CIS Cisco IOS Switch RTR STIG Benchmark

v1.0.0 - 07-24-2024

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/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Internal Only - General

Table of Contents

Internal Only - General

Internal Only - General

Overview

Target Technology Details

Cisco IOS Switch RTR Secure Technical Implementation Guide (STIG)
Version: 3 Release: 1 Benchmark
Date: 24 Jul 2024

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 Switch RTR and are looking to comply with the STIG guidance

Internal Only - General

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

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

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Internal Only - General

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Internal Only - General

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Internal Only - General

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Cisco IOS Switch RTR

Internal Only - General

Recommendations

1 STIG RULES

Cisco IOS Switch

Cisco IOS Switch RTR Secure Technical Implementation Guide (STIG)

Version: 3 Release: 1 Benchmark

Date: 24 Jul 2024

CLASSIFICATION unclassified

Internal Only - General

1.1 CISC-RT-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce approved authorizations for controlling the flow of information within the network based on organization-defined information flow control policies.

```
GROUP ID: V-220419
RULE ID: SV-220419r622190
```

Rationale:

Information flow control regulates where information is allowed to travel within a network and between interconnected networks. The flow of all network traffic must be monitored and controlled so it does not introduce any unacceptable risk to the network infrastructure or data. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems.

Enforcement occurs, for example, in boundary protection devices (e.g., gateways, switches, guards, encrypted tunnels, and firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics).

Internal Only - General

Audit:

Review the switch configuration to verify that ACLs are configured to allow or deny traffic for specific source and destination addresses as well as ports and protocols. For example, the configuration below will allow only printer traffic into subnet 10.1.12.0/24 and SQL traffic into subnet 10.1.13.0/24. ICMP is allowed for troubleshooting and OSPF is the routing protocol used within the network.

```
interface GigabitEthernet0/1
no switchport
ip address 10.2.1.1 255.255.255.252
ip access-group FILTER_SERVER_TRAFFIC in
…
…
…
ip access-list extended FILTER_SERVER_TRAFFIC
permit tcp any 10.1.12.0 0.0.0.255 eq lpd 631 9100
permit tcp any 10.1.13.0 0.0.0.255 eq 1433 1434 4022
permit icmp any any
permit ospf any any
deny ip any any
```

Alternate: Inter-VLAN routing

```
interface Vlan12
ip address 10.1.12.1 255.255.255.0
ip access-group FILTER_PRINTER_VLAN out
!
interface Vlan13
ip address 10.1.13.1 255.255.255.0
ip access-group FILTER_SQL_VLAN out
…
…
…
ip access-list extended FILTER_PRINTER_VLAN
permit tcp any any eq lpd 631 9100
permit icmp any any
deny ip any any
ip access-list extended FILTER_SQL_VLAN
permit tcp any any eq 1433 1434 4022
permit icmp any any
deny ip any any
```

If the switch is not configured to enforce approved authorizations for controlling the flow of information within the network based on organization-defined information flow control policies, this is a finding.

Internal Only - General

Remediation:

Configure ACLs to allow or deny traffic for specific source and destination addresses as well as ports and protocols between various subnets as required. The commands below were used to create the configuration as shown in the check content:

```
SW1(config)#ip access-list extended FILTER_SERVER_TRAFFIC
SW1(config-ext-nacl)#permit tcp any 10.1.12.0 0.0.0.255 eq 515 631 9100
SW1(config-ext-nacl)#permit tcp any 10.1.13.0 0.0.0.255 eq 1433 1434 4022
SW1(config-ext-nacl)#permit icmp any any
SW1(config-ext-nacl)#permit ospf any any
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#interface g0/1
SW1(config-if)#ip access-group FILTER_SERVER_TRAFFIC in
SW1(config-if)#end
```

Alternate: Inter-VLAN routing

```
SW1(config)#ip access-list extended FILTER_PRINTER_VLAN
SW1(config-ext-nacl)#permit tcp any any eq lpd 631 9100
SW1(config-ext-nacl)#permit icmp any any
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended FILTER_SQL_VLAN
SW1(config-ext-nacl)#permit tcp any any eq 1433 1434 4022
SW1(config-ext-nacl)#permit icmp any any
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#interface vlan 12
SW1(config-if)#ip access-group FILTER_PRINTER_VLAN out
SW1(config-if)#exit
SW1(config)#interface vlan 13
SW1(config-if)#ip access-group FILTER_SQL_VLAN out
SW1(config-if)#end
```

Additional Information:

CCI-001368 Enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.2 CISC-RT-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enable routing protocol authentication using FIPS 198-1 algorithms with keys not exceeding 180 days of lifetime.

```
GROUP ID: V-220423
RULE ID: SV-220423r929046
```

Rationale:

A rogue router could send a fictitious routing update to convince a site's perimeter router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information about the site's network or used to disrupt the network's ability to communicate with other networks. This is known as a "traffic attraction attack" and is prevented by configuring neighbor router authentication using FIPS 198-1 algorithms for routing updates. If the keys used for authentication are guessed, the malicious user could create havoc within the network by advertising incorrect routes and redirecting traffic. Some routing protocols allow the use of key chains for authentication. A key chain is a set of keys that is used in succession, with each having a lifetime of no more than 180 days. Changing the keys frequently reduces the risk of them eventually being guessed. If a time period occurs during which no key is activated, neighbor authentication cannot occur, and therefore routing updates will fail.

