CIS Benchmarks

CIS Cisco IOS 15 Benchmark

v4.1.0 - 02-16-2021

Terms of Use

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

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

Table of Contents

Overview

This document, Security Configuration Benchmark for Cisco IOS, provides prescriptive guidance for establishing a secure configuration posture for Cisco Router running Cisco IOS version 15.0M. This guide was tested against Cisco IOS IP Advanced IP Services v15.0.1 as installed by c880data-universalk9-mz.150-1.M4.bin. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Assessment Status

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

Automated

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

Manual

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

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

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor
Justin Opatrny
jason nehrboss
Michael Hamelin
Tim Muniz
Craig Anteman
Jason Braun
Brian Sak
David McMillan
Mike Wicks GCIH, GSEC, GSLC, GCFE, GISP
Philippe Langlois
Darren Freidel
Sara Archacki

Recommendations

1 Management Plane

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

1.1 Local Authentication, Authorization and Accounting (AAA) Rules

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

1.1.1 Enable 'aaa new-model' (Automated)

Profile Applicability:

- Level 1

Description:

This command enables the AAA access control system.

Rationale:

Authentication, authorization and accounting (AAA) services 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.

Impact:

Implementing Cisco AAA is significantly disruptive as former access methods are immediately disabled. Therefore, before implementing Cisco AAA, the organization should carefully review and plan their authentication criteria (logins & passwords, challenges & responses, and token technologies), authorization methods, and accounting requirements.

Audit:

Perform the following to determine if AAA services are enabled:

```
hostname#show running-config | incl aaa new-model
```

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

Remediation:

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

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

Default Value:

AAA is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a2.html#GUID-E05C2E00-C01E-4053-9D12-EC37C7E8EEC5

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.2 Enable 'aaa authentication login' (Automated)

Profile Applicability:

- Level 1

Description:

Sets authentication, authorization and accounting (AAA) authentication at login.

Rationale:

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

Impact:

Implementing Cisco AAA is significantly disruptive as former access methods are immediately disabled. Therefore, before implementing Cisco AAA, the organization should carefully review and plan their authentication methods such as logins and passwords, challenges and responses, and which token technologies will be used.

Audit:

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

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

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

Remediation:

Configure AAA authentication method(s) for login authentication.

```
hostname(config)#aaa authentication login {default | aaa_list_name} [passwd-
expiry]
[method1] [method2]
```

Default Value:

AAA authentication at login is disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-3DB1CC8A-4A98-400B-A906-C42F265C7EA2

Additional Information:

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

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.3 Enable 'aaa authentication enable default' (Automated)

Profile Applicability:

- Level 1

Description:

Authenticates users who access privileged EXEC mode when they use the enable command.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA.

Impact:

Enabling Cisco AAA 'authentication enable' mode is significantly disruptive as former access methods are immediately disabled. Therefore, before enabling 'aaa authentication enable default' mode, the organization should plan and implement authentication logins and passwords, challenges and responses, and token technologies.

Audit:

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

```
hostname#show running-config | incl aaa authentication enable
```

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

Remediation:

Configure AAA authentication method(s) for enable authentication.

```
hostname(config)#aaa authentication enable default {method1} enable
```

Default Value:

By default, fallback to the local database is disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-4171D649-2973-4707-95F3-9D96971893D0

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.4 Set 'login authentication for 'line con 0' (Manual)

Profile Applicability:

- Level 1

Description:

Authenticates users who access the router or switch using the serial console port.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA.

Impact:

Enabling Cisco AAA 'line login' is significantly disruptive as former access methods are immediately disabled. Therefore, before enabling Cisco AAA 'line login', the organization should plan and implement authentication logins and passwords, challenges and responses, and token technologies.

Audit:

Perform the following to determine if AAA authentication for line login is enabled:
If the command does not return a result for each management access method, the feature is not enabled

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

Remediation:

Configure management lines to require login using the default or a named AAA authentication list. This configuration must be set individually for all line types.

```
hostname(config)#line console 0

hostname(config-line)#login authentication {default | _aaa\_list\_name_}
```

Default Value:

Login authentication is not enabled.

Uses the default set with aaa authentication login.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-k1.html#GUID-297BDF33-4841-441C-83F3-4DA51C3C7284

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.5 Set 'login authentication for 'line tty' (Automated)

Profile Applicability:

- Level 1

Description:

Authenticates users who access the router or switch using the TTY port.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA.

Impact:

Enabling Cisco AAA 'login authentication for line TTY' is significantly disruptive as former access methods are immediately disabled. Therefore, before enabling Cisco AAA 'login authentication for line TTY', the organization should plan and implement authentication logins and passwords, challenges and responses, and token technologies.

Audit:

Perform the following to determine if AAA authentication for line login is enabled:
If the command does not return a result for each management access method, the feature is not enabled

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

Remediation:

Configure management lines to require login using the default or a named AAA authentication list. This configuration must be set individually for all line types.

```
hostname(config)#line tty {line-number} [ending-line-number]
hostname(config-line)#login authentication {default | aaa_list_name}
```

Default Value:

Login authentication is not enabled.

Uses the default set with aaa authentication login.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-k1.html#GUID-297BDF33-4841-441C-83F3-4DA51C3C7284

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.6 Set 'login authentication for 'line vty' (Automated)

Profile Applicability:

- Level 1

Description:

Authenticates users who access the router or switch remotely through the VTY port.

Rationale:

Using AAA authentication for interactive management access to the device provides consistent, centralized control of your network. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA.

Impact:

Enabling Cisco AAA 'login authentication for line VTY' is significantly disruptive as former access methods are immediately disabled. Therefore, before enabling Cisco AAA 'login authentication for line VTY', the organization should plan and implement authentication logins and passwords, challenges and responses, and token technologies.

Audit:

Perform the following to determine if AAA authentication for line login is enabled:
If the command does not return a result for each management access method, the feature is not enabled

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

Remediation:

Configure management lines to require login using the default or a named AAA authentication list. This configuration must be set individually for all line types.

```
hostname(config)#line vty {line-number} [<em>ending-line-number]
hostname(config-line)#login authentication {default | aaa_list_name}
```

Default Value:

Login authentication is not enabled.

Uses the default set with aaa authentication login.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-k1.html#GUID-297BDF33-4841-441C-83F3-4DA51C3C7284

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.7 Set 'aaa accounting' to log all privileged use commands using 'commands 15' (Automated)

Profile Applicability:

- Level 2

Description:

Runs accounting for all commands at the specified privilege level.

Rationale:

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

Impact:

Enabling 'aaa accounting' for privileged commands records and sends activity to the accounting servers and enables organizations to monitor and analyze privileged activity.

Audit:

Perform the following to determine if aaa accounting for commands is required:
Verify a command string result returns

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

Remediation:

Configure AAA accounting for commands.

```
hostname(config)#aaa accounting commands 15 {default | list-name | guarantee-
first}
{start-stop | stop-only | none} {radius | group group-name}
```

Default Value:

AAA accounting is disabled.

Additional Information:

Valid privilege level entries are integers from 0 through 15.

CIS Controls:

Version 7

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

1.1.8 Set 'aaa accounting connection' (Automated)

Profile Applicability:

- Level 2

Description:

Provides information about all outbound connections made from the network access server.

Rationale:

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

Impact:

Implementing aaa accounting connection creates accounting records about connections from the network access server. Organizations should regular monitor these connection records for exceptions, remediate issues, and report findings regularly.

Audit:

Perform the following to determine if aaa accounting for connection is required:
Verify a command string result returns

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

Remediation:

Configure AAA accounting for connections.

```
hostname(config)#aaa accounting connection {default | list-name | guarantee-
first}
{start-stop | stop-only | none} {radius | group group-name}
```

Default Value:

AAA accounting is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-0520BCEF-89FB-4505-A5DF-D7F1389F1BBA

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.9 Set 'aaa accounting exec' (Automated)

Profile Applicability:

- Level 2

Description:

Runs accounting for the EXEC shell session.

Rationale:

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

Impact:

Enabling aaa accounting exec creates accounting records for the EXEC terminal sessions on the network access server. These records include start and stop times, usernames, and date information. Organizations should regularly monitor these records for exceptions, remediate issues, and report findings.

Audit:

Perform the following to determine if aaa accounting for EXEC shell session is required: Verify a command string result returns

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

Remediation:

Configure AAA accounting for EXEC shell session.

```
hostname(config)#aaa accounting exec {default | list-name | guarantee-first}
{start-stop | stop-only | none} {radius | group group-name}
```

Default Value:

AAA accounting is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-0520BCEF-89FB-4505-A5DF-D7F1389F1BBA

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

1.1.10 Set 'aaa accounting network' (Automated)

Profile Applicability:

- Level 2

Description:

Runs accounting for all network-related service requests.

Rationale:

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

Impact:

Implementing aaa accounting network creates accounting records for a method list including ARA, PPP, SLIP, and NCPs sessions. Organizations should regular monitor these records for exceptions, remediate issues, and report findings.

Audit:

Perform the following to determine if aaa accounting for connection is required:
Verify a command string result returns

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

Remediation:

Configure AAA accounting for connections.

```
hostname(config)#aaa accounting network {default | list-name | guarantee-
first}
{start-stop | stop-only | none} {radius | group group-name}
```

Default Value:

AAA accounting is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-0520BCEF-89FB-4505-A5DF-D7F1389F1BBA

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

1.1.11 Set 'aaa accounting system' (Automated)

Profile Applicability:

- Level 2

Description:

Performs accounting for all system-level events not associated with users, such as reloads.

