMP Trap Server When SNMP is Used (Level 1, Scorable)

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

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

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure authorized SNMP trap community string and restrict sending messages to authorized management systems. The community string should be unique from all other device credentials.

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

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

Audit:
Perform the following to determine if SNMP is configured:

1. If the command returns configuration values, then SNMP is enabled. Verify that SNMP is configured to send traps to authorized management systems or subnets only.

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

Default Value:
SNMP is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.1.5.4 Require Authorized Read SNMP Community Strings and Access Control (Level 1, Scorable)

Description:
Verify an authorized community string and access control is configured to restrict read access to the device.

Rationale:

SNMP read access should be restricted to authorized management systems, in a restricted zone, using a community string unique to the managing organization to prevent unauthorized device access. If an attacker is able to easily guess or obtain the community string and can access the device then they can potentially gain sensitive device information using SNMP.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure authorized SNMP read community string and restrict access to authorized management systems. The community string should be unique from all other device credentials.

```
hostname(config)#snmp-server community {community_ string}

hostname(config)#snmp-server host {interface_name
ip_address poll} community {read_community_string}
```

Audit:
Perform the following to determine if SNMP is configured with access control:

1. If the command returns configuration values, then SNMP is enabled. Verify that SNMP is configured to send traps to authorized management systems or subnets only.

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

Default Value:
SNMP is not enabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2 Control Plane Level 1

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

1.2.1 Clock Rules

Description:

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

1.2.1.1 Require Clock Time Zone - UTC (Level 1, Scorable)

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

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

Platform(s):
ASA, PIX

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

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

Audit:
Perform the following to determine if UTC is configured:

1. The following command will show if a time zone is configured other than UTC. If no result is returned, UTC is in use.

```
hostname#show run clock
```

Default Value:
UTC is configured by default as the timezone.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

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

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

Platform(s):
ASA, PIX

Remediation:
Disable clock daylight savings time adjustments.

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

Audit:
Perform the following to determine if daylight savings time is configured:

1. The following command will show if daylight savings time is configured. If no result is returned, UTC is in use.

```
hostname#show run clock
```

Default Value:
Daylight savings time is disabled and UTC is configured by default as the timezone.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

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

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

Platform(s):
ASA, PIX

Remediation:
Enable clock summer-time and configure local time-zone.

```
hostname# clock timezone zone [-]hours [minutes]

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

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

Audit:
Perform the following to determine if daylight savings time is configured:

1. The following command will show if daylight savings time is configured. If no result is returned, UTC is in use.

```
hostname#show run clock
```

Default Value:
Daylight savings time is disabled and UTC is configured by default as the time zone.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.2 Global Service Rules

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

1.2.2.1 Forbid DHCP Server Service (Level 1, Scorable)

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

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

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable DHCPD server service and clear all commands, bindings and statistics.

```
hostname(config)#clear configure dhcpd

hostname(config)#no dhcpd enable {interface} (used for
older software revisions)
```

Audit:
Perform the following to determine if DHCP server is configured:

1. The following command will show if the DHCP server is configured. If no result is returned, DHCP server is disabled.

```
hostname#show run dhcpd
```

Default Value:
DHCP server is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.2.2 Forbid ASDM Service If Not Used (Level 1, Scorable)

Description:
Verify the ASDM server service on the device is disabled.

Rationale:
Web-based, remote administration should be disabled if not required to minimize the attack surface of the device. At a minimum, ASDM access should be restricted to authorized management systems.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable the ASDM server service.

```
hostname(config)#no http server enable [port]
```

Audit:
Perform the following to determine if ASDM server is configured:

1. The following command will show if the ASDM server is configured. If no result is returned, web management is disabled.

```
hostname#show run http
```

Default Value:
ASDM management is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3 Logging Rules

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

1.2.3.1 Forbid Console Logging (Level 1, Scorable)

Description:
Verify console logging is disabled.

Rationale:
Console logging is not persistent. If excessive log messages are generated to the console it could potentially render the device unmanageable. Console logging should be disabled unless required for immediate troubleshooting. If enabled then care should be taken to select a severity level that will not adversely affect system resources.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable logging to the console.

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

Audit:
Perform the following to determine if console logging is configured:

1. The following command will show if console logging is configured.