Internal Only - General

Audit:

Review the switch configuration using the configuration examples below for BGP and OSPF.
EIGRP, RIP, and IS-IS only support MD5 and will incur a permanent finding for those protocols.
Note: The 180-day key lifetime is Not Applicable for the DODIN Backbone. The remainder of the requirement still applies.
Verify that neighbor router authentication is enabled for all routing protocols. If neighbor authentication is not enabled this is a finding.
Verify that authentication is configured to use FIPS 198-1 message authentication algorithms. If the routing protocol authentication is not configured to use FIPS 198-1 algorithms this is a finding.
Verify that the protocol key lifetime is configured to not exceed 180 days. If any protocol key lifetime is configured to exceed 180 days this is a finding.
BGP Example:

```
key chain <KEY-CHAIN-NAME> tcp
key <KEY-ID>
send-id <ID>
recv-id <ID>
cryptographic-algorithm hmac-sha256
key-string <KEY>
accept-lifetime 00:00:00 Jan 1 2022 duration 180
send-lifetime 00:00:00 Jan 1 2022 duration 180
!
!
router bgp <ASN>
no synchronization
bgp log-neighbor-changes
neighbor x.x.x.x remote-as <ASN>
neighbor x.x.x.x ao <KEY-CHAIN-NAME>
```


Internal Only - General

Note: TCP-AO is used to replace MD5 in BGP authentication.
OSPF Example:

```
key chain OSPF_KEY_CHAIN
key 1
key-string xxxxxxx
send-lifetime 00:00:00 Jan 1 2018 23:59:59 Mar 31 2018
accept-lifetime 00:00:00 Jan 1 2018 01:05:00 Apr 1 2018
cryptographic-algorithm hmac-sha-256
key 2
key-string yyyyyyy
send-lifetime 00:00:00 Apr 1 2018 23:59:59 Jun 30 2018
accept-lifetime 23:55:00 Mar 31 2018 01:05:00 Jul 1 2018
cryptographic-algorithm hmac-sha-256
…
…
…
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
ip ospf authentication key-chain OSPF_KEY_CHAIN
```


Internal Only - General

Remediation:

Configure routing protocol authentication to use a NIST-validated FIPS 198-1 message authentication code algorithm with keys not exceeding 180 days of lifetime as shown in the examples.
BGP Example:
Step 1: Configure a keychain using a FIPS 198-1 algorithm with a key duration not exceeding 180 days.
key chain <KEY-CHAIN-NAME> tcp
key <KEY-ID>
send-id <ID>
recv-id <ID>
cryptographic-algorithm hmac-sha256
key-string <KEY>
accept-lifetime 00:00:00 Jan 1 2022 duration 180
send-lifetime 00:00:00 Jan 1 2022 duration 180
!
Step 2: Configure BGP autonomous system to use the keychain for authentication.
router bgp <ASN>
no synchronization
bgp log-neighbor-changes
neighbor x.x.x.x remote-as <ASN>
neighbor x.x.x.x ao <KEY-CHAIN-NAME>
OSPF Example:
Step 1: Configure a keychain using a FIPS 198-1 algorithm with a key duration not exceeding 180 days.
key chain OSPF_KEY_CHAIN
key 1
key-string xxxxxxx
send-lifetime 00:00:00 Jan 1 2018 23:59:59 Mar 31 2018
accept-lifetime 00:00:00 Jan 1 2018 01:05:00 Apr 1 2018
cryptographic-algorithm hmac-sha-256
key 2
key-string yyyyyyy
send-lifetime 00:00:00 Apr 1 2018 23:59:59 Jun 30 2018
accept-lifetime 23:55:00 Mar 31 2018 01:05:00 Jul 1 2018
cryptographic-algorithm hmac-sha-256
Step 2: Configure OSPF to use the keychain for authentication.
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
ip ospf authentication key-chain OSPF_KEY_CHAIN

Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-002205 Uniquely identify and authenticate source by organization, system, application, service, and/or individual for information transfer.

- NIST SP 800-53 Revision 4::AC-4 (17)
- NIST SP 800-53 Revision 5::AC-4 (17)

Internal Only - General

1.3 CISC-RT-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must be configured to have all inactive Layer 3 interfaces disabled.

```
GROUP ID: V-220424
RULE ID: SV-220424r622190
```

Rationale:

An inactive interface is rarely monitored or controlled and may expose a network to an undetected attack on that interface. Unauthorized personnel with access to the communication facility could gain access to a switch by connecting to a configured interface that is not in use.

If an interface is no longer used, the configuration must be deleted and the interface disabled. For sub-interfaces, delete sub-interfaces that are on inactive interfaces and delete sub-interfaces that are inactive. If the sub-interface is no longer necessary for authorized communications, it must be deleted.

Audit:

Review the switch configuration and verify that inactive interfaces have been disabled as shown below:
interface GigabitEthernet3
no switchport
shutdown
!
interface GigabitEthernet4
no switchport
shutdown
If an interface is not being used but is configured or enabled, this is a finding.

Remediation:

Disable all inactive interfaces as shown below:
SW1(config)#interface GigabitEthernet3
SW1(config-if)#shutdown
SW1(config)#interface GigabitEthernet4
SW1(config-if)#shutdown

Internal Only - General

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.4 CISC-RT-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must not be configured to have any zero-touch deployment feature enabled when connected to an operational network.

```
GROUP ID: V-220427
RULE ID: SV-220427r856231
```

Rationale:

Network devices that are configured via a zero-touch deployment or auto-loading feature can have their startup configuration or image pushed to the device for installation via TFTP or Remote Copy (rcp). Loading an image or configuration file from the network is taking a security risk because the file could be intercepted by an attacker who could corrupt the file, resulting in a denial of service.