Rationale:

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

Impact:

Enabling aaa accounting system creates accounting records for all system-level events. Organizations should regular monitor these records for exceptions, remediate issues, and report findings regularly.

Audit:

Perform the following to determine if aaa accounting system is required:
Verify a command string result returns

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

Remediation:

Configure AAA accounting system.

```
hostname(config)#aaa accounting system {default | list-name | guarantee-
first}
{start-stop | stop-only | none} {radius | group group-name}
```

Default Value:

AAA accounting is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID-0520BCEF-89FB-4505-A5DF-D7F1389F1BBA

Additional Information:

When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

1.2 Access Rules

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

1.2.1 Set 'privilege 1' for local users (Manual)

Profile Applicability:

- Level 1

Description:

Sets the privilege level for the user.

Rationale:

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

Impact:

Organizations should create policies requiring all local accounts with 'privilege level 1' with encrypted passwords to reduce the risk of unauthorized access. Default configuration settings do not provide strong user authentication to the device.

Audit:

Perform the following to determine if a user with an encrypted password is enabled:
Verify all username results return "privilege 1"

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

Remediation:

Set the local user to privilege level 1.

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

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-t2-z.html#GUID-34B3E43E-0F79-40E8-82B6-A4B5F1AFF1AD

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.2.2 Set 'transport input ssh' for 'line vty' connections (Automated)

Profile Applicability:

- Level 1

Description:

Selects the Secure Shell (SSH) protocol.

Rationale:

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

Impact:

To reduce risk of unauthorized access, organizations should require all VTY management line protocols to be limited to ssh.

Audit:

Perform the following to determine if SSH is the only transport method for incoming VTY logins:
The result should show only "ssh" for "transport input"

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

Remediation:

Apply SSH to transport input on all VTY management lines

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

References:

1. http://www.cisco.com/en/US/docs/ios/termserv/command/reference/tsv_s1.html#wp1069219

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.2.3 Set 'no exec' for 'line aux 0' (Automated)

Profile Applicability:

- Level 1

Description:

The 'no exec' command restricts a line to outgoing connections only.

Rationale:

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

Impact:

Organizations can reduce the risk of unauthorized access by disabling the 'aux' port with the 'no exec' command. Conversely, not restricting access through the 'aux' port increases the risk of remote unauthorized access.

Audit:

Perform the following to determine if the EXEC process for the aux port is disabled:
Verify no exec

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

Verify you see the following "no exec"

```
hostname#sh line aux 0 | incl exec
```

Remediation:

Disable the EXEC process on the auxiliary port.

```
hostname(config)#line aux 0
hostname(config-line)#no exec
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-429A2B8C-FC26-49C4-94C4-0FD99C32EC34

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.2.4 Create 'access-list' for use with 'line vty' (Automated)

Profile Applicability:

- Level 1

Description:

Access lists control the transmission of packets on an interface, control Virtual Terminal Line (VTY) access, and restrict the contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Rationale:

VTY ACLs control what addresses may attempt to log in to the router. Configuring VTY lines to use an ACL, restricts the sources where a user can manage the device. 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 administer the device. For example, you could limit access to specific hosts, so that only network managers can configure the devices only by using specific network management workstations. Make sure you configure all VTY lines to use the same ACL.

Impact:

Organizations can reduce the risk of unauthorized access by implementing access-lists for all VTY lines. Conversely, using VTY lines without access-lists increases the risk of unauthorized access.

Audit:

Perform the following to determine if the ACL is created:
Verify the appropriate access-list definitions

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

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
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a2.html#GUID-9EA733A3-1788-4882-B8C3-AB0A2949120C

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.2.5 Set 'access-class' for 'line vty' (Automated)

Profile Applicability:

- Level 1

Description:

The 'access-class' setting restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the networking devices associated with addresses in an access list.

Rationale:

Restricting the type of network devices, associated with the addresses on the access-list, further restricts remote access to those devices authorized to manage the device and reduces the risk of unauthorized access.

Impact:

Applying 'access'class' to line VTY further restricts remote access to only those devices authorized to manage the device and reduces the risk of unauthorized access. Conversely, using VTY lines with 'access class' restrictions increases the risks of unauthorized access.

Audit:

Perform the following to determine if the ACL is set:
Verify you see the access-class defined

```
hostname#sh run | sec vty <line-number> <ending-line-number>
```

Remediation:

Configure remote management access control restrictions for all VTY lines.

```
hostname(config)#line vty <line-number> <ending-line-number>
hostname(config-line)# access-class <vty_acl_number> in
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a2.html#GUID-FB9BC58A-F00A-442A-8028-1E9E260E54D3

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.2.6 Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0' (Automated)

Profile Applicability:

- Level 1

Description:

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

Rationale:

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

Impact:

Organizations should prevent unauthorized use of unattended or abandoned sessions by an automated control. Enabling 'exec-timeout' with an appropriate length of minutes or seconds prevents unauthorized access of abandoned sessions.

Audit:

Perform the following to determine if the timeout is configured:
Verify you return a result NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname#sh run | sec line aux 0
```

Remediation:

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

```
hostname(config)#line aux 0
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.2.7 Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0' (Automated)

Profile Applicability:

- Level 1

Description:

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

Rationale:

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

Impact:

Organizations should prevent unauthorized use of unattended or abandoned sessions by an automated control. Enabling 'exec-timeout' with an appropriate length reduces the risk of unauthorized access of abandoned sessions.

Audit:

Perform the following to determine if the timeout is configured:
Verify you return a result NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname#sh run | sec line con 0
```

Remediation:

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

```
hostname(config)#line con 0
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.2.8 Set 'exec-timeout' less than or equal to 10 minutes 'line tty' (Automated)

Profile Applicability:

- Level 1

Description:

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

Rationale:

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

Impact:

Organizations should prevent unauthorized use of unattended or abandoned sessions by an automated control. Enabling 'exec-timeout' with an appropriate length reduces the risks of unauthorized access of abandoned sessions.

Audit:

Perform the following to determine if the timeout is configured:
Verify you return a result NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname#sh line tty <tty_line_number> | begin Timeout
```

Remediation:

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

```
hostname(config)#line tty {line_number} [ending_line_number]
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.2.9 Set 'exec-timeout' to less than or equal to 10 minutes 'line vty' (Automated)

Profile Applicability:

- Level 1

Description:

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

Rationale:

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

Impact:

Organizations should prevent unauthorized use of unattended or abandoned sessions by an automated control. Enabling 'exec-timeout' with an appropriate length of minutes or seconds prevents unauthorized access of abandoned sessions.

Audit:

Perform the following to determine if the timeout is configured:
Verify you return a result NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname#sh line vty <tty_line_number> | begin Timeout
```

Remediation:

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

```
hostname(config)#line vty {line_number} [ending_line_number]
hostname(config-line)#exec-timeout <<span>timeout_in_minutes>
<timeout_in_seconds</span>>
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.2.10 Set 'exec-timeout' to less than or equal to 10 minutes 'line vty' (Automated)

Profile Applicability:

- Level 1

Description:

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

Rationale:

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

Impact:

Organizations should prevent unauthorized use of unattended or abandoned sessions by an automated control. Enabling 'exec-timeout' with an appropriate length of minutes or seconds prevents unauthorized access of abandoned sessions.

Audit:

Perform the following to determine if the timeout is configured:
Verify you return a result NOTE: If you set an exec-timeout of 10 minutes, this will not show up in the configuration

```
hostname#sh line vty <tty_line_number> | begin Timeout
```

Remediation:

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

```
hostname(config)#line vty {line_number} [ending_line_number]
hostname(config-line)#exec-timeout <<span>timeout_in_minutes>
<timeout_in_seconds</span>>
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.2.11 Set 'transport input none' for 'line aux 0' (Automated)

Profile Applicability:

- Level 1

Description:

When you want to allow only an outgoing connection on a line, use the no exec command.

Rationale:

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

Impact:

Organizations should prevent all unauthorized access of auxiliary ports by disabling all protocols using the 'transport input none' command.

Audit:

Perform the following to determine if inbound connections for the aux port are disabled:
Verify you see the following "Allowed input transports are none

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

Remediation:

Disable the inbound connections on the auxiliary port.