```
hostname#show run logging
```

Default Value:
Console logging is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3.2 Require Console Logging Severity Level if required by policy (Level 1, Scorable)

Description:
If console logging is required by security policy it should be limited to a rational severity level to avoid affecting system performance and management.

Rationale:
This configuration determines the severity of messages that will generate console messages. Logging to console should be limited only to those messages required for immediate troubleshooting while logged into the device. This form of logging is not persistent; the device does not store messages printed to the console. Console logging is helpful for operators when using the console, but is otherwise of little value since they are not persistent.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure console logging level.

```
hostname(config)#logging console {2 | critical}
```

Audit:
Perform the following to determine if console logging is configured:

1. The following command will show if console logging is configured.

```
hostname#show run logging
```

Default Value:
Console logging is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3.3 Require Logging Facility (Level 1, Scorable)

Description:
Verify the required syslog facility is configured and submitted when sending logging messages to a remote syslog server.

Rationale:
Syslog servers file messages based on the facility number in the message. Logs should be directed to a consistent and expected logging facility to ensure proper processing and storage by the remote system.

Platform(s):
ASA, FWSM, PIX

Remediation:

```
hostname (config)#logging facility {20}
```

References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.2.3.4 Require Logging History Level (Level 1, Scorable)

Description:
Ensure that syslog messages sent to the history table and to an SNMP network management station are limited based on severity.

Rationale:

This determines the severity of messages that will generate simple network management protocol (SNMP) trap and or syslog messages. This setting should be set to either "informational" (6) or "notification" (5), but no lower to ensure receipt of sufficient information concerning the devices operational status.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure logging history level.

```
hostname(config)#logging history {5 | notification}
```

Audit:
Perform the following to determine if console logging is configured:

1. The following command will show if console logging is configured.

```
hostname#show run logging
```

Default Value:
Console logging is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

Description:
Verify the device is configured to submit system logs to one or more syslog servers to centrally record system events.

Rationale:
Cisco devices can send their log messages to a Unix-style syslog service. A syslog service simply accepts messages, and stores them in files or prints them according to a simple configuration file. This form of logging is best because it can provide protected long-term storage for logs (the devices internal logging buffer has limited capacity to store events.) Additionally, most security regulations require or highly recommend device logging to an external system. The Syslog server should be a protected repository and as such should be under the organizations administrative control.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure one or more internal and protected syslog servers by IP address.

```
hostname(config)#logging host {interface_name
syslog_server_ip}
```

Audit:
Perform the following to determine if syslog logging is configured:

1. The following command will show if syslog logging is configured.

```
hostname#show run logging
```

Default Value:
Syslog logging is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

Description:
Verify simple network management protocol (SNMP) trap and syslog are set to required severity level.

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

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure logging trap level.

```
hostname(config)#logging trap {6 | informational}
```

Audit:
Perform the following to determine if syslog and SNMP logging level is configured:

1. The following command will show if syslog logging level is configured.

```
hostname#show run logging
```

Default Value:
Logging trap level is not configured by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2

2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3.7 Require System Logging (Level 1, Scorable)

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

Rationale:
Logging should be enabled to allow monitoring of both operational and security related events. Logs are critical for responding to general as well as security incidents. Additionally, most security regulations require or highly recommend device logging.

Platform(s):
ASA, FWSM, PIX

Remediation:
Enable system logging.

```
hostname(config)#logging enable  (logging on for PIX 6.x)
```

Audit:
Perform the following to determine if logging is configured:

1. The following command will show if logging is configured.

```
hostname#show run logging
```

Default Value:
Logging is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3.8 Require Timestamps in Log Messages (Level 1, Scorable)

Description:
Verify timestamps are included in log messages.

Rationale:
Including timestamps in log messages reduces the complexity of correlating events and tracing network attacks across multiple devices. Enabling timestamps, to mark the generation time of log messages, simplifies obtaining a holistic view of events enabling faster troubleshooting of issues or attacks.

Platform(s):
ASA, FWSM, PIX

Remediation:

Enable inclusion of timestamps in system logs.

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

Audit:
Perform the following to determine if logging timestamps are configured:

1. The following command will show if logging time stamps are configured.