Audit:

Review the device configuration to determine if auto-configuration or zero-touch deployment via Cisco Networking Services (CNS) is enabled.
Auto-configuration example:
version 15.0
service config
…
…
…
boot-start-marker
boot network tftp://x.x.x.x/R5-config
boot-end-marker
CNS Zero-Touch example:
cns trusted-server config x.x.x.x
cns trusted-server image x.x.x.x
cns config initial x.x.x.x 80
cns exec 80
cns image
If a configuration auto-loading feature or zero-touch deployment feature is enabled, this is a finding.
Note: Auto-configuration or zero-touch deployment features can be enabled when the switch is offline for the purpose of image loading or building out the configuration. In addition, this would not be applicable to the provisioning of virtual switches via a software-defined network (SDN) orchestration system.

Internal Only - General

Remediation:

Disable configuration auto-loading if enabled using the following commands:
SW1(config)#no boot network
SW1(config)#no service config
Disable CNS zero-touch deployment if enabled as shown in the example below:
SW2(config)#no cns config initial
SW2(config)#no cns exec
SW2(config)#no cns image
SW2(config)#no cns trusted-server config x.x.x.x
SW2(config)#no cns trusted-server image x.x.x.x

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.5 CISC-RT-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to protect against or limit the effects of denial-of-service (DoS) attacks by employing control plane protection.

```
GROUP ID: V-220428
RULE ID: SV-220428r991872
```

Rationale:

The Route Processor (RP) is critical to all network operations because it is the component used to build all forwarding paths for the data plane via control plane processes. It is also instrumental with ongoing network management functions that keep the routers and links available for providing network services. Any disruption to the RP or the control and management planes can result in mission-critical network outages.

A DoS attack targeting the RP can result in excessive CPU and memory utilization. To maintain network stability and RP security, the router must be able to handle specific control plane and management plane traffic that is destined to the RP. In the past, one method of filtering was to use ingress filters on forwarding interfaces to filter both forwarding path and receiving path traffic, as well as limiting traffic destined to the device. However, this method does not scale well as the number of interfaces grows and the size of the ingress filters grows. Control plane policing increases the security of routers and multilayer switches by protecting the RP from unnecessary or malicious traffic. Filtering and rate limiting the traffic flow of control plane packets can be implemented to protect routers against reconnaissance and DoS attacks, allowing the control plane to maintain packet forwarding and protocol states despite an attack or heavy load on the router or multilayer switch.

Internal Only - General

Audit:

Review the Cisco switch configuration to verify that is protects against known types of DoS attacks by employing organization-defined security safeguards.
Step 1: Verify traffic types have been classified based on importance levels. The following is an example configuration:
class-map match-all CoPP_CRITICAL
match access-group name CoPP_CRITICAL
class-map match-any CoPP_IMPORTANT
match access-group name CoPP_IMPORTANT
match protocol arp
class-map match-all CoPP_NORMAL
match access-group name CoPP_NORMAL
class-map match-any CoPP_UNDESIRABLE
match access-group name CoPP_UNDESIRABLE
class-map match-all CoPP_DEFAULT
match access-group name CoPP_DEFAULT
Step 2: Review the access control lists (ACLs) referenced by the class maps to determine if the traffic is being classified appropriately. The following is an example configuration:
ip access-list extended CoPP_CRITICAL
remark our control plane adjacencies are critical
permit ospf host [OSPF neighbor A] any
permit ospf host [OSPF neighbor B] any
permit pim host [PIM neighbor A] any
permit pim host [PIM neighbor B] any
permit pim host [RP addr] any
permit igmp any 224.0.0.0 15.255.255.255
deny ip any any
ip access-list extended CoPP_IMPORTANT
permit tcp host [TACACS server] eq tacacs any
permit tcp [management subnet] 0.0.0.255 any eq 22
permit udp host [SNMP manager] any eq snmp
permit udp host [NTP server] eq ntp any
deny ip any any

Internal Only - General

ip access-list extended CoPP_NORMAL
remark we will want to rate limit ICMP traffic
deny icmp any host x.x.x.x fragments
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any unreachable
deny ip any any
ip access-list extended CoPP_UNDESIRABLE
remark other management plane traffic that should not be received
permit udp any any eq ntp
permit udp any any eq snmp
permit tcp any any eq 22
permit tcp any any eq 23
remark other control plane traffic not configured on switch
permit eigrp any any
permit udp any any eq rip
deny ip any any
ip access-list extended CoPP_DEFAULT
permit ip any any
Note: Explicitly defining undesirable traffic with ACL entries enables the network operator to collect statistics. Excessive ARP packets can potentially monopolize Route Processor resources, starving other important processes. Currently, ARP is the only Layer 2 protocol that can be specifically classified using the match protocol command.
Step 3: Review the policy-map to determine if the traffic is being policed appropriately for each classification. The following is an example configuration:
policy-map CONTROL_PLANE_POLICY
class CoPP_CRITICAL
police 512000 8000 conform-action transmit exceed-action transmit
class CoPP_IMPORTANT
police 256000 4000 conform-action transmit exceed-action drop
class CoPP_NORMAL
police 128000 2000 conform-action transmit exceed-action drop
class CoPP_UNDESIRABLE
police 8000 1000 conform-action drop exceed-action drop
class CoPP_DEFAULT
police 64000 1000 conform-action transmit exceed-action drop
Step 4: Verify that the Control Plane Policing (CoPP) policy is enabled. The following is an example configuration:
control-plane
service-policy input CONTROL_PLANE_POLICY
Note: Control Plane Protection (CPPr) can be used to filter as well as police control plane traffic destined to the RP. CPPr is very similar to CoPP and has the ability to filter and police traffic using finer granularity by dividing the aggregate control plane into three separate categories: 1) host, 2) transit, and 3) CEF-exception. Hence, a separate policy-map could be configured for each traffic category.