```
hostname(config)#line aux 0
hostname(config-line)#transport input none
```

References:

1. http://www.cisco.com/en/US/docs/ios/termserv/command/reference/tsv_s1.html#wp1069219

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

1.3 Banner Rules

Rules in the banner class communicate legal rights to users.

1.3.1 Set the 'banner-text' for 'banner exec' (Manual)

Profile Applicability:

- Level 1

Description:

This command specifies a message to be displayed when an EXEC process is created (a line is activated, or an incoming connection is made to a vty). Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a router, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

Rationale:

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

- 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)

Impact:

Organizations provide appropriate legal notice(s) and warning(s) to persons accessing their networks by using a 'banner-text' for the banner exec command.

Audit:

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

```
hostname#sh running-config | beg banner exec
```

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

Remediation:

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

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

Default Value:

No banner is set by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/A_through_B.html#GUID-0DEF5B57-A7D9-4912-861F-E837C82A3881

Additional Information:

The default is no banner.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.3.2 Set the 'banner-text' for 'banner login' (Manual)

Profile Applicability:

- Level 1

Description:

Follow the banner login command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

Rationale:

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

- 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)

Impact:

Organizations provide appropriate legal notice(s) and warning(s) to persons accessing their networks by using a 'banner-text' for the banner login command.

Audit:

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

```
hostname#show running-config | beg banner login
```

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

Remediation:

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

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

Default Value:

No banner is set by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/A_through_B.html#GUID-FF0B6890-85B8-4B6A-90DD-1B7140C5D22F

CIS Controls:

Version 7

17 Implement a Security Awareness and Training Program
Implement a Security Awareness and Training Program

1.3.3 Set the 'banner-text' for 'banner motd' (Manual)

Profile Applicability:

- Level 1

Description:

This MOTD banner is displayed to all terminals connected and is useful for sending messages that affect all users (such as impending system shutdowns). Use the no exec-banner or no motd-banner command to disable the MOTD banner on a line. The no exec-banner command also disables the EXEC banner on the line.

When a user connects to the router, the MOTD banner appears before the login prompt. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

Rationale:

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

- 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)

Impact:

Organizations provide appropriate legal notice(s) and warning(s) to persons accessing their networks by using a 'banner-text' for the banner motd command.

Audit:

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

```
hostname#sh running-config | beg banner motd
```

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

Remediation:

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

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

Default Value:

No banner is set by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/A_through_B.html#GUID-7416C789-9561-44FC-BB2A-D8D8AFFB77DD

CIS Controls:

Version 7

17 Implement a Security Awareness and Training Program
Implement a Security Awareness and Training Program

1.4 Password Rules

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

1.4.1 Set 'password' for 'enable secret' (Automated)

Profile Applicability:

- Level 1

Description:

Use the enable secret command to provide an additional layer of security over the enable password. The enable secret command provides better security by storing the enable secret password using a nonreversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

Rationale:

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

Impact:

Organizations should protect privileged EXEC mode through policies requiring the 'enabling secret' setting, which enforces a one-way cryptographic hash (MD5).

Audit:

Perform the following to determine enable secret is set:
If the command does not return a result, the enable password is not set.

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

Remediation:

Configure a strong, enable secret password.

```
hostname(config)#enable secret {ENABLE_SECRET_PASSWORD}
```

Default Value:

No enable secret password setup by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-e1.html#GUID-944C261C-7D4A-49E1-AA8F-C754750BDE47

Additional Information:

Note: You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

CIS Controls:

Version 6

5.8 Administrators Should Not Directly Log In To A System (i.e. use RunAs/sudo)

Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

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

1.4.2 Enable 'service password-encryption' (Automated)

Profile Applicability:

- Level 1

Description:

When password encryption is enabled, the encrypted form of the passwords is displayed when a more system:running-config command is entered.

Rationale:

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

Impact:

Organizations implementing 'service password-encryption' reduce the risk of unauthorized users learning clear text passwords to Cisco IOS configuration files. However, the algorithm used is not designed to withstand serious analysis and should be treated like clear-text.

Audit:

Perform the following to determine if a user with an encrypted password is enabled:
Ensure a result that matches the command return

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

Remediation:

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

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

Default Value:

Service password encryption is not set by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s1.html#GUID-CC0E305A-604E-4A74-8A1A-975556CE5871

Additional Information:

Caution: This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note: You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

1.4.3 Set 'username secret' for all local users (Automated)

Profile Applicability:

- Level 1

Description:

Use the username secret command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The username secret command provides an additional layer of security over the username password. It also provides better security by encrypting the password using non reversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Rationale:

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

Impact:

Organizations implementing 'username secret' across their enterprise reduce the risk of unauthorized users gaining access to Cisco IOS devices by applying a MD5 hash and encrypting user passwords.

Audit:

Perform the following to determine if a user with an encrypted password is enabled:
If a result does not return with secret, the feature is not enabled

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

Remediation:

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

```
hostname(config)#username {{em}LOCAL_USERNAME{/em}} secret
{{em}LOCAL_PASSWORD{/em}}
```

Default Value:

No passwords are set by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-t2-z.html#GUID-5071E577-5249-4EA1-9226-BD426BEAD5B9

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

1.5 SNMP Rules

Simple Network Management Protocol (SNMP) provides a standards-based interface to manage and monitor network devices. This section provides guidance on the secure configuration of SNMP parameters.

The recommendations in this Section apply to Organizations using SNMP. Organizations using SNMP should review and implement the recommendations in this section.

1.5.1 Set 'no snmp-server' to disable SNMP when unused (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Impact:

Organizations not using SNMP should require all SNMP services to be disabled by running the 'no snmp-server' command.

Audit:

Verify the result reads "SNMP agent not enabled"

```
hostname#show snmp community
```

Remediation:

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

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

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-book.html

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5.2 Unset 'private' for 'snmp-server community' (Manual)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, Organizations should disable default, easy to guess, settings such as the 'private' setting for snmp-server community.

Audit:

Perform the following to determine if the public community string is enabled:
Ensure `private` does not show as a result

```
hostname# show snmp community
```

Remediation:

Disable the default SNMP community string "private"

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

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5.3 Unset 'public' for 'snmp-server community' (Manual)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, Organizations should disable default, easy to guess, settings such as the 'public' setting for snmp-server community.

Audit:

Perform the following to determine if the public community string is enabled: Ensure `public` does not show as a result

```
hostname# show snmp community
```

Remediation:

Disable the default SNMP community string "public"

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

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5.4 Do not set 'RW' for any 'snmp-server community' (Manual)

Profile Applicability:

- Level 1

Description:

Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.

Rationale:

Enabling SNMP read-write enables remote management of the device. Unless absolutely necessary, do not allow simple network management protocol (SNMP) write access.

Impact:

To reduce the risk of unauthorized access, Organizations should disable the SNMP 'write' access for snmp-server community.

Audit:

Perform the following to determine if a read/write community string is enabled:
Verify the result does not show a community string with a "RW"

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

Remediation:

Disable SNMP write access.

```
hostname(config)#no snmp-server community {<em>write_community_string</em>}
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5.5 Set the ACL for each 'snmp-server community' (Manual)

Profile Applicability:

- Level 1

Description:

This feature specifies a list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, Organizations should enable access control lists for all snmp-server communities and restrict the access to appropriate trusted management zones. If possible, implement SNMPv3 to apply authentication, authorization, and data privatization (encryption) for additional benefits to the organization.

Audit:

Perform the following to determine if an ACL is enabled:
Verify the result shows a number after the community string

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

Remediation:

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

```
hostname(config)#snmp-server community <<em>community_string</em>> ro
{<em>snmp_access-list_number |
<span>snmp_access-list_name</span></em><span>}</span>
```

Default Value:

No ACL is set for SNMP

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.5.6 Create an 'access-list' for use with SNMP (Manual)

Profile Applicability:

- Level 1

Description:

You can use access lists to control the transmission of packets on an interface, control Simple Network Management Protocol (SNMP) access, and restrict the contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

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.

Audit:

Perform the following to determine if the ACL is created:
Verify you the appropriate access-list definitions

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

Remediation:

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

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

Default Value:

SNMP does not use an access list.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a2.html#GUID-9EA733A3-1788-4882-B8C3-AB0A2949120C

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.5.7 Set 'snmp-server host' when using SNMP (Manual)

Profile Applicability:

- Level 1

Description:

SNMP notifications can be sent as traps to authorized management systems.

Rationale:

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

Impact:

Organizations using SNMP should restrict sending SNMP messages only to explicitly named systems to reduce unauthorized access.

Audit:

Perform the following to determine if SNMP traps are enabled:
If the command returns configuration values, then SNMP is enabled.

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

Remediation:

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

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

Default Value:

A recipient is not specified to receive notifications.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-D84B2AB5-6485-4A23-8C26-73E50F73EE61

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.5.8 Set 'snmp-server enable traps snmp' (Manual)

Profile Applicability:

- Level 1

Description:

SNMP notifications can be sent as traps to authorized management systems.

Rationale:

SNMP has the ability to submit traps .

Impact:

Organizations using SNMP should restrict trap types only to explicitly named traps to reduce unintended traffic. Enabling SNMP traps without specifying trap type will enable all SNMP trap types.

Audit:

Perform the following to determine if SNMP traps are enabled:
If the command returns configuration values, then SNMP is enabled.

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

Remediation:

Enable SNMP traps.

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

Default Value:

SNMP notifications are disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s3.html#GUID-EB3EB677-A355-42C6-A139-85BA30810C54

CIS Controls:

Version 6

11.7 Manage Network Infrastructure Using Segregation

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Version 7

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.5.9 Set 'priv' for each 'snmp-server group' using SNMPv3 (Manual)

Profile Applicability:

- Level 2

Description:

Specifies authentication of a packet with encryption when using SNMPv3

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages. When configuring a user for SNMPv3 you have the option of using a range of encryption schemes, or no encryption at all, to protect messages in transit. AES128 is the minimum strength encryption method that should be deployed.

Impact:

Organizations using SNMP can significantly reduce the risks of unauthorized access by using the 'snmp-server group v3 priv' setting to encrypt messages in transit.