```
hostname#show run logging
```

Default Value:
Logging timestamps are disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.3.9 Require NetFlow Secure Event Logging (Level 1, Scorable)

Description:
Configure NetFlow Secure Event Logging to monitor traffic flow through the firewall.

Rationale:
Support was added in ASA 8.1 and up for Netflow event logging, which provides greater visibility into traffic flow passing through the firewall that can enable the identification of unusual network communication, which may be indicative of a previously unknown attack vector. NSEL is not like typical NetFlow in that it does not provide real-time statistics on traffic flow, and is more concerned with delivering specific traffic events that were traditionally only available through syslog. ASA 8.2 supports NetFlow v9 and will report on flows created, denied by ACL, and flow teardown. Configuration is preformed thorough the modular policy framework and can be configured to report on all traffic or specific networks/interfaces.

Platform(s):
ASA

Remediation:
Enable NSEL logging.

```
hostname(config)# flow-export destination interface-name
ipv4-address|hostname udp-port
hostname(config)# flow-export template timeout-rate minutes
hostname(config)# flow-export delay flow-create seconds
hostname(config)# access-list flow_export_acl permit ip
source  destination
hostname(config)# class-map flow_export_class
hostname(config-cmap)# match access-list flow_export_acl
hostname(config)# policy-map flow_export_policy
```

```
hostname(config-pmap)# class flow_export_class
hostname(config-pmap-c)# flow-export event-type event-type
destination
hostname(config)#service-policy flow_export_policy global
```

Audit:
Perform the following to determine if NSEL is configured:

1. The following command will show if logging time stamps are configured.

```
hostname#show run flow-export
```

Default Value:
NSEL is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.4 NTP Rules

Description:
Rules in the network time protocol (NTP) class enforce synchronization of the devices clock to trusted, authoritative timer sources.

1.2.4.1 Require Primary NTP Server (Level 1, Scorable)

Description:
Verify configuration of a primary, trusted network protocol (NTP) timeserver used to synchronize the device clock.

Rationale:
Network time protocol (NTP) enables devices to maintain accurate time when synchronized to a trusted and reliable timeserver. Synchronizing system time to a centralized and trusted time source enables reliable correlation of events based on the actual sequence they occurred. The ability to accurately, determine the time and sequence events occur in increases confidence in event data. Accurate system time and events facilitate efficient troubleshooting and incident response. Additional time sources increase the accuracy and dependability of system time.

Platform(s):
ASA, PIX

Note:
FWSM receives its clock information from the Supervisor module of the switch it is installed in and NTP cannot be configured on the module itself. NTP should be configured on the Supervisor module to allow synchronized time for logging.

Remediation:

Designate a primary, trusted NTP timeserver.

```
hostname(config)#ntp server {ntp-server_ip_address}
[prefer]
```

Audit:
Perform the following to determine if ntp is configured:

1. The following command will show if ntp is configured.

```
hostname#show run ntp
```

Default Value:
NTP is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.2.4.2 Require NTP Authentication (Level 1, Scorable)

Description:
Verify the device is configured to use authenticated NTP messages with peers.

Rationale:
Accurate timestamps are critical for troubleshooting issues and forensic analysis. NTP authentication, using md5 encryption, reduces the chance that an attacker can spoof the devices trusted timeserver and alter its system clock. Network time protocol (NTP) enables devices to maintain accurate time when synchronized to a trusted and reliable timeserver. Synchronizing system time to a centralized and trusted time source enables reliable correlation of events based on the actual sequence they occurred. The ability to accurately, determine the time and sequence events occur in increases confidence in event data. Accurate system time and events facilitate efficient troubleshooting and incident response. Additional time sources increase the accuracy and dependability of system time.

Platform(s):
ASA, PIX, FWSM

Remediation:
Enable authentication with an NTP server, set an encrypted authentication key

```
hostname(config)#ntp authenticate
hostname(config)#ntp trusted-key {ntp_key_id}
hostname(config)#ntp authentication-key {ntp_key_id} md5
{ntp_key}
hostname(config)#ntp server {ntp-server_ip_address}{key
ntp_key_id} [source interface_name] [prefer]
```

Audit:

Perform the following to determine if ntp authentication is configured:

1. The following command will show if ntp authentication is configured.

