Center for Internet Security Benchmark For Cisco IOS

Version 2.2

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 IOS Benchmark

Introduction

This document defines a set of benchmarks or standards for securing Cisco IOS. 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 IOS appliances running version 12.x or higher software.

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 Level-1 Benchmark

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

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

1.1 Management Plane Level 1

Description: Services, settings and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative 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 (new-model) 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.

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

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

Scoring Status: Scorable

Additional References:

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

1.1.1.2 Require AAA Authentication for Login

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

Dependencies:

- Requires: 1.1.1.1 Require AAA Service

Warning: Only "the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list." (Cisco IOS Security Guide v12.3)

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

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

Scoring Status: Scorable

Additional References:

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

1.1.1.3 Require AAA Authentication for Enable Mode

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services 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.

Dependencies:

- Requires: 1.1.1.1 Require AAA Service

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

hostname(config)#**aaa authentication enable** { **default** } **enable**

Scoring Status: Scorable

Additional References:

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

1.1.1.4 Require AAA Authentication for Local Console and VTY Lines

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

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. If a named AAA authentication list, other than **default**, is required then authentication must be configured explicitly on each IOS line.

Dependencies:

- Requires: 1.1.1.1 Require AAA Service

Warning: Only "the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list." (Cisco IOS Security Guide v12.3)

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

hostname(config)#**line** {**aux** | **console** | **tty** | **vty**} { *line-number* } [*ending-line-number*]
hostname(config-line)#**login authentication** { **default** | *aaa_list_name* }

Scoring Status: Scorable

Additional References:

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

1.1.2 Access Rules

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

1.1.2.1 Require Local User and Encrypted Password

Description: Verify at least one local user exists and ensure all locally defined user passwords are protected by encryption.

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

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

! This fix is commented out because you have to supply a sensitive value.
! To apply this rule, uncomment (remove the leading "!" on the commands below)
! and replace "LOCAL PASSWORD" with the value you have chosen.
! Do not use "LOCAL PASSWORD"
!
! hostname(config)#**username** { *LOCAL_USERNAME* } **password** { *LOCAL_PASSWORD* **}**
!
! Use the following syntax for version after 12.0(18)S, 12.1(8a)E, 12.2(8)T
!
! hostname(config)#**username** { *LOCAL_USERNAME* } **secret** { *LOCAL_PASSWORD* **}**

Scoring Status: Scorable

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

1.1.2.2 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.

Remediation: Enable remote administration via SSH for incoming VTY login.

hostname(config)#**ip ssh timeout** [*60*]
hostname(config)#**ip ssh authentication-retries** [*3*]

Scoring Status: Scorable

Additional References:
1. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
2. Center for Internet Security Gold Standard Benchmark for Cisco PIX Version 1.0
3. NSA Router Security Configuration Guide
4. Cisco Auto Secure
5. Cisco IOS Security Configuration Guide, Release 12.4

1.1.2.3 Require VTY Transport SSH

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

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

Remediation: Apply VTY transport SSH on all management lines

hostname(config)#**line** {**aux** | **console** | **tty** | **vty**} **{***line-number*} [*ending-line-number*]
hostname(config-line)#**transport input ssh**

Scoring Status: Scorable

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

1.1.2.4 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.

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

hostname(config)#**line** {**aux** | **console** | **tty** | **vty} {***line-number*} [*ending-line-number*]
hostname(config-line)#**exec-timeout** {*timeout_in_minutes*} [*timeout_in_seconds*]

Scoring Status: Scorable

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

1.1.2.5 Forbid Auxiliary Port

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

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

Remediation: Disable exec on the auxiliary port.

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

Scoring Status: Scorable

Additional References:
1. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
2. NSA Router Security Configuration Guide
3. Cisco Auto Secure
4. Improving Security on Cisco Routers
5. Cisco IOS Security Configuration Guide, Release 12.4

1.1.2.6 Require SSH Access Control

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

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

Remediation: Configure remote management restrictions for all VTY lines.

hostname(config)#**line** {**aux** | **console** | **tty** | **vty**} **{***line-number*} [*ending-line-number*]
hostname(config-line)# **access-class** [*vty_acl_number*] **in**

Scoring Status: Scorable

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

1.1.2.7 Require VTY ACL

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

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

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

hostname(config)#**access-list** {*vty_acl_number*} **permit tcp** {*vty_acl_block_with_mask*} any
hostname(config)#**access-list** {*vty_acl_number*} **permit tcp host** [*vty_acl_host*] any
hostname(config)#**deny ip any any log**

Scoring Status: Scorable

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

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)

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)

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)

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 Enable Secret

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.