Audit:

Verify the result show the appropriate group name and security model

```
hostname#show snmp group
```

Remediation:

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

```
hostname(config)#snmp-server group {<em>group_name</em>} v3 priv
```

Default Value:

No SNMP server groups are configured.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-56E87D02-C56F-4E2D-A5C8-617E31740C3F

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.5.10 Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3 (Manual)

Profile Applicability:

- Level 2

Description:

Specify the use of a minimum of 128-bit AES algorithm for encryption when using SNMPv3.

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages. When configuring a user for SNMPv3 you have the option of using a range of encryption schemes, or no encryption at all, to protect messages in transit. AES128 is the minimum strength encryption method that should be deployed.

Impact:

Organizations using SNMP can significantly reduce the risks of unauthorized access by using the 'snmp-server user' setting with appropriate authentication and privacy protocols to encrypt messages in transit.

Audit:

Verify the result show the appropriate user name and security settings

```
hostname#show snmp user
```

Remediation:

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

```
hostname(config)#snmp-server user {user_name} {group_name} v3 auth sha
{auth_password} priv aes 128 {priv_password} {acl_name_or_number}
```

Default Value:

SNMP username as not set by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-4EED4031-E723-4B84-9BBF-610C3CF60E31

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

2 Control Plane

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.

2.1 Global Service Rules

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

2.1.1 Setup SSH

Ensure use of SSH remote console sessions to Cisco routers.

2.1.1.1 Configure Prerequisites for the SSH Service

[This space intentionally left blank]

2.1.1.1.1 Set the 'hostname' (Automated)

Profile Applicability:

- Level 1

Description:

The hostname is used in prompts and default configuration filenames.

Rationale:

The domain name is prerequisite for setting up SSH.

Impact:

Organizations should plan the enterprise network and identify an appropriate host name for each router.

Audit:

Perform the following to determine if the local time zone is configured:
Verify the result shows the summer-time recurrence is configured properly.

```
hostname#sh run | incl hostname
```

Remediation:

Configure an appropriate host name for the router.

```
hostname(config)#hostname {<em>router_name</em>}
```

Default Value:

The default hostname is Router.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/F_through_K.html#GUID-F3349988-EC16-484A-BE81-4C40110E6625

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

2.1.1.1.2 Set the 'ip domain-name' (Automated)

Profile Applicability:

- Level 1

Description:

Define a default domain name that the Cisco IOS software uses to complete unqualified hostnames

Rationale:

The domain name is a prerequisite for setting up SSH.

Impact:

Organizations should plan the enterprise network and identify an appropriate domain name for the router.

Audit:

Perform the following to determine if the domain name is configured:
Verify the domain name is configured properly.

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

Remediation:

Configure an appropriate domain name for the router.

```
hostname (config)#ip domain-name {<em>domain-name</em>}
```

Default Value:

No domain is set.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-i3.html#GUID-A706D62B-9170-45CE-A2C2-7B2052BE2CAB

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

2.1.1.1.3 Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa' (Manual)

Profile Applicability:

- Level 1

Description:

Use this command to generate RSA key pairs for your Cisco device.

RSA keys are generated in pairs--one public RSA key and one private RSA key.

Rationale:

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

NOTE: IOS does NOT display the modulus bit value in the Audit Procedure.

Impact:

Organizations should plan and implement enterprise network cryptography and generate an appropriate RSA key pairs, such as 'modulus', greater than or equal to 2048.

Audit:

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

```
 hostname#sh crypto key mypubkey rsa
```

Remediation:

Generate an RSA key pair for the router.

```
hostname(config)#crypto key generate rsa general-keys modulus <em>2048</em>
```

Default Value:

RSA key pairs do not exist.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-c4.html#GUID-2AECF701-D54A-404E-9614-D3AAB049BC13

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

2.1.1.1.4 Set 'seconds' for 'ip ssh timeout' (Manual)

Profile Applicability:

- Level 1

Description:

The time interval that the router waits for the SSH client to respond before disconnecting an uncompleted login attempt.

Rationale:

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

Impact:

Organizations should implement a security policy requiring minimum timeout settings for all network administrators and enforce the policy through the 'ip ssh timeout' command.

Audit:

Perform the following to determine if the SSH timeout is configured:
Verify the timeout is configured properly.

```
hostname#sh ip ssh
```

Remediation:

Configure the SSH timeout

```
hostname(config)#ip ssh time-out [<em>60</em>]
```

Default Value:

SSH in not enabled by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i3.html#GUID-5BAC7A2B-0A25-400F-AEE9-C22AE08513C6

Additional Information:

This cannot exceed 120 seconds.

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

2.1.1.1.5 Set maximimum value for 'ip ssh authentication-retries' (Automated)

Profile Applicability:

- Level 1

Description:

The number of retries before the SSH login session disconnects.

Rationale:

This limits the number of times an unauthorized user can attempt a password without having to establish a new SSH login attempt. This reduces the potential for success during online brute force attacks by limiting the number of login attempts per SSH connection.

Impact:

Organizations should implement a security policy limiting the number of authentication attempts for network administrators and enforce the policy through the 'ip ssh authentication-retries' command.

Audit:

Perform the following to determine if SSH authentication retries is configured:
Verify the authentication retries is configured properly.

```
hostname#sh ip ssh
```

Remediation:

Configure the SSH timeout:

```
hostname(config)#ip ssh authentication-retries [<em>3</em>]
```

Default Value:

SSH is not enabled by default. When set, the default value is 3.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i3.html#GUID-5BAC7A2B-0A25-400F-AEE9-C22AE08513C6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

2.1.1.2 Set version 2 for 'ip ssh version' (Automated)

Profile Applicability:

- Level 1

Description:

Specify the version of Secure Shell (SSH) to be run on a router

Rationale:

SSH Version 1 has been subject to a number of serious vulnerabilities and is no longer considered to be a secure protocol, resulting in the adoption of SSH Version 2 as an Internet Standard in 2006.

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

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy to review their current protocols to ensure the most secure protocol versions are in use.

Audit:

Perform the following to determine if SSH version 2 is configured:
Verify that SSH version 2 is configured properly.

```
hostname#sh ip ssh
```

Remediation:

Configure the router to use SSH version 2

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

Default Value:

SSH is not enabled by default. When enabled, SSH operates in compatibility mode (versions 1 and 2 supported).

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i3.html#GUID-170AECF1-4B5B-462A-8CC8-999DEDC45C21

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

2.1.2 Set 'no cdp run' (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in network monitoring and troubleshooting situations but is considered a security risk because of the amount of information provided from queries. In addition, there have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless necessary.

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting network protocols and explicitly require disabling all insecure or unnecessary protocols.

Audit:

Perform the following to determine if CDP is enabled:
Verify the result shows "CDP is not enabled"

```
hostname#show cdp
```

Remediation:

Disable Cisco Discovery Protocol (CDP) service globally.

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

Default Value:

Enabled on all platforms except the Cisco 10000 Series Edge Services Router

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/cdp/command/cdp-cr-a1.html#GUID-E006FAC8-417E-4C3F-B732-4D47B0447750

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.3 Set 'no ip bootp server' (Manual)

Profile Applicability:

- Level 1

Description:

Disable the Bootstrap Protocol (BOOTP) service on your routing device.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting network protocols and explicitly require disabling all insecure or unnecessary protocols such as 'ip bootp server'.

Audit:

Perform the following to determine if bootp is enabled:
Verify a "no ip bootp server" result returns

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

Remediation:

Disable the bootp server.

```
hostname(config)#ip dhcp bootp ignore
```

Default Value:

Enabled

References:

1. Cisco IOS software receives Cisco Discovery Protocol information

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.4 Set 'no service dhcp' (Automated)

Profile Applicability:

- Level 1

Description:

Disable the Dynamic Host Configuration Protocol (DHCP) server and relay agent features on your router.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting network protocols and explicitly require disabling all insecure or unnecessary protocols such as the Dynamic Host Configuration Protocol (DHCP).

Audit:

Perform the following to determine if the DHCP service is enabled:
Verify no result returns

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

Remediation:

Disable the DHCP server.

```
hostname(config)#<strong>no service dhcp</strong>
```

Default Value:

Enabled by default, but also requires a DHCP pool to be set to activate the DHCP server.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-1516B259-AA28-4839-B968-8DDBF0B382F6

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.5 Set 'no ip identd' (Automated)

Profile Applicability:

- Level 1

Description:

Disable the identification (identd) server.

Rationale:

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

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting network protocols and explicitly require disabling all insecure or unnecessary protocols such as the identification protocol (identd).

Audit:

Perform the following to determine if identd is enabled:
Verify no result returns

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

Remediation:

Disable the ident server.

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

Default Value:

Disabled by default

References:

1. http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap4.html#wp1056539

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.6 Set 'service tcp-keepalives-in' (Automated)

Profile Applicability:

- Level 1

Description:

Generate keepalive packets on idle incoming network connections.

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 connection is closed within five minutes if no keepalives are received or immediately if the host replies with a reset packet.

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting how long to allow terminated sessions and enforce this policy through the use of 'tcp-keepalives-in' command.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

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

Remediation:

Enable TCP keepalives-in service:

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

Default Value:

Disabled by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/R_through_setup.html#GUID-1489ABA3-2428-4A64-B252-296A035DB85E

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.7 Set 'service tcp-keepalives-out' (Automated)

Profile Applicability:

- Level 1

Description:

Generate keepalive packets on idle outgoing network connections.