```
hostname#show run ntp
```

Default Value:
NTP authentication is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3 Data Plane Level 1

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

1.3.1 Attack Guards

Description:
Attack Guard configuration settings minimize network attacks by auditing, blocking or limiting traffic thru the device.

1.3.1.1 Require OS Version (Level 1, Scorable)

Description:
Verify the device is running an authorized OS version.

Rationale:
Devices should be configured with a standard OS image and version to enable consistent and effective management as well as improve security. Example, if security guidance or advisories are released affecting the device then it would be easier to address or mitigate if all devices are running the same OS.

Platform(s):
ASA, FWSM, PIX

Remediation:
Upgrade the system software.

Audit:
Perform the following to determine software version:

1. Verify the OS version is authorized and has no vulnerabilities

```
hostname#show ver | include Version
```

Default Value:
Not applicable.

References:
1. Cisco Security Advisories and PSIRT Notices
2. ASA 5500 Series Configuration Guide using the CLI 8.2
3. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.1.2 Require Connection Timeout (Level 1, Scorable)

Description:
Verify timers are set so that the device closes connections after they become idle, to minimize impact to memory and resources available for new connections.

Rationale:
The timeout command sets the idle time for connection slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. This reduces the risk of someone from accessing an already established but idle connection.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure the connection and translation slot timeouts.

```
hostname(config)#timeout conn {00:30:00}
```

Audit:
Perform the following to determine if timeout value are set to appropriate levels:

1. The following command will show configured timeout values.

```
hostname#show run  inc timeout conn
```

Default Value:
Connection timeout default is 1 hour.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.1.3 Require Translation Slot Timeout (Level 1, Scorable)

Description:
Verify timers are set so that the device closes connections after they become idle, to minimize impact to memory and resources available for new connections.

Rationale:

The xlate time is the duration the device will hold an idle translation connection open before closing it down. Short values are more secure, but may be more disruptive to users. The xlate timeout must be no longer than the translation timeout.

Platform(s):
ASA, FWSM, PIX

Remediation:

```
hostname (config)#timeout xlate {01:00:00}
```

Audit:
Perform the following to determine if timeout value are set to appropriate levels:

1. The following command will show configured timeout values.

```
hostname#show run | inc timeout xlate
```

Default Value:
Xlate timeout default is 3 hours.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.1.4 Require Intrusion Detection Actions (Level 1, Scorable)

Description:
Verify required intrusion detection system (IDS) audit policies are configured.

Rationale:
When intrusion detection is enabled, the device can detect unusual activity using informational and attack signatures. Informational signatures identify activity that can be useful for forensics but are not necessarily malicious. Attack signatures identify activity that is or leads to exploitation. Once a signature is triggered, the device can perform a specified action based on rules. When packets match a signature, the device can take the following actions; alarm generating a system message, drop the packet(s), or reset which drops the packet(s) and closes the connection.

Platform(s):
ASA, PIX

Remediation:

```
hostname(config)#ip audit attack {action
{alarm}{drop}{reset}}

hostname(config)#ip audit info {action
{alarm}{drop}{reset}}
```

Audit:
Perform the following to determine IDS configuration parameters:

1. The following commands will show IDS configuration values.

```
hostname#show run ip audit attack

hostname#show run ip audit info
```

Default Value:
IDS inspection is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.1.6 Require Fragment Chain Fragmentation Checks (Level 1, Scorable)

Description:
Verify the device is configured to prevent fragmented packets on external or high-risk interfaces.

Rationale:
By default, the device accepts up to 24 packet fragments to reconstruct a full IP packet. Disabling fragmentation minimizes the amount of resources the device consumes attempting to reassemble fragmented packets. An attacker could potentially submit a large number of packet fragments to cause a fragmentation denial-of-service (DoS) attack.

Platform(s):
ASA, FWSM, PIX

Remediation:
Disable fragment reassembly on all external or high risk interfaces.

```
hostname (config)#fragment chain 1 {interface_name}
```

Audit:
Perform the following to determine fragment protection parameters are configured on high-risk interfaces:

1. The following command will show fragment chain values.

```
hostname#show run fragment
```

Default Value:
Default Fragment Chain value is 24.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2

2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.1.7 Require Protocol Inspection (Level 1, Scorable)

Description:
Verify traffic inspection is enabled for commonly attacked protocols.

Rationale:
Protocol inspection ensures that only legitimate requests are permitted and protects against specific attacks and other threats that may be associated with the configured protocol. Traffic inspection is performed on for all traffic matching, both inbound and outbound, matching the enabled protocol(s). Changes to the default port associated with a particular protocol can be made if required.

Platform(s):
FWSM, PIX

Remediation:
Configure fixup traffic inspection for commonly attacked protocols; HTTP, HTTP and ESMTP.