Remediation: Configure a strong enable secret password.

! This fix is commented out because you have to supply a sensitive value.
! To apply this rule, uncomment (remove the leading "!" on the commands below)
! and replace "ENABLE SECRET" with the value you have chosen.
! Do not use "ENABLE SECRET".
!
! hostname(config)#**enable secret** {*ENABLE_SECRET*}

Scoring Status: Scorable

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

1.1.4.2 Require Encrypted Line Passwords

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

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

Remediation: Configure each line with a strong, encrypted password

! This fix is commented out because you have to supply a sensitive value.
! To apply this rule, uncomment (remove the leading "!" on the commands below)
! and replace "LINE PASSWORD" with the value you have chosen.
! Do not use "LINE PASSWORD". Instead, choose a value that is longer
! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.
!
! hostname(config)# **line** {**aux** | **console** | **tty** | **vty**} **{***line-number*} [*ending-line-number*]
! hostname(config-line)#**password** *LINE_PASSWORD*

Scoring Status: Scorable

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

1.1.4.3 Require Encrypted User Passwords

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

Rationale: If 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.

Remediation: Configure user with an encrypted password.

! This fix is commented out because you have to supply a sensitive value.
! To apply this rule, uncomment (remove the leading "!" on the commands below)
! and replace "LOCAL_PASSWORD" with the value you have chosen.
! Do not use "LOCAL_PASSWORD". Instead, choose a value that is longer
! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.
!
! hostname(config)#**username** { *LOCAL_USERNAME* } **password** { *LOCAL_PASSWORD* **}**
!
! Use the following syntax for version after 12.0(18)S, 12.1(8a)E, 12.2(8)T
!
! hostname(config)#**username** { *LOCAL_USERNAME* } **secret** { *LOCAL_PASSWORD* **}**

Scoring Status: Scorable

Additional References:

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

1.1.4.4 Require Password Encryption Service

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

Rationale: This requires passwords to be encrypted in the configuration file to prevent unauthorized users from learning the passwords by reading the configuration. If this service is not enabled then many of the devices passwords will be rendered in plain text in its configuration file. This service ensures passwords are rendered as encrypted strings preventing an attacker from easily determining the configured value.

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

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

Scoring Status: Scorable

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

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 Community String private

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

Rationale: SNMP allows management and monitoring of networked devices. "private" is a well known default community string. Using easy to guess, well known, community strings poses a threat that an attacker can effortlessly gain unauthorized access to the device. 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 enable password, line password, BGP key or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication, authorization and data privatization (encryption), when available.

Remediation: Disable default or prohibited SNMP community strings.

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

Scoring Status: Scorable

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

1.1.5.2 Forbid SNMP Community String public

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

Rationale: SNMP allows management and monitoring of networked devices. "public" is a well known default community string. Using easy to guess, well known, community strings poses a threat that an attacker can effortlessly gain unauthorized access to the device. 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 enable password, line password, BGP key or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication, authorization and data privatization (encryption), when available.

Remediation: Disable default or prohibited SNMP community strings.

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

Scoring Status: Scorable

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

1.1.5.3 Forbid SNMP Read and Write Access

Description: Disable simple network management protocol (SNMP), read and write access, if not in use.

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, authorization and data privatization (encryption), when available. SNMP versions 1 and 2 use clear-text community strings, which are considered a weak security implementation.

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

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

Scoring Status: Scorable

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

1.1.5.4 Forbid SNMP Write Access

Description: Verify the device will not allow simple network management protocol (SNMP) write access.

Rationale: Enabling SNMP read-write enables remote (mis)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). Enabling write access poses the threat that an attacker can potentially capture SNMP packets, determine the write community string and remotely manipulate the device.

Remediation: Disable SNMP write access.

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

Scoring Status: Scorable

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

1.1.5.5 Forbid SNMP without ACL

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

Rationale: If ACLs are not applied, then anyone with a valid SNMP community string can potentially monitor and manage the router. An ACL should be defined and applied for all SNMP access to limit access to a small number of authorized management stations segmented in a trusted management zone.

Remediation: Configure SNMP access restrictions via an ACL.