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.

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting how long to allow terminated sessions and enforce this policy through the use of 'tcp-keepalives-out' command.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

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

Remediation:

Enable TCP keepalives-out service:

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

Default Value:

Disabled by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/R_through_setup.html#GUID-9321ECDC-6284-4BF6-BA4A-9CEEF5F993E5

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

2.1.8 Set 'no service pad' (Automated)

Profile Applicability:

- Level 1

Description:

Disable X.25 Packet Assembler/Disassembler (PAD) service.

Rationale:

If the PAD service is not necessary, disable the service to prevent intruders from accessing the X.25 PAD command set on the router.

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting unnecessary services such as the 'PAD' service.

Audit:

Perform the following to determine if the feature is disabled:
Verify no result returns

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

Remediation:

Disable the PAD service.

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

Default Value:

Enabled by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/wan/command/wan-s1.html#GUID-C5497B77-3FD4-4D2F-AB08-1317D5F5473B

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.2 Logging Rules

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

2.2.1 Set 'logging on' (Manual)

Profile Applicability:

- Level 1

Description:

Enable logging of system messages.

Rationale:

Logging provides a chronological record of activities on the Cisco device and allows monitoring of both operational and security related events.

Impact:

Enabling the Cisco IOS 'logging on' command enforces the monitoring of technology risks for the organizations' network devices.

Audit:

Perform the following to determine if the feature is enabled:
Verify no result returns

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

Remediation:

Enable system logging.

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

Default Value:

Logging is not enabled/

References:

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#wp1014324

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.2 Set 'buffer size' for 'logging buffered' (Automated)

Profile Applicability:

- Level 1

Description:

Enable system message logging to a local 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.

Impact:

Data forensics is effective for managing technology risks and an organization can enforce such policies by enabling the 'logging buffered' command.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

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

Remediation:

Configure buffered logging (with minimum size). Recommended size is 64000.

```
hostname(config)#logging buffered [<em>log_buffer_size</em>]
```

Default Value:

No logging buffer is set by default

References:

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#wp1060051

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.3 Set 'logging console critical' (Automated)

Profile Applicability:

- Level 1

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.

Impact:

Logging critical messages at the console is important for an organization managing technology risk. The 'logging console' command should capture appropriate severity messages to be effective.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

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

Remediation:

Configure console logging level.

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

Default Value:

Tthe default is to log all messages

Additional Information:

The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.4 Set IP address for 'logging host' (Automated)

Profile Applicability:

- Level 1

Description:

Log system messages and debug output to a remote host.

Rationale:

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

Impact:

Logging is an important process for an organization managing technology risk. The 'logging host' command sets the IP address of the logging host and enforces the logging process.

Audit:

Perform the following to determine if a syslog server is enabled:
Verify one or more IP address(es) returns

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

Remediation:

Designate one or more syslog servers by IP address.

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

Default Value:

System logging messages are not sent to any remote host.

References:

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#wp1082864

CIS Controls:

Version 6

6.6 Deploy A SIEM OR Log Analysis Tools For Aggregation And Correlation/Analysis

Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Version 7

6.6 Deploy SIEM or Log Analytic tool

Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.8 Regularly Tune SIEM

On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

2.2.5 Set 'logging trap informational' (Manual)

Profile Applicability:

- Level 1

Description:

Limit messages logged to the syslog servers based on severity level informational.

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.

Impact:

Logging is an important process for an organization managing technology risk. The 'logging trap' command sets the severity of messages and enforces the logging process.

Audit:

Perform the following to determine if a syslog server for SNMP traps is enabled:
Verify "level informational" returns

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

Remediation:

Configure SNMP trap and syslog logging level.

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

Default Value:

Disabled

References:

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#wp1015177

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.6 Set 'service timestamps debug datetime' (Automated)

Profile Applicability:

- Level 1

Description:

Configure the system to apply a time stamp to debugging messages or system logging messages

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.

Impact:

Logging is an important process for an organization managing technology risk and establishing a timeline of events is critical. The 'service timestamps' command sets the date and time on entries sent to the logging host and enforces the logging process.

Audit:

Perform the following to determine if the additional detail is enabled:
Verify a command string result returns

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

Remediation:

Configure debug messages to include timestamps.

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

Default Value:

Time stamps are applied to debug and logging messages.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/R_through_setup.html#GUID-DC110E59-D294-4E3D-B67F-CCB06E607FC6

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.2.7 Set 'logging source interface' (Automated)

Profile Applicability:

- Level 1

Description:

Specify the source IPv4 or IPv6 address of system logging packets

Rationale:

This is required so that the router sends log messages to the logging server from a consistent IP address.

Impact:

Logging is an important process for an organization managing technology risk and establishing a consistent source of messages for the logging host is critical. The 'logging source interface loopback' command sets a consistent IP address to send messages to the logging host and enforces the logging process.

Audit:

Perform the following to determine if logging services are bound to a source interface: Verify a command string result returns

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

Remediation:

Bind logging to the loopback interface.

```
hostname(config)#logging source-interface loopback
{<em>loopback_interface_number</em>}
```

Default Value:

The wildcard interface address is used.

References:

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#wp1095099

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.3 NTP Rules

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

2.3.1 Require Encryption Keys for NTP

Encryption keys should be set for NTP Servers.

2.3.1.1 Set 'ntp authenticate' (Automated)

Profile Applicability:

- Level 2

Description:

Enable NTP authentication.

Rationale:

Using authenticated NTP ensures the Cisco device only permits time updates from authorized NTP servers.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp authenticate' command enforces authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

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

Remediation:

Configure NTP authentication:

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

Default Value:

NTP authentication is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-8BEBDAF4-6D03-4C3E-B8D6-6BCBC7D0F324

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.3.1.2 Set 'ntp authentication-key' (Automated)

Profile Applicability:

- Level 2

Description:

Define an authentication key for Network Time Protocol (NTP).

Rationale:

Using an authentication key provides a higher degree of security as only authenticated NTP servers will be able to update time for the Cisco device.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp authentication-key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

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

Remediation:

Configure at the NTP key ring and encryption key using the following command

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

Default Value:

No authentication key is defined for NTP.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-0435BFD1-D7D7-41D4-97AC-7731C11226BC

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.3.1.3 Set the 'ntp trusted-key' (Automated)

Profile Applicability:

- Level 2

Description:

Ensure you authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize

Rationale:

This authentication function provides protection against accidentally synchronizing the system to another system that is not trusted, because the other system must know the correct authentication key.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp trusted-key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

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

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

Remediation:

Configure the NTP trusted key using the following command

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

Default Value:

Authentication of the identity of the system is disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-89CA798D-0F12-4AE8-B382-DE10CBD261DB

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.3.1.4 Set 'key' for each 'ntp server' (Manual)

Profile Applicability:

- Level 2

Description:

Specifies the authentication key for NTP.

Rationale:

This authentication feature provides protection against accidentally synchronizing the ntp system to another system that is not trusted, because the other system must know the correct authentication key.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp server key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

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

Remediation:

Configure each NTP Server to use a key ring using the following command.

```
hostname(config)#ntp server {<em>ntp-server_ip_address</em>}{key
<em>ntp_key_id</em>}
```

Default Value:

No NTP key is set by default

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.3.2 Set 'ip address' for 'ntp server' (Automated)

Profile Applicability:

- Level 1

Description:

Use this command if you want to allow the system to synchronize the system software clock with the specified NTP server.

Rationale:

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

Ensure you also configure consistent timezone and daylight savings time setting for all devices. For simplicity, the default of Coordinated Universal Time (UTC).

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp server ip address' enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
hostname#sh ntp associations
```

Remediation:

Configure at least one external NTP Server using the following commands

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

Default Value:

No servers are configured by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-255145EB-D656-43F0-B361-D9CBCC794112

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.4 Loopback Rules

When a router needs to initiate connections to remote hosts, for example for SYSLOG or NTP, it will use the nearest interface for the packets source address. This can cause issues due to the possible variation in source, potentially causing packets to be denied by intervening firewalls or handled incorrectly by the receiving host. To prevent these problems the router should be configured with a Loopback interface and any services should be bound to this address.

2.4.1 Create a single 'interface loopback' (Automated)

Profile Applicability:

- Level 2

Description:

Configure a single loopback interface.

Rationale:

Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms.

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

Impact:

Organizations should plan and establish 'loopback interfaces' for the enterprise network. Loopback interfaces enable critical network information such as OSPF Router IDs and provide termination points for routing protocol sessions.

Audit:

Perform the following to determine if a loopback interface is defined:
Verify an IP address returns for the defined loopback interface

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

Remediation:

Define and configure one loopback interface.

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

Default Value:

There are no loopback interfaces defined by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.4.2 Set AAA 'source-interface' (Automated)

Profile Applicability:

- Level 2

Description:

Force AAA to use the IP address of a specified interface for all outgoing AAA packets

Rationale:

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

Impact:

Organizations should design and implement authentication, authorization, and accounting (AAA) services for effective monitoring of enterprise network devices. Binding AAA services to the source-interface loopback enables these services.

Audit:

Perform the following to determine if AAA services are bound to a source interface:
Verify a command string result returns

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

Remediation:

Bind AAA services to the loopback interface.