Internal Only - General

If the Cisco switch is not configured to protect against known types of DoS attacks by employing organization-defined security safeguards, this is a finding.

Remediation:

Configure the Cisco switch to protect against known types of DoS attacks on the route processor. Implementing a CoPP policy as shown in the example below is a best practice method:
Step 1: Configure ACL specific traffic types.

```
SW1(config)#ip access-list extended CoPP_CRITICAL
SW1(config-ext-nacl)#remark our control plane adjacencies are critical
SW1(config-ext-nacl)#permit ospf host x.x.x.x any
SW1(config-ext-nacl)#permit ospf host x.x.x.x any
SW1(config-ext-nacl)#permit pim host x.x.x.x any
SW1(config-ext-nacl)#permit pim host x.x.x.x any
SW1(config-ext-nacl)#permit igmp any 224.0.0.0 15.255.255.255
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_IMPORTANT
SW1(config-ext-nacl)#permit tcp host x.x.x.x eq tacacs any
SW1(config-ext-nacl)#permit tcp x.x.x.x 0.0.0.255 any eq 22
SW1(config-ext-nacl)#permit udp host x.x.x.x any eq snmp
SW1(config-ext-nacl)#permit udp host x.x.x.x eq ntp any
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_NORMAL
SW1(config-ext-nacl)#remark we will want to rate limit ICMP traffic
SW1(config-ext-nacl)#deny icmp any host x.x.x.x fragments
SW1(config-ext-nacl)#permit icmp any any echo
SW1(config-ext-nacl)#permit icmp any any echo-reply
SW1(config-ext-nacl)#permit icmp any any time-exceeded
SW1(config-ext-nacl)#permit icmp any any unreachable
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_UNDESIRABLE
SW1(config-ext-nacl)#remark management plane traffic that should not be received
SW1(config-ext-nacl)#permit udp any any eq ntp
SW1(config-ext-nacl)#permit udp any any eq snmp
```


Internal Only - General

```
SW1(config-ext-nacl)#permit tcp any any eq 22
SW1(config-ext-nacl)#permit tcp any any eq 23
SW1(config-ext-nacl)#remark control plane traffic not configured on switch
SW1(config-ext-nacl)#permit eigrp any any
SW1(config-ext-nacl)#permit udp any any eq rip
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_DEFAULT
SW1(config-ext-nacl)#permit ip any any
SW1(config-ext-nacl)#exit
```
Step 2: Configure class-maps referencing each of the ACLs.
```
SW1(config)#class-map match-all CoPP_CRITICAL
SW1(config-cmap)#match access-group name CoPP_CRITICAL
SW1(config-cmap)#class-map match-any CoPP_IMPORTANT
SW1(config-cmap)#match access-group name CoPP_IMPORTANT
SW1(config-cmap)#match protocol arp
SW1(config-cmap)#class-map match-all CoPP_NORMAL
SW1(config-cmap)#match access-group name CoPP_NORMAL
SW1(config-cmap)#class-map match-any CoPP_UNDESIRABLE
SW1(config-cmap)#match access-group name CoPP_UNDESIRABLE
SW1(config-cmap)#class-map match-all CoPP_DEFAULT
SW1(config-cmap)#match access-group name CoPP_DEFAULT
SW1(config-cmap)#exit
```
Step 3: Configure a policy-map referencing the configured class-maps and apply appropriate bandwidth allowance and policing attributes.
```
SW1(config)#policy-map CONTROL_PLANE_POLICY
SW1(config-pmap)#class CoPP_CRITICAL
SW1(config-pmap-c)#police 512000 8000 conform-action transmit exceed-action
transmit
SW1(config-pmap-c-police)#class CoPP_IMPORTANT
SW1(config-pmap-c)#police 256000 4000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#class CoPP_NORMAL
SW1(config-pmap-c)#police 128000 2000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#class CoPP_UNDESIRABLE
SW1(config-pmap-c)#police 8000 1000 conform-action drop exceed-action drop
SW1(config-pmap-c-police)#class CoPP_DEFAULT
SW1(config-pmap-c)#police 64000 1000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#exit
SW1(config-pmap-c)#exit
SW1(config-pmap)#exit
```
Step 4: Apply the policy-map to the control plane.
```
SW1(config)#control-plane
SW1(config-cp)#service-policy input CONTROL_PLANE_POLICY
SW1(config-cp)#end
```


Internal Only - General

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

CCI-004866 Employ organization-defined controls by type of denial-of-service to achieve the denial-of-service objective.

- NIST SP 800-53 Revision 5::SC-5 b

Internal Only - General

1.6 CISC-RT-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to have gratuitous ARP disabled on all external interfaces.

```
GROUP ID: V-220431
RULE ID: SV-220431r856233
```

Rationale:

A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used to inform the network about a host IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

Audit:

Review the configuration to determine if gratuitous ARP is disabled. The following command should not be found in the switch configuration:
ip gratuitous-arps
Note: With Cisco IOS, gratuitous ARP is enabled and disabled globally.
If gratuitous ARP is enabled on any external interface, this is a finding.

Remediation:

Disable gratuitous ARP as shown in the example below:
SW1(config)#no ip gratuitous-arps

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.7 CISC-RT-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must be configured to have IP directed broadcast disabled on all interfaces.

```
GROUP ID: V-220432
RULE ID: SV-220432r856234
```

Rationale:

An IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last switch in the chain, which is connected directly to the target subnet, can conclusively identify a directed broadcast.