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

Scoring Status: Scorable

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

1.1.5.6 Require a Defined SNMP ACL

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

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

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

hostname(config)#**access-list** {*snmp_access-list_number*}**permit** {*snmp_access-list*}
hostname(config)#**access-list deny any log**

Scoring Status: Scorable

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

1.1.5.7 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.

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** {read_*community_ string*} {**ro**} {*snmp_access-list_number*}

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 Timezone - UTC

Description: Verify the timezone 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.

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. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
2. NSA Router Security Configuration Guide page 134

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.

Remediation: Disable clock summer-time adjustments.

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

Scoring Status: Scorable

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

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 CDP Run Globally

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

Rationale: The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in specialized situations, and is considered a security risk. There have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless there is a need for it.

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

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

Scoring Status: Scorable

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

1.2.2.2 Forbid Finger Service

Description: Disable finger server.

Rationale: Finger is used to find out which users are logged into a device. This service is rarely used in practical environments and can potentially provide an attacker with useful information. Additionally, the finger service can exposed the device Finger of Death denial-of-service (DoS) attack. From Cisco IOS documentation: "As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."

Remediation: Disable finger server.

hostname(config)#**no ip finger** (versions after 12.1(5) and 12.1(5)T)
or
hostname(config)#**no service finger** (versions before 12.1(5) and 12.1(5)T)

Scoring Status: Not Scorable

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

1.2.2.3 Forbid IP BOOTP server

Description: Disable bootstrap protocol (BOOTP) server.

Rationale: From Cisco IOS documentation: "As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."

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

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

Scoring Status: Scorable

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

1.2.2.4 Forbid Identification Service

Description: Disable identification (identd) server.

Rationale: Identification protocol enables identifying a users transmission control protocol (TCP) session. This information disclosure could potentially provide an attacker with information about users. Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.

Remediation: Disable ident server.

hostname(config)#**no identd**

Scoring Status: Scorable

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

1.2.2.5 Forbid IP HTTP Server

Description: Disable HTTP server.

Rationale: The HTTP server allows remote management of routers. Unfortunately, it uses simple HTTP authentication which sends passwords in the clear. This could allow unauthorized access to, and [mis]management of the router. The http server should be disabled.

Remediation: Disable http server.

hostname(config)#**no ip http server**

Scoring Status: Scorable

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

1.2.2.6 Forbid Remote Startup Configuration

Description: Disable autoloading of remote configuration files from a network server.

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

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

hostname(config)#**no boot network**
hostname(config)#**no service config**

Scoring Status: Scorable

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

1.2.2.7 Require TCP keepalives-in Service

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

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

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

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

Scoring Status: Scorable

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

1.2.2.8 Require TCP keepalives-out Service

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

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

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

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

Scoring Status: Scorable

Additional References:
1. Cisco Auto Secure

1.2.2.9 Forbid tcp-small-servers

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

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

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

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

Scoring Status: Scorable

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

1.2.2.10 Forbid udp-small-servers

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

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

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

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

Scoring Status: Scorable

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

1.2.2.11 Forbid TFTP Server

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

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

Remediation: Disable tftp-server service.

hostname(config)#**no tftp-server**

Scoring Status: Scorable

Additional References:
1. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1

2. NSA Router Security Configuration Guide
3. Cisco Auto Secure

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 Require Logging

Description: Verify logging is enabled.

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, device logging is highly recommended or required by most security regulations.

Remediation: Enable logging.

hostname(config)#**logging on**

Scoring Status: Scorable

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

1.2.3.2 Require Logging Buffer

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

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

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

hostname(config)#**logging buffered** *log_buffer_size*

Scoring Status: Scorable

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

1.2.3.3 Require Logging to Device Console

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

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

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

Remediation: Configure console logging level.

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

Scoring Status: Scorable

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

1.2.3.4 Require Logging to Syslog Server

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

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

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

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

Scoring Status: Scorable

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

1.2.3.5 Require Logging Trap Severity Level

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

Rationale: This determines the severity of messages that will generate simple network management protocol (SNMP) trap and or syslog messages. this setting should be set to either "debugging" (7) or "informational" (6), but no lower. The default, in IOS 11.3 and later is [informational].

Remediation: Configure SNMP trap and syslog logging level.

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

Scoring Status: Scorable

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

1.2.3.6 Require Service Timestamps for Debug Messages

Description: Configure debug message to include timestamps.

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

Remediation: Configure debug message to include timestamps.

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

Scoring Status: Scorable

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

1.2.3.7 Require Service Timestamps in Log Messages

Description: Configure logging to include message timestamps.