```
Hostname(config)#ip radius source-interface loopback
{loopback_interface_number}
or
Hostname(config)#aaa group server tacacs+ {group name} hostname(config-sg-
tacacs+)#ip tacacs source-interface {loopback_interface_number}
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i2.html#GUID-22E8B211-751F-48E0-9C76-58F0FE0AABA8
2. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i3.html#GUID-54A00318-CF69-46FC-9ADC-313BFC436713

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

2.4.3 Set 'ntp source' to Loopback Interface (Automated)

Profile Applicability:

- Level 2

Description:

Use a particular source address in Network Time Protocol (NTP) packets.

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.

Impact:

Organizations should plan and implement network time protocol (NTP) services to establish official time for all enterprise network devices. Setting 'ntp source loopback' enforces the proper IP address for NTP services.

Audit:

Perform the following to determine if NTP services are bound to a source interface:
Verify a command string result returns

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

Remediation:

Bind the NTP service to the loopback interface.

```
hostname(config)#ntp source loopback {<em>loopback_interface_number}</em>
```

Default Value:

Source address is determined by the outgoing interface.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-DF29FBFB-E1C0-4E5C-9013-D4CE59CA0B88

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

2.4.4 Set 'ip tftp source-interface' to the Loopback Interface (Automated)

Profile Applicability:

- Level 2

Description:

Specify the IP address of an interface as the source address for TFTP connections.

Rationale:

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

Impact:

Organizations should plan and implement trivial file transfer protocol (TFTP) services in the enterprise by setting 'tftp source-interface loopback', which enables the TFTP servers to identify routers and authenticate requests by IP address.

Audit:

Perform the following to determine if TFTP services are bound to a source interface:
Verify a command string result returns

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

Remediation:

Bind the TFTP client to the loopback interface.

```
hostname(config)#ip tftp source-interface loopback
{<em>loobpback_interface_number</em>}
```

Default Value:

The address of the closest interface to the destination is selected as the source address.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/F_through_K.html#GUID-9AA27050-A578-47CD-9F1D-5A8E2B449209

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3 Data Plane

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

3.1 Routing Rules

Unneeded services should be disabled.

3.1.1 Set 'no ip source-route' (Automated)

Profile Applicability:

- Level 1

Description:

Disable the handling of IP datagrams with source routing header options.

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.

Impact:

Organizations should plan and implement network policies to ensure unnecessary services are explicitly disabled. The 'ip source-route' feature has been used in several attacks and should be disabled.

Audit:

Verify the command string result returns

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

Remediation:

Disable source routing.

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

Default Value:

Enabled by default

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-i4.html#GUID-C7F971DD-358F-4B43-9F3E-244F5D4A3A93

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.2 Set 'no ip proxy-arp' (Automated)

Profile Applicability:

- Level 2

Description:

Disable proxy ARP on all interfaces.

Rationale:

Address Resolution Protocol (ARP) provides resolution between IP and MAC Addresses (or other Network and Link Layer addresses on none IP networks) within a Layer 2 network.

Proxy ARP is a service where a device connected to one network (in this case the Cisco router) answers ARP Requests which are addressed to a host on another network, replying with its own MAC Address and forwarding the traffic on to the intended host.

Sometimes used for extending broadcast domains across WAN links, in most cases Proxy ARP on enterprise networks is used to enable communication for hosts with mis-configured subnet masks, a situation which should no longer be a common problem. Proxy ARP effectively breaks the LAN Security Perimeter, extending a network across multiple Layer 2 segments. Using Proxy ARP can also allow other security controls such as PVLAN to be bypassed.

Impact:

Organizations should plan and implement network policies to ensure unnecessary services are explicitly disabled. The 'ip proxy-arp' feature effectively breaks the LAN security perimeter and should be disabled.

Audit:

Verify the proxy ARP status

```
hostname#sh ip int {<em>interface</em>} | incl proxy-arp
```

Remediation:

Disable proxy ARP on all interfaces.

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

Default Value:

Enabled

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-i4.html#GUID-AEB7DDCB-7B3D-4036-ACF0-0A0250F3002E

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.1.3 Set 'no interface tunnel' (Automated)

Profile Applicability:

- Level 2

Description:

Verify no tunnel interfaces are defined.

Rationale:

Tunnel interfaces should not exist in general. They can be used for malicious purposes. If they are necessary, the network admin's should be well aware of them and their purpose.

Impact:

Organizations should plan and implement enterprise network security policies that disable insecure and unnecessary features that increase attack surfaces such as 'tunnel interfaces'.

Audit:

Verify no tunnel interfaces are defined

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

Remediation:

Remove any tunnel interfaces.

```
hostname(config)#no interface tunnel {<em>instance</em>}
```

Default Value:

No tunnel interfaces are defined

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.1.4 Set 'ip verify unicast source reachable-via' (Manual)

Profile Applicability:

- Level 2

Description:

Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).

Rationale:

Enabled uRPF helps mitigate IP spoofing by ensuring only packet source IP addresses only originate from expected interfaces. Configure unicast reverse-path forwarding (uRPF) on all external or high risk interfaces.

Impact:

Organizations should plan and implement enterprise security policies that protect the confidentiality, integrity, and availability of network devices. The 'unicast Reverse-Path Forwarding' (uRPF) feature dynamically uses the router table to either accept or drop packets when arriving on an interface.

Audit:

Verify uRPF is running on the appropriate interface(s)

```
hostname#sh ip int {<em>interface</em>} | incl verify source
```

Remediation:

Configure uRPF.

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

Default Value:

Unicast RPF is disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i3.html#GUID-2ED313DB-3D3F-49D7-880A-047463632757

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.2 Border Router Filtering

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.

3.2.1 Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks (Manual)

Profile Applicability:

- Level 2

Description:

This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the deny and permit commands.

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).

Ensure the `permit` rule(s) above the final `deny` rule only allow traffic according to your organization's least privilege policy.

Impact:

Organizations should plan and implement enterprise security policies that explicitly separate internal from external networks. Adding 'ip access-list' explicitly permitting and denying internal and external networks enforces these policies.

Audit:

Verify you have the appropriate access-list definitions

```
hostname#sh ip access-list {<em>name | number</em>}
```

Remediation:

Configure ACL for private source address restrictions from external networks.

```
hostname(config)#ip access-list extended {<span><em>name | number</em>}
</span><span>hostname(config-nacl)#deny ip
{</span><em>internal_networks</em>} any log
hostname(config<span>-nacl</span>)#deny ip 127.0.0.0 0.255.255.255 any log
hostname(config<span>-nacl</span>)#deny ip 10.0.0.0 0.255.255.255 any log
hostname(config<span>-nacl</span>)#deny ip 0.0.0.0 0.255.255.255 any log
```

```
hostname(config<span>-nacl</span>)#deny ip 172.16.0.0 0.15.255.255 any log
hostname(config<span>-nacl</span>)#deny ip 192.168.0.0 0.0.255.255 any log
hostname(config<span>-nacl</span>)#deny ip 192.0.2.0 0.0.0.255 any log
hostname(config<span>-nacl</span>)#deny ip 169.254.0.0 0.0.255.255 any log
hostname(config<span>-nacl</span>)#deny ip 224.0.0.0 31.255.255.255 any log
hostname(config<span>-nacl</span>)#deny ip host 255.255.255.255 any log
hostname(config<span>-nacl</span>)#permit {protocol} {source_ip}
{source_mask} {destination} {destination_mask} log
hostname(config<span>-nacl</span>)#deny any any log
hostname(config)#interface <external_<em>interface</em>>
hostname(config-if)#access-group <<em>access-list</em>> in
```

Default Value:

No access list defined

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i1.html#GUID-BD76E065-8EAC-4B32-AF25-04BA94DD2B11

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.2.2 Set inbound 'ip access-group' on the External Interface (Manual)

Profile Applicability:

- Level 2

Description:

This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the deny and permit commands.

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).

Ensure the `permit` rule(s) above the final `deny` rule only allow traffic according to your organization's least privilege policy.

Impact:

Organizations should plan and implement enterprise security policies explicitly permitting and denying access based upon access lists. Using the 'ip access-group' command enforces these policies by explicitly identifying groups permitted access.

Audit:

Verify the access-group is applied to the appropriate interface

```
hostname#sh run | sec interface {<em>external_interface</em>}
```

Remediation:

Apply the access-group for the external (untrusted) interface

```
hostname(config)#interface {external_interface}
hostname(config-if)#ip access-group {name | number} in
```

Default Value:

No access-group defined

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i1.html#GUID-D9FE7E44-7831-4C64-ACB8-840811A0C993

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3 Neighbor Authentication

Enable routing authentication.

3.3.1 Require EIGRP Authentication if Protocol is Used

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

3.3.1.1 Set 'key chain' (Manual)

Profile Applicability:

- Level 2

Description:

Define an authentication key chain to enable authentication for routing protocols. A key chain must have at least one key and can have up to 2,147,483,647 keys.

NOTE: Only DRP Agent, EIGRP, and RIPv2 use key chains.

Rationale:

Routing protocols such as DRP Agent, EIGRP, and RIPv2 use key chains for authentication.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'key chains' for routing protocols enforces these policies.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Establish the key chain.

```
hostname(config)#key chain {<em>key-chain_name</em>}
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-A62E89F5-0B8B-4CF0-B4EB-08F2762D88BB

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.2 Set 'key' (Manual)

Profile Applicability:

- Level 2

Description:

Configure an authentication key on a key chain.

Rationale:

This is part of the routing authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'key numbers' for key chains for routing protocols enforces these policies.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Configure the key number.