IP directed broadcasts are used in the extremely common and popular smurf, or denial-of-service (DoS), attacks. In a smurf attack, the attacker sends Internet Control Message Protocol (ICMP) echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified. This service should be disabled on all interfaces when not needed to prevent smurf and DoS attacks.

Directed broadcast can be enabled on internal-facing interfaces to support services such as Wake-On-LAN. Case scenario may also include support for legacy applications where the content server and the clients do not support multicast. The content servers send streaming data using UDP broadcast. Used in conjunction with the IP multicast helper-map feature, broadcast data can be sent across a multicast topology. The broadcast streams are converted to multicast and vice versa at the first-hop switches and last-hop switches before entering and leaving the multicast transit area respectively. The last-hop switch must convert the multicast to broadcast. Hence, this interface must be configured to forward a broadcast packet (i.e., a directed broadcast address is converted to the all nodes broadcast address).

Internal Only - General

Audit:

Review the switch configuration to determine if IP directed broadcast is disabled. The IP directed broadcast command must not be found on any interface as shown in the example below:
interface GigabitEthernet0/1
no switchport
ip address x.x.x.x 255.255.255.0
ip directed-broadcast
…
…
…
Interface Vlan11
no switchport
ip address x.x.x.x 255.255.255.0
ip directed-broadcast
If IP directed broadcast is not disabled on all interfaces, this is a finding.

Remediation:

Disable IP directed broadcast on all interfaces as shown in the example below:
SW1(config)#int g0/1
SW1(config-if)#no ip directed-broadcast
SW1(config)#int vlan11
SW1(config-if)#no ip directed-broadcast

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.8 CISC-RT-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to have Internet Control Message Protocol (ICMP) unreachable messages disabled on all external interfaces.

```
GROUP ID: V-220433
RULE ID: SV-220433r856235
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Switches automatically send ICMP messages under a wide variety of conditions. Host unreachable ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

Review the configuration to verify the no ip unreachables command has been configured on all external interfaces as shown in the configuration example below:
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
no ip unreachables
If ICMP unreachable notifications are sent from any external or null0 interface, this is a finding.
Alternative - DODIN Backbone:
Verify that the PE switch is configured to rate limit ICMP unreachable messages as shown in the example below:
ip icmp rate-limit unreachable 60000
ip icmp rate-limit unreachable DF 1000
Note: In the example above, packet-too-big message (ICMP Type 3 Code 4) can be sent once every second, while all other destination unreachable messages can be sent once every minute. This will avoid disrupting Path MTU Discovery for traffic traversing the backbone while mitigating the risk of an ICMP unreachable DoS attack.
If the PE switch is not configured to rate limit ICMP unreachable messages, this is a finding.

Internal Only - General

Remediation:

Step 1: Disable ip unreachables on all external interfaces.
SW1(config)#int g0/1
SW1(config-if)#no ip unreachables
Step 2: Disable ip unreachables on the Null0 interface if it is used to backhole packets.
SW1(config-if)#int null 0
SW1(config-if)#no ip unreachables
Alternative - DODIN Backbone:
Configure the PE switch to rate limit ICMP unreachable messages as shown in the example below:
SW1(config)#ip icmp rate-limit unreachable df 100
SW1(config)#ip icmp rate-limit unreachable 100000
SW1(config)#end
Alternative - Non-DODIN Backbone:
An alternative for non-backbone networks (e.g., enclave, base, camp, etc.) is to filter messages generated by the switch and silently drop ICMP Administratively Prohibited and Host Unreachable messages using the following configuration steps:
Step 1: Configure ACL to include ICMP Type 3 Code 1 (Host Unreachable) and Code 13 (Administratively Prohibited) as shown in the example below:
SW1(config)#ip access-list ext ICMP_T3C1C13
SW1(config-ext-nacl)#permit icmp any any host-unreachable
SW1(config-ext-nacl)#permit icmp any any administratively-prohibited
SW1(config-ext-nacl)#exit
Step 2: Create a route-map to forward these ICMP messages to the Null0 interface.
SW1(config)#route-map LOCAL_POLICY
SW1(config-route-map)#match ip address ICMP_T3C1C13
SW1(config-route-map)#set interface Null0
SW1(config-route-map)#exit
Step 3: Configure no ip unreachables on the Null0 interface.
SW1(config)#int null 0
SW1(config-if)#no ip unreachables
SW1(config-if)#exit
Step 4: Apply the policy to filter messages generated by the switch.
SW1(config)#ip local policy route-map LOCAL_POLICY
SW1(config)#end

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.9 CISC-RT-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to have Internet Control Message Protocol (ICMP) mask reply messages disabled on all external interfaces.

```
GROUP ID: V-220434
RULE ID: SV-220434r856236
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Switches automatically send ICMP messages under a wide variety of conditions. Mask Reply ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

Review the switch configuration and verify that ip mask-reply command is not enabled on any external interfaces as shown in the example below:
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
ip mask-reply
If the ip mask-reply command is configured on any external interface, this is a finding.

Remediation:

Disable ip mask-reply on all external interfaces as shown below:
SW1(config)#int g0/1
SW1(config-if)#no ip mask-reply

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.10 CISC-RT-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to have Internet Control Message Protocol (ICMP) redirect messages disabled on all external interfaces.

```
GROUP ID: V-220435
RULE ID: SV-220435r856237
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Switches automatically send ICMP messages under a wide variety of conditions. Redirect ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

Review the switch configuration to verify that the no ip redirects command has been configured on all external interfaces as shown in the example below:
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
no ip redirects
If ICMP Redirect messages are enabled on any external interfaces, this is a finding.

Remediation:

Disable ICMP redirects on all external interfaces as shown in the example below:
SW1(config)#int g0/1
SW1(config-if)#no ip redirects

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.11 CISC-RT-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must be configured to log all packets that have been dropped at interfaces via an access control list (ACL).