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

Remediation: Configure logging to include message timestamps.

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

Scoring Status: Scorable

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

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.

Remediation: Designate a primary, trusted NTP timeserver.

hostname(config)#**ntp server** {*ntp_server_1*}

Scoring Status: Scorable

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

1.2.4.2 Require Secondary NTP Server

Description: Verify configuration of a secondary, 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.

Remediation: Designate a secondary, trusted NTP timeserver.

hostname(config)#**ntp server** {*ntp_server_2*}

Scoring Status: Scorable

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

1.2.4.3 Require Tertiary NTP Server

Description: Verify configuration of a tertiary, 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.

Remediation: Designate a tertiary, trusted NTP timeserver.

hostname(config)#**ntp server** {*ntp_server_3*}

Scoring Status: Scorable

Additional References:
1. Center for Internet Security Gold Standard Benchmark for Cisco IOS Version 2.1
2. 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 Routing Rules

Description: Unneeded services should be disabled.

1.3.1.1 Forbid Directed Broadcast

Description: Disallow IP directed broadcast on each interface.

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

Remediation: Disable directed broadcast on each interface.

hostname(config)#**interface** *interface-id*
hostname(config-if)#**no ip directed-broadcast**

Scoring Status: Scorable

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

1.3.1.2 Forbid IP source-route

Description: Disable source routing.

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

Remediation: Disable source routing.

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

Scoring Status: Scorable

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

2 Level-2 Benchmark

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

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

2.1 Management Plane Level 2

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. Exam- ples of management plane services include: administrative telnet, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.

2.1.1 Authentication, Authorization and Accounting Rules

Description: Rules in the authentication, authorization and accounting (AAA) configuration class enforce centralized device access control.

2.1.1.1 Require AAA Authentication Enable

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

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.

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

hostname(config)#**aaa authentication enable** { **default** } **group tacacs+** [**enable** ...]

Scoring Status: Scorable

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

2.1.1.2 Require AAA Authentication Login

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

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.

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

hostname(config)#**aaa authentication login** { **default** | *aaa_list_name* } **group tacacs+** [**local-case** ...]

Scoring Status: Scorable

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

2.1.1.3 Require AAA Accounting Commands

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring accounting 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.

Remediation: Configure AAA accounting for commands.

hostname(config)#**aaa accounting** {**commands 15**} {**default**} {**start-stop**} **{group-tacacs+**} [**local-case …**]

Scoring Status: Scorable

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

2.1.1.4 Require AAA Accounting Connection

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring accounting 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.

Remediation: Configured AAA accounting for connections.

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

Scoring Status: Scorable

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

2.1.1.5 Require AAA Accounting Exec

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring accounting 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.

Remediation: Configure AAA accounting for exec.

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

Scoring Status: Scorable

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

2.1.1.6 Require AAA Accounting Network

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring accounting 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.

Remediation: Configure AAA accounting for network events.

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

Scoring Status: Scorable

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

2.1.1.7 Require AAA Accounting System

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

Rationale: Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring accounting 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.

Remediation: Configure AAA accounting for system events.

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

Scoring Status: Scorable

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

2.2 Control Plane Level 2

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

2.2.1 Loopback Rules

Description: Rules in the loopback class enforce virtual interfaces source address standardization to enhance security, consistency of device identification and stability. Note that addresses that are assigned loopback interfaces on device must have routes to communicate with management devices (syslog, Telnet, TACACS+, SNMP.)

2.2.1.1 Require Binding AAA Service to Loopback Interface

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

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

Remediation: Bind AAA services to the loopback interface.

Hostname(config)#**ip tacacs+ source-interface loopback** {*0*}

Scoring Status: Scorable

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

2.2.1.2 Require Binding NTP Service to Loopback Interface

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

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

Remediation: Bind the NTP service to the loopback interface.

hostname(config)#**ntp source loopback** {*0*}

Scoring Status: Scorable

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

2.2.1.3 Require Binding TFTP Service to Loopback Interface

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

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

Remediation: Bind the TFTP client to the loopback interface.

hostname(config)#**ip tftp source-interface loopback** {*0*}

Scoring Status: Scorable

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

2.2.1.4 Require Loopback Interface

Description: Define and configure one loopback interface.

Rationale: The loopback interface provides a standard interface to be used in logging, time, routing protocols, and for ACLs limiting administrative access.