```
hostname(config-keychain)#key {<em>key-number</em>}
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-3F31B2E0-0E4B-4F49-A4A8-8ADA1CA0D73F

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.3 Set 'key-string' (Manual)

Profile Applicability:

- Level 2

Description:

Configure the authentication string for a key.

Rationale:

This is part of the routing authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'key strings' for key chains for routing protocols enforces these policies.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Configure the key string.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-D7A8DC18-2E16-4EA5-8762-8B68B94CC43E

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.4 Set 'address-family ipv4 autonomous-system' (Manual)

Profile Applicability:

- Level 2

Description:

Configure the EIGRP address family.

Rationale:

Rationale: EIGRP is a true multi-protocol routing protocol and the 'address-family' feature enables restriction of exchanges with specific neighbors

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'address-family' for EIGRP enforces these policies by restricting the exchanges between predefined network devices.

Audit:

Verify the appropriate address family is set

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

Remediation:

Configure the EIGRP address family.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-67388D6C-AE9C-47CA-8C35-2A2CF9FA668E
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-C03CFC8A-3CE3-4CF9-9D65-52990DBD3377

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.5 Set 'af-interface default' (Manual)

Profile Applicability:

- Level 2

Description:

Defines user defaults to apply to EIGRP interfaces that belong to an address-family.

Rationale:

Part of the EIGRP address-family setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'af-interface default' for EIGRP interfaces enforces these policies by restricting the exchanges between predefined network devices.

Audit:

Verify the setting

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

Remediation:

Configure the EIGRP address family.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-67388D6C-AE9C-47CA-8C35-2A2CF9FA668E
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-C03CFC8A-3CE3-4CF9-9D65-52990DBD3377
3. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-DC0EF1D3-DFD4-45DF-A553-FA432A3E7233

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.6 Set 'authentication key-chain' (Manual)

Profile Applicability:

- Level 2

Description:

Configure the EIGRP address family key chain.

Rationale:

This is part of the EIGRP authentication configuration

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using the address-family 'key chain' for EIGRP enforces these policies by restricting the exchanges between predefined network devices.

Audit:

Verify the appropriate key chain is set

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

Remediation:

Configure the EIGRP address family key chain.

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

Default Value:

No key chains are specified for EIGRP

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-67388D6C-AE9C-47CA-8C35-2A2CF9FA668E
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-C03CFC8A-3CE3-4CF9-9D65-52990DBD3377
3. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-6B6ED6A3-1AAA-4EFA-B6B8-9BF11EEC37A0

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.7 Set 'authentication mode md5' (Manual)

Profile Applicability:

- Level 2

Description:

Configure authentication to prevent unapproved sources from introducing unauthorized or false service messages.

Rationale:

This is part of the EIGRP authentication configuration

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using the 'authentication mode' for EIGRP address-family or service-family packets enforces these policies by restricting the type of authentication between network devices.

Audit:

Verify the appropriate address family authentication mode is set

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

Remediation:

Configure the EIGRP address family authentication mode.

```
hostname(config)#router eigrp <virtual-instance-name>
hostname(config-router)#address-family ipv4 autonomous-system {eigrp_as-
number}
hostname(config-router-af)#af-interface {interface-name}
hostname(config-router-af-interface)#authentication mode md5
```

Default Value:

Not defined

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-67388D6C-AE9C-47CA-8C35-2A2CF9FA668E
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-C03CFC8A-3CE3-4CF9-9D65-52990DBD3377
3. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-a1.html#GUID-A29E0EF6-4CEF-40A7-9824-367939001B73

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.8 Set 'ip authentication key-chain eigrp' (Manual)

Profile Applicability:

- Level 2

Description:

Specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets per interface.

Rationale:

Configuring EIGRP authentication key-chain number and name to restrict packet exchanges between network devices.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the interface with 'ip authentication key chain' for EIGRP by name and number enforces these policies by restricting the exchanges between network devices.

Audit:

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

```
hostname#sh ip eigrp int
hostname#sh run int {<em>interface_name</em>} | incl key-chain
```

Remediation:

Configure the interface with the EIGRP key chain.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-0B344B46-5E8E-4FE2-A3E0-D92410CE5E91

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.1.9 Set 'ip authentication mode eigrp' (Manual)

Profile Applicability:

- Level 2

Description:

Configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages.

Rationale:

This is part of the EIGRP authentication configuration

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the interface with 'ip authentication mode' for EIGRP by number and mode enforces these policies by restricting the exchanges between network devices.

Audit:

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

```
hostname#sh ip eigrp int
hostname#sh run int {<em>interface_name</em>} | incl authentication mode
```

Remediation:

Configure the interface with the EIGRP authentication mode.

```
hostname(config)#interface {<em>interface_name</em>}
hostname(config-if)#ip authentication mode eigrp {<em><span>eigrp_as-
number</span></em><span>}</span> md5
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/command/ire-i1.html#GUID-8D1B0697-8E96-4D8A-BD20-536956D68506

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.2 Require OSPF Authentication if Protocol is Used

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

3.3.2.1 Set 'authentication message-digest' for OSPF area (Manual)

Profile Applicability:

- Level 2

Description:

Enable MD5 authentication for OSPF.

Rationale:

This is part of the OSPF authentication setup.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the area 'authentication message-digest' for OSPF enforces these policies by restricting exchanges between network devices.

Audit:

Verify message digest for OSPF is defined

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

Remediation:

Configure the Message Digest option for OSPF.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/ospf-i1.html#GUID-3D5781A3-F8DF-4760-A551-6A3AB80A42ED
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/ospf-a1.html#GUID-81D0F753-D8D5-494E-9A10-B15433CFD445

Additional Information:

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.2.2 Set 'ip ospf message-digest-key md5' (Manual)

Profile Applicability:

- Level 2

Description:

Enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication.

Rationale:

This is part of the OSPF authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the proper interface(s) for 'ip ospf message-digest-key md5' enforces these policies by restricting exchanges between network devices.

Audit:

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

```
hostname#sh run int {<em>interface</em>}
```

Remediation:

Configure the appropriate interface(s) for Message Digest authentication

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/ospf-i1.html#GUID-939C79FF-8C09-4D5A-AEB5-DAF25038CA18

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.3 Require RIPv2 Authentication if Protocol is Used

Routing Information Protocol is a distance vector protocol used for interior gateway routing on some networks.

RIP is a complex protocol, with many configuration options which may have effects which are not immediately obvious.

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

3.3.3.1 Set 'key chain' (Manual)

Profile Applicability:

- Level 2

Description:

Define an authentication key chain to enable authentication for RIPv2 routing protocols.

Rationale:

This is part of the routing authentication process.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the proper authentication 'key-chain (name)' for RIPv2 protocols enforces these policies by restricting acceptable authentication between network devices.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Establish the key chain.

```
hostname(config)#key chain {<em>rip_key-chain_name</em>}
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-A62E89F5-0B8B-4CF0-B4EB-08F2762D88BB

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.3.2 Set 'key' (Manual)

Profile Applicability:

- Level 2

Description:

Configure an authentication key on a key chain.

Rationale:

This is part of the routing authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the proper authentication 'key' for RIPv2 protocols enforces these policies by restricting acceptable authentication between network devices.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Configure the key number.

```
hostname(config-keychain)#key {<em>key-number</em>}
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-3F31B2E0-0E4B-4F49-A4A8-8ADA1CA0D73F

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.3.3 Set 'key-string' (Manual)

Profile Applicability:

- Level 2

Description:

Configure the authentication string for a key.

Rationale:

This is part of the routing authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'key-string' for key chains for routing protocols enforces these policies.

Audit:

Verify the appropriate key chain is defined

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

Remediation:

Configure the key string.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/command/iri-cr-a1.html#GUID-D7A8DC18-2E16-4EA5-8762-8B68B94CC43E

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.3.4 Set 'ip rip authentication key-chain' (Manual)

Profile Applicability:

- Level 2

Description:

Enable authentication for Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface.

Rationale:

This is part of the RIPv2 authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the interface with 'ip rip authentication key-chain' by name enforces these policies by restricting the exchanges between network devices.

Audit:

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