```
GROUP ID: V-220436
RULE ID: SV-220436r622190
```

Rationale:

Auditing and logging are key components of any security architecture. It is essential for security personnel to know what is being done or attempted to be done, and by whom, to compile an accurate risk assessment. Auditing the actions on network devices provides a means to recreate an attack or identify a configuration mistake on the device.

Audit:

Review all ACLs used to filter traffic and verify that packets being dropped at interfaces via an ACL are logged as shown in the configuration below:
ip access-list extended INGRESS_FILTER
permit tcp any any established
permit tcp any host x.11.1.5 eq www
permit icmp host x.11.1.1 host x.11.1.2 echo
permit icmp any any echo-reply
…
…
…
deny ip any any log
If packets being dropped are not logged, this is a finding.

Remediation:

Configure ACLs to log packets that are dropped as shown in the example below:
SW1(config)#ip access-list extended INGRESS_FILTER
…
…
…
SW1(config-ext-nacl)#deny ip any any log

Internal Only - General

Additional Information:

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

Internal Only - General

1.12 CISC-RT-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to produce audit records containing information to establish where the events occurred.

```
GROUP ID: V-220437
RULE ID: SV-220437r622190
```

Rationale:

Without establishing where events occurred, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know where events occurred, such as switch components, modules, device identifiers, node names, and functionality.

Associating information about where the event occurred within the network provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured switch.

Audit:

Review the switch configuration to verify that events are logged containing information to establish where the events occurred as shown in the example below:
ip access-list extended INGRESS_FILTER
permit tcp any any established
permit tcp any host x.11.1.5 eq www
permit icmp host x.11.1.1 host x.11.1.2 echo
permit icmp any any echo-reply
…
…
…
deny ip any any log-input
Note: When the log-input parameter is configured on deny statements, the log record will contain the interface where the ingress packet has been dropped.
If the switch is not configured to produce audit records containing information to establish to establish where the events occurred, this is a finding.

Internal Only - General

Remediation:

Configure the switch to log events containing information to establish where the events occurred as shown in the example below:
SW1(config)#ip access-list extended INGRESS_FILTER
…
…
…
SW1(config-ext-nacl)#deny ip any any log-input

Additional Information:

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

Internal Only - General

1.13 CISC-RT-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to produce audit records containing information to establish the source of the events.

```
GROUP ID: V-220438
RULE ID: SV-220438r622190
```

Rationale:

Without establishing the source of the event, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

To compile an accurate risk assessment and provide forensic analysis, security personnel need to know the source of the event.

In addition to logging where events occur within the network, the audit records must also identify sources of events such as IP addresses, processes, and node or device names.

Audit:

Review the switch configuration to verify that events are logged containing information to establish the source of the events as shown in the example below:
ip access-list extended INGRESS_FILTER
permit tcp any any established
permit tcp any host x.11.1.5 eq www
permit icmp host x.11.1.1 host x.11.1.2 echo
permit icmp any any echo-reply
…
…
…
deny ip any any log-input
Note: When the log-input parameter is configured on deny statements, the log record will contain the Layer 2 address of the forwarding device for any packet being dropped.
If the switch is not configured to produce audit records containing information to establish the source of the events, this is a finding.

Internal Only - General

Remediation:

Configure the switch to log events containing information to establish where the events occurred as shown in the example below:
SW1(config)#ip access-list extended INGRESS_FILTER
…
…
…
SW1(config-ext-nacl)#deny ip any any log-input

Additional Information:

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

Internal Only - General

1.14 CISC-RT-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must be configured to disable the auxiliary port unless it is connected to a secured modem providing encryption and authentication.

```
GROUP ID: V-220439
RULE ID: SV-220439r622190
```

Rationale:

The use of POTS lines to modems connecting to network devices provides clear text of authentication traffic over commercial circuits that could be captured and used to compromise the network. Additional war dial attacks on the device could degrade the device and the production network.

Secured modem devices must be able to authenticate users and must negotiate a key exchange before full encryption takes place. The modem will provide full encryption capability (Triple DES) or stronger. The technician who manages these devices will be authenticated using a key fob and granted access to the appropriate maintenance port; thus, the technician will gain access to the managed device. The token provides a method of strong (two-factor) user authentication. The token works in conjunction with a server to generate one-time user passwords that will change values at second intervals. The user must know a personal identification number (PIN) and possess the token to be allowed access to the device.

Audit:

Review the configuration and verify that the auxiliary port is disabled unless a secured modem providing encryption and authentication is connected to it.
line aux 0
no exec
Note: transport input none is the default; hence, it will not be shown in the configuration.
If the auxiliary port is not disabled or is not connected to a secured modem when it is enabled, this is a finding.

Remediation:

Disable the auxiliary port.
SW2(config)#line aux 0
SW2(config-line)#no exec
SW2(config-line)#transport input none

Internal Only - General

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.15 CISC-RT-000235 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to have Cisco Express Forwarding enabled.

```
GROUP ID: V-237749
RULE ID: SV-237749r648775
```

Rationale:

The Cisco Express Forwarding (CEF) switching mode replaces the traditional Cisco routing cache with a data structure that mirrors the entire system routing table. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably when presented with large volumes of traffic addressed to many destinations such as a SYN flood attacks that. Because many SYN flood attacks use randomized source addresses to which the hosts under attack will reply to, there can be a substantial amount of traffic for a large number of destinations that the switch will have to handle. Consequently, switches configured for CEF will perform better under SYN floods directed at hosts inside the network than switches using the traditional cache.

Audit:

Review the switch to verify that CEF is enabled.
IPv4 Example: ip cef
IPv6 Example: ipv6 cef
If the switch is not configured to have CEF enabled, this is a finding.

Remediation:

Enable CEF
IPv4 Example: ip cef
IPv6 Example: ipv6 cef

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.16 CISC-RT-000236 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must be configured to advertise a hop limit of at least 32 in Switch Advertisement messages for IPv6 stateless auto-configuration deployments.