```
hostname (config)#fixup protocol {protocol} [port]
```

Platform(s):
ASA

Remediation:
Configure traffic inspection for commonly attacked protocols HTTP, HTTP and SMTP.

```
hostname (config)#inspect {ftp | http| esmtp} [map_name]
```

Default Value:
Not defined

References:
1. Cisco Security Appliance Command Reference, Version 7.2
2. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.3.1.8 Require Object Groups to Simplify Access Control Entries (Level 1, Scorable)

Description:
Verify the device is configured to utilize object groups to simplify security policy rules.

Rationale:
Object groups can greatly simplify policy enforcement through access control lists, by grouping services, networks, protocols, and ICMP type's into reusable components for access control entries. In addition, the use of object groups with access control entries makes firewall rules easier to troubleshoot and audit.

Platform(s):

ASA, FWSM, PIX

Remediation:
Configure object groups for access control entries.

```
!--- Protocol Objects
hostname (config)# object-group protocol obj_grp_id
hostname (config-protocol)# description text
hostname (config-protocol)# protocol-object protocol

!--- Network Object
hostname (config)# object-group network obj_grp_id
hostname (config-protocol)# description text
hostname (config-protocol)# network-object network {host
ip_address | ip_address mask}

!--- Service Object
hostname (config)# object-group service grp_id {tcp | udp |
tcp-udp}
hostname (config-service)# description text
hostname (config-service)# port-object {eq port | range
begin_port end_port}

!--- ICMP Object
hostname (config)# object-group icmp-type grp_id
hostname (config-service)# description text
hostname (config-service)# icmp-object icmp-type
```

Audit:
Perform the following to determine if object groups are configured:

1. The following command will show all object groups configured on the firewall.

```
hostname#show run object-group
```

Default Value:
Object groups are not used by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

1.3.2 Border Device Filtering

Description:
A border-filtering device connects "internal" networks such as desktop networks, DMZ networks, etc., to "external" networks such as the Internet. If this group is chosen, then

ingress and egress filter rules will be required. "Building Internet Firewalls" by Zwicky, Cooper and Chapman, O'Reilly and Associates.

1.3.2.1 Forbid External Source Addresses on Outbound Traffic (Level 1, Scorable)

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

Rationale:
You can prevent users from spoofing other networks by ensuring that any outbound traffic from your network uses only source IP addresses that are in your organization's IP addresses range. Your ISP can also implement this type of filtering, which is collectively referred to as RFC 2827 filtering. This filtering denies any traffic that does not have the source address that was expected on a particular interface.

Platform(s):
ASA, FWSM, PIX

Remediation:

```
hostname(config)#access-list {access-list} permit ip
{internal_networks} any

hostname(config)#access-group {access-list} in interface
{interface}
```

Audit:
Perform the following to inspect anti-spoofing access lists:

1. The following command will display the access lists configured.

```
hostname#show run access-list
hostname#show run access-group
```

Default Value:
Not defined

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0
3. RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

1.3.2.2 Forbid Private Source Addresses from External Networks (Level 1, Scorable)

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

Rationale:

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

Platform(s):
ASA, FWSM, PIX

Remediation:

```
hostname(config)#access-list {access-list} deny ip
{internal_networks} any log
hostname(config)#access-list {access-list} deny ip
127.0.0.0 255.0.0.0 any log
hostname(config)#access-list {access-list} deny ip 10.0.0.0
255.0.0.0 any log
hostname(config)#access-list {access-list} deny ip 0.0.0.0
255.0.0.0 any log
hostname(config)#access-list {access-list} deny ip
172.16.0.0 255.240.0.0 any log
hostname(config)#access-list {access-list} deny ip
192.168.0.0 255.255.0.0 any log
hostname(config)#access-list {access-list} deny ip
192.0.2.0 255.255.255.0 any log
hostname(config)#access-list {access-list} deny ip
169.254.0.0 255.255.0.0 any log
hostname(config)#access-list {access-list} deny ip
224.0.0.0 224.0.0.0 any log
hostname(config)#access-list {access-list} deny ip host
255.255.255.255 any log
hostname(config)#access-group {access-list} in interface
{interface}
```

Audit:
Perform the following to inspect anti-spoofing access lists:

1. The following command will display the access lists configured.