```
hostname#sh run int {<em>interface_name</em>}
```

Remediation:

Configure the Interface with the RIPv2 key chain.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_rip/command/irr-cr-rip.html#GUID-C1C84D0D-4BD0-4910-911A-ADAB458D0A84

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.3.5 Set 'ip rip authentication mode' to 'md5' (Manual)

Profile Applicability:

- Level 2

Description:

Configure the Interface with the RIPv2 key chain.

Rationale:

This is part of the RIPv2 authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using the 'ip rip authentication mode md5' enforces these policies by restricting the type of authentication between network devices.

Audit:

Verify the appropriate mode is set on the appropriate interface(s)

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

Remediation:

Configure the RIPv2 authentication mode on the necessary interface(s)

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_rip/command/irr-cr-rip.html#GUID-47536344-60DC-4D30-9E03-94FF336332C7

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.4 Require BGP Authentication if Protocol is Used

Border Gateway Protocol (BGP)is a path vector protocol used for interior and exterior gateway routing on some networks.

BGP is a complex protocol, with many configuration options which may have effects which are not immediately obvious.

Verify Border Gateway Protocol (BGP) authentication is enabled, if routing protocol is used, where feasible.

3.3.4.1 Set 'neighbor password' (Manual)

Profile Applicability:

- Level 2

Description:

Enable message digest5 (MD5) authentication on a TCP connection between two BGP peers

Rationale:

Enforcing routing authentication reduces the likelihood of routing poisoning and unauthorized routers from joining BGP routing.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using the 'neighbor password' for BGP enforces these policies by restricting the type of authentication between network devices.

Audit:

Verify you see the appropriate neighbor password is defined:

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

Remediation:

Configure BGP neighbor authentication where feasible.

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

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/command/bgp-n1.html#GUID-A8900842-ECF3-42D3-B188-921BE0EC060B
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/command/bgp-m1.html#GUID-159A8006-F0DF-4B82-BB71-C39D2C134205

Additional Information:

MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers.

CIS Controls:

Version 6

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Management Plane**		
1.1	**Local Authentication, Authorization and Accounting (AAA) Rules**		
1.1.1	Enable 'aaa new-model' (Automated)	☐	☐
1.1.2	Enable 'aaa authentication login' (Automated)	☐	☐
1.1.3	Enable 'aaa authentication enable default' (Automated)	☐	☐
1.1.4	Set 'login authentication for 'line con 0' (Manual)	☐	☐
1.1.5	Set 'login authentication for 'line tty' (Automated)	☐	☐
1.1.6	Set 'login authentication for 'line vty' (Automated)	☐	☐
1.1.7	Set 'aaa accounting' to log all privileged use commands using 'commands 15' (Automated)	☐	☐
1.1.8	Set 'aaa accounting connection' (Automated)	☐	☐
1.1.9	Set 'aaa accounting exec' (Automated)	☐	☐
1.1.10	Set 'aaa accounting network' (Automated)	☐	☐
1.1.11	Set 'aaa accounting system' (Automated)	☐	☐
1.2	**Access Rules**		
1.2.1	Set 'privilege 1' for local users (Manual)	☐	☐
1.2.2	Set 'transport input ssh' for 'line vty' connections (Automated)	☐	☐
1.2.3	Set 'no exec' for 'line aux 0' (Automated)	☐	☐
1.2.4	Create 'access-list' for use with 'line vty' (Automated)	☐	☐
1.2.5	Set 'access-class' for 'line vty' (Automated)	☐	☐
1.2.6	Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0' (Automated)	☐	☐
1.2.7	Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0' (Automated)	☐	☐
1.2.8	Set 'exec-timeout' less than or equal to 10 minutes 'line tty' (Automated)	☐	☐
1.2.9	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty' (Automated)	☐	☐
1.2.10	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty' (Automated)	☐	☐
1.2.11	Set 'transport input none' for 'line aux 0' (Automated)	☐	☐
1.3	**Banner Rules**		
1.3.1	Set the 'banner-text' for 'banner exec' (Manual)	☐	☐
1.3.2	Set the 'banner-text' for 'banner login' (Manual)	☐	☐
1.3.3	Set the 'banner-text' for 'banner motd' (Manual)	☐	☐
1.4	**Password Rules**		

1.4.1	Set 'password' for 'enable secret' (Automated)	☐	☐
1.4.2	Enable 'service password-encryption' (Automated)	☐	☐
1.4.3	Set 'username secret' for all local users (Automated)	☐	☐
1.5	**SNMP Rules**		
1.5.1	Set 'no snmp-server' to disable SNMP when unused (Manual)	☐	☐
1.5.2	Unset 'private' for 'snmp-server community' (Manual)	☐	☐
1.5.3	Unset 'public' for 'snmp-server community' (Manual)	☐	☐
1.5.4	Do not set 'RW' for any 'snmp-server community' (Manual)	☐	☐
1.5.5	Set the ACL for each 'snmp-server community' (Manual)	☐	☐
1.5.6	Create an 'access-list' for use with SNMP (Manual)	☐	☐
1.5.7	Set 'snmp-server host' when using SNMP (Manual)	☐	☐
1.5.8	Set 'snmp-server enable traps snmp' (Manual)	☐	☐
1.5.9	Set 'priv' for each 'snmp-server group' using SNMPv3 (Manual)	☐	☐
1.5.10	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3 (Manual)	☐	☐
2	**Control Plane**		
2.1	**Global Service Rules**		
2.1.1	**Setup SSH**		
2.1.1.1	**Configure Prerequisites for the SSH Service**		
2.1.1.1.1	Set the 'hostname' (Automated)	☐	☐
2.1.1.1.2	Set the 'ip domain-name' (Automated)	☐	☐
2.1.1.1.3	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa' (Manual)	☐	☐
2.1.1.1.4	Set 'seconds' for 'ip ssh timeout' (Manual)	☐	☐
2.1.1.1.5	Set maximum value for 'ip ssh authentication-retries' (Automated)	☐	☐
2.1.1.2	Set version 2 for 'ip ssh version' (Automated)	☐	☐
2.1.2	Set 'no cdp run' (Manual)	☐	☐
2.1.3	Set 'no ip bootp server' (Manual)	☐	☐
2.1.4	Set 'no service dhcp' (Automated)	☐	☐
2.1.5	Set 'no ip identd' (Automated)	☐	☐
2.1.6	Set 'service tcp-keepalives-in' (Automated)	☐	☐
2.1.7	Set 'service tcp-keepalives-out' (Automated)	☐	☐
2.1.8	Set 'no service pad' (Automated)	☐	☐
2.2	**Logging Rules**		
2.2.1	Set 'logging on' (Manual)	☐	☐
2.2.2	Set 'buffer size' for 'logging buffered' (Automated)	☐	☐
2.2.3	Set 'logging console critical' (Automated)	☐	☐
2.2.4	Set IP address for 'logging host' (Automated)	☐	☐
2.2.5	Set 'logging trap informational' (Manual)	☐	☐
2.2.6	Set 'service timestamps debug datetime' (Automated)	☐	☐

2.2.7	Set 'logging source interface' (Automated)	☐	☐
2.3	**NTP Rules**		
2.3.1	**Require Encryption Keys for NTP**		
2.3.1.1	Set 'ntp authenticate' (Automated)	☐	☐
2.3.1.2	Set 'ntp authentication-key' (Automated)	☐	☐
2.3.1.3	Set the 'ntp trusted-key' (Automated)	☐	☐
2.3.1.4	Set 'key' for each 'ntp server' (Manual)	☐	☐
2.3.2	Set 'ip address' for 'ntp server' (Automated)	☐	☐
2.4	**Loopback Rules**		
2.4.1	Create a single 'interface loopback' (Automated)	☐	☐
2.4.2	Set AAA 'source-interface' (Automated)	☐	☐
2.4.3	Set 'ntp source' to Loopback Interface (Automated)	☐	☐
2.4.4	Set 'ip tftp source-interface' to the Loopback Interface (Automated)	☐	☐
3	**Data Plane**		
3.1	**Routing Rules**		
3.1.1	Set 'no ip source-route' (Automated)	☐	☐
3.1.2	Set 'no ip proxy-arp' (Automated)	☐	☐
3.1.3	Set 'no interface tunnel' (Automated)	☐	☐
3.1.4	Set 'ip verify unicast source reachable-via' (Manual)	☐	☐
3.2	**Border Router Filtering**		
3.2.1	Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks (Manual)	☐	☐
3.2.2	Set inbound 'ip access-group' on the External Interface (Manual)	☐	☐
3.3	**Neighbor Authentication**		
3.3.1	**Require EIGRP Authentication if Protocol is Used**		
3.3.1.1	Set 'key chain' (Manual)	☐	☐
3.3.1.2	Set 'key' (Manual)	☐	☐
3.3.1.3	Set 'key-string' (Manual)	☐	☐
3.3.1.4	Set 'address-family ipv4 autonomous-system' (Manual)	☐	☐
3.3.1.5	Set 'af-interface default' (Manual)	☐	☐
3.3.1.6	Set 'authentication key-chain' (Manual)	☐	☐
3.3.1.7	Set 'authentication mode md5' (Manual)	☐	☐
3.3.1.8	Set 'ip authentication key-chain eigrp' (Manual)	☐	☐
3.3.1.9	Set 'ip authentication mode eigrp' (Manual)	☐	☐
3.3.2	**Require OSPF Authentication if Protocol is Used**		
3.3.2.1	Set 'authentication message-digest' for OSPF area (Manual)	☐	☐
3.3.2.2	Set 'ip ospf message-digest-key md5' (Manual)	☐	☐
3.3.3	**Require RIPv2 Authentication if Protocol is Used**		
3.3.3.1	Set 'key chain' (Manual)	☐	☐
3.3.3.2	Set 'key' (Manual)	☐	☐
3.3.3.3	Set 'key-string' (Manual)	☐	☐

3.3.3.4	Set 'ip rip authentication key-chain' (Manual)	☐	☐
3.3.3.5	Set 'ip rip authentication mode' to 'md5' (Manual)	☐	☐
3.3.4	**Require BGP Authentication if Protocol is Used**		
3.3.4.1	Set 'neighbor password' (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Feb 5, 2021	4.1.0	Change domain name to domain-name (Ticket 12258)
Feb 17, 2021	4.1.0	Artifact update (Ticket 6248)