```
GROUP ID: V-237751
RULE ID: SV-237751r648779
```

Rationale:

The Neighbor Discovery protocol allows a hop limit value to be advertised by routers in a Router Advertisement message being used by hosts instead of the standardized default value. If a very small value was configured and advertised to hosts on the LAN segment, communications would fail due to the hop limit reaching zero before the packets sent by a host reached its destination.

Audit:

Review the switch configuration to determine if the hop limit has been configured for Router Advertisement messages as shown in the example.
ipv6 hop-limit 128
If hop-limit has been configured and has not been set to at least 32, it is a finding.

Remediation:

Configure the switch to advertise a hop limit of at least 32 in Router Advertisement messages as shown in the example.
SW1(config)#ipv6 hop-limit 128

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.17 CISC-RT-000237 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must not be configured to use IPv6 Site Local Unicast addresses.

```
GROUP ID: V-237755
RULE ID: SV-237755r648786
```

Rationale:

As currently defined, site local addresses are ambiguous and can be present in multiple sites. The address itself does not contain any indication of the site to which it belongs. The use of site-local addresses has the potential to adversely affect network security through leaks, ambiguity, and potential misrouting as documented in section 2 of RFC3879. RFC3879 formally deprecates the IPv6 site-local unicast prefix FEC0::/10 as defined in RFC3513.

Audit:

Review the switch configuration to ensure FEC0::/10 IPv6 addresses are not defined. If IPv6 Site Local Unicast addresses are defined, this is a finding.

Remediation:

Configure the switch using only authorized IPv6 addresses.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.18 CISC-RT-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco perimeter switch must be configured to deny network traffic by default and allow network traffic by exception.

```
GROUP ID: V-220440
RULE ID: SV-220440r622190
```

Rationale:

A deny-all, permit-by-exception network communications traffic policy ensures that only connections that are essential and approved are allowed.

This requirement applies to both inbound and outbound network communications traffic. All inbound and outbound traffic must be denied by default. Firewalls and perimeter switches should only allow traffic through that is explicitly permitted. The initial defense for the internal network is to block any traffic at the perimeter that is attempting to make a connection to a host residing on the internal network. In addition, allowing unknown or undesirable outbound traffic by the firewall or switch will establish a state that will permit the return of this undesirable traffic inbound.

Internal Only - General

Audit:

Review the switch configuration to verify that the inbound access control list (ACL) applied to all external interfaces is configured to allow specific ports and protocols and deny all other traffic.
Step 1: Verify that an inbound ACL is applied to all external interfaces as shown in the example below:
interface GigabitEthernet0/2
ip address x.11.1.2 255.255.255.254
ip access-group EXTERNAL_ACL in
Step 2: Review the inbound ACL to verify that it is configured to deny all other traffic that is not explicitly allowed.
ip access-list extended EXTERNAL_ACL
permit tcp any any established
permit icmp host x.11.1.1 host x.11.1.2 echo
permit icmp host x.11.1.1 host x.11.1.2 echo-reply
…
…
…
deny ip any any log-input
If the ACL is not configured to allow specific ports and protocols and deny all other traffic, this is a finding.
If the ACL is not configured inbound on all external interfaces, this is a finding.

Remediation:

Step 1: Configure an inbound ACL to deny all other traffic by default as shown in the example below:
SW1(config)#ip access-list extended EXTERNAL_ACL
SW1(config-ext-nacl)#permit tcp any any established
SW1(config-ext-nacl)#permit icmp host x.11.1.1 host x.11.1.2 echo
SW1(config-ext-nacl)#permit icmp host x.11.1.1 host x.11.1.2 echo-reply
…
…
…
SW1(config-ext-nacl)#deny ip any any log-input
Step 2: Apply the ingress filter to all external interfaces.
SW1(config)#int g0/2
SW1(config-if)#ip access-group EXTERNAL_ACL in

Internal Only - General

Additional Information:

CCI-001109 Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces; and/or for organization-defined systems.

- NIST SP 800-53::SC-7 (5)
- NIST SP 800-53A::SC-7 (5).1 (i) (ii)
- NIST SP 800-53 Revision 4::SC-7 (5)
- NIST SP 800-53 Revision 5::SC-7 (5)

Internal Only - General

1.19 CISC-RT-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to enforce approved authorizations for controlling the flow of information between interconnected networks in accordance with applicable policy.