Remediation: Define and configure one loopback interface.

hostname(config)#**interface loopback** {*0*}
hostname(config-if)#**ip address** {*loopback_ip_address*}

Scoring Status: Scorable

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

2.2.1.5 Forbid Multiple Loopback Interfaces

Description: Define no more than one loopback interface.

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

Remediation: Define no more than one loopback interface.
hostname(config)#**no loopback {***instance***}**

Scoring Status: Scorable

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

2.3 Data Plane Level 2

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

2.3.1 Border Router Filtering

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

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

2.3.1.1 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).

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

Remediation: Configure ACL for private source address restrictions from external networks
hostname(config)#**access-list** {*access-list*} **deny ip** {*internal_networks*} **any log**
hostname(config)#**access-list** {*access-list*} **deny ip 127.0.0.0 0.255.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 10.0.0.0 0.255.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 0.0.0.0 0.255.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 172.16.0.0 0.15.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 192.168.0.0 0.0.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 192.0.2.0 0.0.0.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 169.254.0.0 0.0.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip 224.0.0.0 31.255.255.255 any log**
hostname(config)#**access-list** {*access-list*} **deny ip host 255.255.255.255 any log**
hostname(config)#**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

2.3.1.2 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.

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

2.3.2 Neighbor Authentication

2.3.2.1 Require BGP Authentication if Protocol is Used

Description: Verify border gateway protocol (BGP) 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 BGP neighbor authentication where feasible

hostname(config)#**router bgp** { *bgp_as-number* }
hostname(config-router)#**neighbor** { *bgp_neighbor-ip* | *peer-group-name* } **password { ***bgp_md5_key* **}**

Scoring Status: Scorable

Additional References:

1. NSA Router Security Configuration Guide

2.3.2.2 Require EIGRP Authentication if Protocol is Used

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)#**router eigrp** { *eigrp_as-number* }
hostname(config)#**key chain** { *eigrp_key-chain_name* }
hostname(config-keychain)#**key {** *eigrp_key-number* **}**
hostname(config-keychain-key)#**key-string {** *eigrp_key-string* **}**

hostname(config)#**interface** {*interface_name* }
hostname(config-if)#**ip authentication mode eigrp** { *eigrp_as-number* } **md5**
hostname(config-if)#**ip authentication key-chain eigrp** { *eigrp_as-number* } { *eigrp_key-chain_name* }

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

2.3.2.3 Require OSPF Authentication if Protocol is Used

Description: Verify open shortest path first (OSPF) protocol 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 OSPF neighbor authentication where feasible

hostname(config)#**router ospf** {*ospf_process-id* }
hostname(config-router)#**area {** *ospf_area-id* **} authentication message-digest**
hostname(config)#**interface** {*interface_name* }
hostname(config-if)#**ip ospf message-digest-key** {*ospf_md5_key-id* } **md5** { *ospf_md5_key* }

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

2.3.2.4 Require RIPv2 Authentication if Protocol is used

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 feasbile

hostname(config)#**key chain** { *rip_key-chain_name* }
hostname(config-keychain)#**key {** *rip_key-number* **}**
hostname(config-keychain-key)#**key-string {** *rip_key-string* **}**
hostname(config)#**interface** {*interface_name* }
hostname(config-if)#**ip rip authentication key-chain** { *rip_key-chain_name* }
hostname(config-if)#**ip rip authentication mode md5**

Scoring Status: Scorable

Additional References:
1. NSA Router Security Configuration Guide

2.3.3 Routing Rules

Description: Unneeded services should be disabled.

2.3.3.1 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.

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

hostname(config)#**ip cef**
hostname(config)#**interface** {*interface_name*}
hostname(config-if)#**ip verify unicast reverse-path rx** (versions after 12.0(15)S)
hostname(config-if)#**ip verify unicast reverse-path** (versions before 12.0(15)S)

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

2.3.3.2 Forbid IP Proxy ARP

Description: Verify proxy ARP is disabled on all interfaces.

Rationale: Proxy ARP breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments.

Remediation: Disable proxy ARP on all interfaces.

hostname(config)#**interface** {*interface_name*}
hostname(config-if)#**no ip proxy-arp**

Scoring Status: Scorable

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

2.3.3.3 Forbid Tunnel Interfaces

Description: Verify no tunnel interfaces are defined.

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

Remediation: Do not define any tunnel interfaces.

Hostname(config)#**no interface tunnel** {*instance*}

Scoring Status: Scorable

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

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**