```
hostname#show run access-list
hostname#show run access-group
```

Default Value:
Not defined

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

3. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
4. NSA Router Security Configuration Guide
5. Cisco Guide to Harden Cisco IOS Devices
6. RFC 3704 - Ingress Filtering for Multi-homed Networks (Updates RFC 2827)
7. RFC 3300 - Special-Use IPv4 Addresses
8. RFC 3171 - IANA Guidelines for IPv4 Multicast Address Assignments
9. RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
10. RFC 1918 - Address Allocation for Private Internets

1.3.2.3 Forbid Inbound Traceroute Messages (Level 1, Scorable)

Description:
Verify traceroute packets are not allowed to enter the network.

Rationale:
Attackers can use traceroute to map your network. At each router, traceroute returns a packet that indicates the route the packet is taking through the network to get to its destination. If you allow traceroute messages to enter your network, an attacker can map your network to help plan attacks. Thus, you should prevent traceroute messages from entering the network at edge routers.

Platform(s):
ASA, FWSM, PIX

Remediation:
hostname(config)#deny udp any any range 33434 33534 log

```
hostname(config)#access-group {access_list} {in} interface
{interface_name}
```

Audit:
Perform the following to inspect access lists:

1. The following command will display the access lists configured.

```
hostname#show run access-list
hostname#show run access-group
```

Default Value:
Not defined

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0
3. NSA Router Security Configuration Guide

1.3.2.4 Require Explicit Deny Any in ACLs (Level 1, Scorable)

Description:
Verify device ACLs include an explicit deny ip any any entry at the end of the ACL.

Rationale:
Configuring an explicit deny entry, with log option, at the end of access control lists enables monitoring and troubleshooting traffic flows that are have been denied. Logging these events can provide an effective record to troubleshoot issues and attacks.

Platform(s):
ASA, FWSM, PIX

Remediation:

```
hostname(config)#deny ip any any log
hostname(config)#access-group <acl-id> <dir> interface
<if_name>
```

Audit:
Perform the following to inspect access lists:

1. The following command will display the access lists configured.

```
hostname#show run access-list
hostname#show run access-group
```

Default Value:
Not defined

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0
3. NSA Router Security Configuration Guide

1.3.3 Routing Rules

Description:
Unneeded services should be disabled.

1.3.3.1 Require Unicast Reverse-Path Forwarding (Level 1, Scorable)

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

Rationale:
Verifying the source address of IP traffic against routing rules reduces the possibility that an attacker can spoof the source of an attack. A number of attacks methods rely on

falsifying the traffic source to create a denial-of-service (DoS) or make it harder to trace the source of an attack. When enabled, the device checks the source address of the packet against the interface through which the packet arrived. Packets are dropped if the device determines, by verifying routing tables, there is no feasible path through the interface for the source address. Enabling reverse-path verification in environments with asymmetric routes can adversely affect network traffic.

Platform(s):
ASA, FWSM, PIX

Remediation:
Configure reverse-path verification on all device interfaces.

```
hostname(config)#interface {interface_name}
hostname(config-if)#ip verify reverse-path interface
{interface_name}
```

Audit:
Perform the following to inspect anti-spoofing interface features:

1. The following command shows all interfaces configured to verify reverse-path.

```
hostname#show run ip verify reverse-path
```

Default Value:
Not defined

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0
3. NSA Router Security Configuration Guide
4. RFC 2267 - Network Ingress Filtering

2 Level-2 Benchmark Profile

2.1 Data Plane Level 2

2.1.1 Neighbor Authentication

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

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

Rationale:

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

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

Remediation:
Configure EIGRP neighbor authentication where feasible.

```
hostname(config)#interface <interface_name>
hostname(config-if)# authentication mode eigrp as-num md5
hostname(config-if)# authentication key eigrp as-num key
key-id key-id
```

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

1. Verify that authentication and md5 password are set on the appropriate interface(s)

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

Default Value:
EIGRP authentication is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

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

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

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

Remediation:
Configure OSPF neighbor authentication where feasible.

```
hostname(config)#router ospf <ospf_process-id>

hostname(config-router)#area area-id authentication
message-digest

hostname(config)#interface <interface_name>

hostname(config-if)#ospf authentication [message-digest |
null]

hostname(config-if)# ospf message-digest-key key_id md5 key
```

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

1. Verify message digest for OSPF areas are defined.

```
hostname#sh run router ospf
```

2. Verify the appropriate md5 key and authentication is defined on the appropriate interface(s).

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

Default Value:
OSPF authentication is disabled by default.

References:

1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

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

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

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

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

Remediation:
Configure RIPv2 neighbor authentication where feasible.

