Center for Internet Security Benchmark for Cisco Firewall Devices

Version 2.0
November 2007

Edited by:
Steven Piliero
Leviathan Security Group

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

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**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, or 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 the Products or the Recommendations. 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:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. 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;
4. 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;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. 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:

1. 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;
2. 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.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

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.

Terms of Use Agreement Version 2.1 – 02/20/04

Cisco Firewall Benchmark

Introduction

This document defines a set of benchmarks or standards for securing Cisco devices. The benchmark is an industry consensus of current best practices listing actions to be taken as well as reasons for those actions. The enclosed recommendations are intended to provide step-by-step guidance to front line system and network administrators. They may be implemented manually or in conjunction with automated tools.

Applicability

This document applies to securing Cisco Adaptive Security Appliance (ASA), Firewall Services Module (FWSM) and PIX appliances.

Document Conventions

This document uses the following conventions within the remediation section of individual benchmark rules. The term device generally refers to the target system of this benchmark. "Cisco … uses the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument)
{y}	Braces enclose a required element (keyword or argument)
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
!	An exclamation point at the beginning of a line indicates a comment line.

"(Cisco Systems "About Cisco IOS Software Documentation for Release 12.4")

1 Benchmark for Cisco Firewalls

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

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

1.1 Management Plane Level 1

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

1.1.1.1 Require AAA Service

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

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: Globally enable authentication, authorization and accounting (AAA).

hostname(config)#**aaa authentication**

Scoring Status: Scorable

Additional References:

1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
3. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.1.2 Require AAA Authentication for Enable Mode

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 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 AAA authentication method(s) for enable authentication.

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

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.1.1.3 Require AAA Authentication for Console and VTY Lines

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

Rationale: Using AAA authentication for line 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.

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, ssh …)

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

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.1.1.4 Require Defined AAA Servers and Protocols

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** { **tacacs+** | radius }
hostname(config)#**aaa-server** {*server-tag*} **host** {*aaa_server-ip*} [*key*] [**timeout** *seconds*]

Scoring Status: Scorable

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

1.1.2 Access Rules

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

1.1.2.1 Require Local Password

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**

Scoring Status: Scorable

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

1.1.2.2 Require ASDM Access Control

Description: Verify the device configuration restricts remote management access via HTTP and adaptive security device manager (ASDM) to authorized management systems.

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

Platform(s): ASA, FWSM, PIX

Remediation: Configure remote administration access restrictions for HTTP and ADSM.

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

Scoring Status: Scorable

Additional References:
1. Cisco Security Appliance Command Reference, Version 7.2

1.1.2.3 Require HTTP Access Control

Description: Verify web browser access to the HTTP server service on the device is restricted.

Rationale: Web-based, remote administration access should be restricted to authorized management systems to minimize the devices attack surface and avoid potential compromise.

Platform(s): ASA, FWSM, PIX

Remediation: Restrict HTTP access to the device to authorized management systems.

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

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

1.1.2.4 Require SSH for Remote Device Access

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

Rationale: SSH 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. SSH also prevents session hijacking and many other kinds of network attacks. SSH should be employed to replace Telnet where available.

Platform(s): ASA, PIX

Remediation: Disable remote administration access via Telnet for all hosts and enable SSH.

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

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure
2. Cisco IOS Security Configuration Guide, Release 12.2
3. NSA Router Security Configuration Guide
4. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
5. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.2.5 Require Timeout for Login Sessions

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)#**telnet timeout** {*minutes*}
hostname(config)#**ssh timeout** {*minutes*}

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.2.6 Require Telnet and SSH Access Control

Description: Verify that management access to the device is restricted on all VTY lines.

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

Platform(s): ASA, FWSM, PIX

Remediation: Configure remote management restrictions for all VTY lines.

hostname(config)#**telnet** {*ip_address mask*} *interface*
hostname(config)#**ssh** {*ip_address mask*} *interface*

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure
2. NSA Router Security Configuration Guide

3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.3 Banner Rules

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

1.1.3.1 Require EXEC Banner

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*}

Scoring Status: Scorable

Additional References:

1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide

1.1.3.2 Require Login Banner

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*}

Scoring Status: Scorable

Additional References:

1. US Department of Justice - Cybercrime - Sample Network Login Banner
2. Improving Security on Cisco Routers
3. NSA Router Security Configuration Guide

1.1.3.3 Require MOTD Banner

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*}

Scoring Status: Scorable

Additional References:
1. US Department of Justice - Cybercrime - Sample Network Login Banner
2. Improving Security on Cisco Routers
3. NSA Router Security Configuration Guide

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

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*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.1.4.2 Require Enable Password

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**

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
3. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.4.3 Require Encrypted User Passwords

Description: Verify all locally defined users have encrypted passwords configured.

Rationale: If passwords are not set, an attacker can gain access to the device without a password if they can determine a valid username. Low quality passwords are easily guessed possibly providing unauthorized access to the router.

Platform(s): ASA, FWSM, PIX

Remediation: Configure user with an encrypted password.

hostname(config-line)# **username** {*local_username*} **password** {*local_password*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

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

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)

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.1.5.2 Forbid SNMP Traps

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**}

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide

1.1.5.3 Require SNMP Trap Server

Description: Verify device is configured to submit SNMP traps 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**
hostname(config)#**snmp-server host** {*interface_name ip_address* **trap**} **community** {*trap_community_string*}

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide

1.1.5.4 Require Authorized Read SNMP Community Strings and Access Control

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*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

1.2 Control Plane Level 1

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

1.2.1 Clock Rules

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

1.2.1.1 Require Clock Time Zone - UTC

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}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.2.1.2 Forbid Summer Time Clock

Description: Verify 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 summer time clock settings. Timestamp adjustments can lead to errors when correlating logs across multiple devices. Employ coordinated universal time (UTC) instead of local time zones and do not use summer-time, daylight saving, clock adjustments

Platform(s): ASA, PIX

Remediation: Disable clock summer-time adjustments.