```
hostname(config)#interface <interface_name>
hostname(config-if)# rip authentication mode {text | md5}
hostname(config-if)# rip authentication key key key-id key-
id
```

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

1. Verify that authentication and md5 password are set on the appropriate interface(s)

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

Default Value:
RIPv2 authentication is disabled by default.

References:
1. ASA 5500 Series Configuration Guide using the CLI 8.2
2. CIS Cisco ASA, FWSM, and PIX Benchmark v2.0.0

Appendix A: Prerequisites for Configuring SSH

Prior to configuring SSH access, perform the following prerequisite tasks:

1. Configure the device hostname

```
hostname(config)#hostname { device_hostname }
```

2. Configure the device domain name.

```
hostname(config)#domain-name { domain-name }
```

3. Generate an RSA key pair, which is required for SSH access.

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

4. Save the RSA key pair to persistent Flash memory

```
hostname(config)#write mem
```

Appendix B: References

1. National Security Agency (2009). *NSA Router Security Configuration Guide*. Available: http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf. Last accessed November 9, 2010.
2. United States Department of Justice (2009). *US Department of Justice – Cybercrime – Appendix A - Sample Network Login Banner*. Available: http://www.cybercrime.gov/ssmanual/06ssma.html#AppA. Last accessed November 9, 2010.
3. Cisco Systems, Inc (2010). *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2*. Avaialble: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/config.html. Last accessed November 9, 2010.
4. Cisco Systems, Inc. *Cisco Guide to Harden Cisco IOS Devices*. Available: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a008080120f48.shtml. Last accessed 31 December 2010.
5. Cisco Systems, Inc. *Cisco Security Advisories and PSIRT Notices*. Available: http://www.cisco.com/en/US/products/products_security_advisories_listing.html. Last accessed 31 December 2010.
6. Cisco Systems, Inc. Cisco Security Appliance Command Reference, Version 7.2. Available: http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/crt_72.pdf. Last accessed 31 December 2010.
7. Center for Internet Security (2009). *Cisco Firewall Benchmark v2.0.0*. Available: http://community.cisecurity.org/download/. Last accessed 31 December 2010.
8. Internet Engineering Task Force (1996). *RFC 1918 – Address Allocation for Private Internets*. Accessible: http://www.ietf.org/rfc/rfc1918.txt. Last accessed 31 December 2010.
9. Internet Engineering Task Force (2000). *RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.* Accessible: http://www.ietf.org/rfc/rfc2827.txt. Last accessed 31 December 2010.
10. Internet Engineering Task Force (2001). *RFC 3171 – IANA Guidelines for IPv4 Multicast Address Assignments*. Accessible: http://www.ietf.org/rfc/rfc3171.txt. Last accessed 31 December 2010.
11. Internet Engineering Task Force (2002). *RFC 3300 – Internet Official Protocol Standards*. Accessible: http://www.ietf.org/rfc/rfc3300.txt. Last accessed 31 December 2010.
12. Internet Engineering Task Force (2004). *RFC 3704 – Ingress Filtering for Multihomed Networks*. Accessible: http://www.ietf.org/rfc/rfc3704.txt. Last accessed 31 December 2010.

Appendix C: Change History

Date	Version	Changes for this version
November 9, 2010	2.1.0	Converted benchmark v2.0 to new template.
November 9, 2010	2.1.0	Updated all items with default values.
November 9, 2010	2.1.0	Updated all items with audit steps.
November 9, 2010	2.1.0	Removed require AAA service global command.
November 9, 2010	2.1.0	Removed forbid HTTP access control-HTTP is not used only HTTPS.
November 9, 2010	2.1.0	Removed require encrypted user passwords-this is the default as of v6.3 and not configurable.
November 9, 2010	2.1.0	Added require NetFlow logging.
November 9, 2010	2.1.0	Removed Require AAA flood guard. Now default behavior.
November 9, 2010	2.1.0	Added routing neighbor authentication requirements for EIGRP, OSPF, and RIP.
November 9, 2010	2.1.0	Updated grammar and sentence flow as needed for all items.
November 30, 2010	2.1.3	Added requirements for AAA accounting and authorization.
December 15, 2010	2.1.5	Removed requirement for AAA Floodguard. On by default in current FW Software.
December 30, 2010	2.2.0	Public Release