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

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.2.1.3 Require Summer Time Clock

Description: Verify clock summer-time is configure 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(config)#**clock summer-time** [*time-zone*]

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

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

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)

Scoring Status: Scorable

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

1.2.2.2 Forbid HTTP Service

Description: Verify the HTTP 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, HTTP access should be restricted to authorized management systems.

Platform(s): ASA, FWSM, PIX

Remediation: Disable the HTTP server service.

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

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

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

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**

Scoring Status: Scorable

1.2.3.2 Require Console Logging Severity Level

Description: Verify logging to device console is enabled and 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 unless since they are not persistent.

Platform(s): ASA, FWSM, PIX

Remediation: Configure console logging level.

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

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
3. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.2.3.3 Require Logging Facility

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***}**

Scoring Status: Scorable

Additional 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

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 "debugging" (7) or "informational" (6), but no lower to ensure receipt of sufficient information concerning the devices

operational status. You can view the history table using the show logging history command.

Platform(s): ASA, FWSM, PIX

Remediation: Configure logging history level.

hostname(config)#**logging history {6 | informational}**

Scoring Status: Scorable

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

1.2.3.5 Require Logging to Syslog Server

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.

Platform(s): ASA, FWSM, PIX

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

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

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.2.3.6 Require Logging Trap Severity Level

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}**

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. NSA Router Security Configuration Guide
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.2.3.7 Require System Logging

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)

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. Cisco IOS Security Configuration Guide, Release 12.2
3. Cisco Auto Secure
4. NSA Router Security Configuration Guide
5. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
6. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

1.2.3.8 Require Timestamps in Log Messages

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**

Scoring Status: Scorable

Additional References:
1. Improving Security on Cisco Routers
2. Cisco IOS Security Configuration Guide, Release 12.2
3. Cisco Auto Secure
4. NSA Router Security Configuration Guide
5. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
6. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

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

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

Remediation: Designate a primary, trusted NTP timeserver.

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

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.2.4.2 Require NTP Authentication

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

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**]

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

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 function- ality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

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 Forbid Conduits

Description: Verify that legacy conduit statements are not configured.

Rationale: Using the legacy conduit facility to restrict access does not offer sufficient control of stateful traffic filtering. Conduit statements are deprecated and are not available in new releases.

Platform(s): PIX

Remediation:
hostname(config)#**no conduit**

Scoring Status: Scorable

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

1.3.1.2 Require OS Version

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.

Scoring Status: Scorable

Additional References:
1. Cisco Security Advisories and Notices

1.3.1.3 Require Connection Timeout

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*** | ***xlate***} {*00:30:00*}

Scoring Status: Scorable

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

1.3.1.4 Require Translation Slot Timeout

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*}

Scoring Status: Scorable

Additional References:

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

1.3.1.5 Require Intrusion Detection Actions

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 info {action {alarm}}**
hostname(config)#**ip audit audit {action {alarm}}**

Scoring Status: Scorable

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

1.3.1.6 Require AAA Flood Guard

Description: Verify flood guard is enabled to protect against flood attacks.

Rationale: Enable floodguard to protect against flood attacks against the uauth, authentication system on the device. If the system is attacked with excessive tcp connections, the device will actively reclaim TCP user resources, connection slots, which are ending. See the command reference regarding the order in which tcp connections are reclaimed (timewait, last-ack, finwait, etc.). Floodguard protects against denial-of-service attacks (DoS) on authentication, authorization and accounting (AAA) services.

Platform(s): FWSM, PIX

Remediation: Enable floodguard.

hostname(config)#**floodguard** {**enable**}

Scoring Status: Scorable

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

1.3.1.7 Require Fragment Chain Fragmentation Checks

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*}

Scoring Status: Scorable

Additional 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 Protocol Inspection

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*]

Scoring Status: Scorable

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

1.3.2 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

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*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Improving Security on Cisco Routers
3. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address

Spoofing
4. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.3.2.2 Forbid Private Source Addresses from External Networks

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*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide
2. Improving Security on Cisco Routers
3. RFC 3704 - Ingress Filtering for Multi-homed Networks (Updates RFC 2827)
4. RFC 3300 - Special-Use IPv4 Addresses
5. RFC 3171 - IANA Guidelines for IPv4 Multicast Address Assignments
6. RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
7. RFC 1918 - Address Allocation for Private Internets
8. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

1.3.2.3 Forbid Inbound Traceroute Messages

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*}

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

1.3.2.4 Require Explicit Deny Any in ACLs

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*>

Scoring Status: Scorable

Additional References:
1. 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

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*}

Scoring Status: Scorable

Additional References:
1. RFC 2267 - Network Ingress Filtering
2. Improving Security on Cisco Routers
3. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
4. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0

Appendix A: Prerequisites for Configuring SSH

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

1. Configure the device hostname
2. Configure the device domain name
3. Generate an RSA key pair, which is required for SSH access
4. Save the RSA key pair to persistent Flash memory

hostname(config)#**hostname** { *device_hostname* }
hostname(config)#**domain-name** { *domain-name* }
hostname(config)#**crypto key generate rsa modulus** { *2048* }
hostname(config)#**write mem**