```
GROUP ID: V-220441
RULE ID: SV-220441r622190
```

Rationale:

Information flow control regulates authorized information to travel within a network and between interconnected networks. Controlling the flow of network traffic is critical so it does not introduce any unacceptable risk to the network infrastructure or data.

An example of a flow control restriction is blocking outside traffic claiming to be from within the organization. For most switches, internal information flow control is a product of system design.

Audit:

Review the switch configuration to verify that access control lists (ACLs) are configured to allow or deny traffic for specific source and destination addresses as well as ports and protocols. In the example below, ICMP echo and echo-reply packets are allowed for troubleshooting connectivity. WWW traffic is permitted inbound to the NIPRNet host-facing web server (x.12.1.22).
interface GigabitEthernet0/1
description Link to DISN
ip address x.12.1.10 255.255.255.0
ip access-group FILTER_PERIMETER in
…
…
…
ip access-list extended FILTER_PERIMETER
permit tcp any any established
permit icmp host x.12.1.9 host x.12.1.10 echo
permit icmp host x.12.1.9 host x.12.1.10 echo-reply
permit tcp any host x.12.1.22 eq www
deny ip any any log-input
If the switch is not configured to enforce approved authorizations for controlling the flow of information between interconnected networks, this is a finding.

Internal Only - General

Remediation:

Step 1: Configure an ACL to allow or deny traffic as shown in the example below:
R1(config)#ip access-list extended FILTER_PERIMETER
R1(config-ext-nacl)#permit tcp any any established
R1(config-ext-nacl)#permit tcp host x.12.1.9 host x.12.1.10 eq bgp
R1(config-ext-nacl)#permit tcp host x.12.1.9 eq bgp host x.12.1.10
R1(config-ext-nacl)#permit icmp host x.12.1.9 host x.12.1.10 echo
R1(config-ext-nacl)#permit icmp host x.12.1.9 host x.12.1.10 echo-reply
R1(config-ext-nacl)#permit tcp any host x.12.1.22 eq www
R1(config-ext-nacl)#deny ip any any log-input
R1(config-ext-nacl)#exit
Step 2: Apply the ACL inbound on all external interfaces.
R2(config)#int g0/0
R1(config-if)#ip access-group FILTER_PERIMETER in
R1(config-if)#end

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.20 CISC-RT-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to only allow incoming communications from authorized sources to be routed to authorized destinations.

```
GROUP ID: V-220442
RULE ID: SV-220442r856238
```

Rationale:

Unrestricted traffic may contain malicious traffic that poses a threat to an enclave or to other connected networks. Additionally, unrestricted traffic may transit a network, which uses bandwidth and other resources.

Traffic can be restricted directly by an access control list (ACL), which is a firewall function, or by Policy Routing. Policy Routing is a technique used to make routing decisions based on a number of different criteria other than just the destination network, including source or destination network, source or destination address, source or destination port, protocol, packet size, and packet classification. This overrides the switch's normal routing procedures used to control the specific paths of network traffic. It is normally used for traffic engineering but can also be used to meet security requirements; for example, traffic that is not allowed can be routed to the Null0 or discard interface. Policy Routing can also be used to control which prefixes appear in the routing table.

This requirement is intended to allow network administrators the flexibility to use whatever technique is most effective.

Audit:

Review the switch configuration to determine if the switch allows only incoming communications from authorized sources to be routed to authorized destinations. The hypothetical example below allows inbound NTP from server x.1.12.9 only to host x.12.1.21.
ip access-list extended FILTER_PERIMETER
permit tcp any any established
…
…
…
permit udp host x.12.1.9 host x.12.1.21 eq ntp
deny ip any any log-input
If the switch does not restrict incoming communications to allow only authorized sources and destinations, this is a finding.

Internal Only - General

Remediation:

Configure the switch to allow only incoming communications from authorized sources to be routed to authorized destinations.
SW1(config)#ip access-list extended FILTER_PERIMETER
SW1(config-ext-nacl)#permit udp host x.12.1.9 host x.12.1.21 eq ntp
SW1(config-ext-nacl)#end

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.21 CISC-RT-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to block inbound packets with source Bogon IP address prefixes.

```
GROUP ID: V-220443
RULE ID: SV-220443r863240
```

Rationale:

Packets with Bogon IP source addresses should never be allowed to traverse the IP core. Bogon IP networks are RFC1918 addresses or address blocks that have never been assigned by the IANA or have been reserved.

Internal Only - General

Audit:

Review the switch configuration to verify that an ingress access control list (ACL) applied to all external interfaces is blocking packets with Bogon source addresses.
Step 1: Verify that an ACL has been configured containing the current Bogon prefixes as shown in the example below:
ip access-list extended FILTER_PERIMETER
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 10.0.0.0 0.255.255.255 any log-input
deny ip 100.64.0.0 0.63.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip 172.16.0.0 0.15.255.255 any log-input
deny ip 192.0.0.0 0.0.0.255 any log-input
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 192.168.0.0 0.0.255.255 any log-input
deny ip 198.18.0.0 0.1.255.255 any log-input
deny ip 198.51.100.0 0.0.0.255 any log-input
deny ip 203.0.113.0 0.0.0.255 any log-input
deny ip 224.0.0.0 31.255.255.255 any log-input
deny ip 240.0.0.0 15.255.255.255 any log-input
permit tcp any any established
permit icmp host x.12.1.9 host x.12.1.10 echo
permit icmp host x.12.1.9 host x.12.1.10 echo-reply
…
…
…
deny ip any any log-input
Step 2: Verify that the inbound ACL applied to all external interfaces will block all traffic from Bogon source addresses.
interface GigabitEthernet0/1
description Link to DISN
ip address x.12.1.10 255.255.255.254
ip access-group FILTER_PERIMETER in
If the switch is not configured to block inbound packets with source Bogon IP address prefixes, this is a finding.

Internal Only - General

Remediation:

Configure the perimeter to block inbound packets with Bogon source addresses.
Step 1: Configure an ACL containing the current Bogon prefixes as shown below:

```
SW1(config)#ip access-list extended FILTER_PERIMETER
SW1(config-ext-nacl)#deny ip 0.0.0.0 0.255.255.255 any log-input
SW1(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 any log-input
SW1(config-ext-nacl)#deny ip 100.64.0.0 0.63.255.255 any log-input
SW1(config-ext-nacl)#deny ip 127.0.0.0 0.255.255.255 any log-input
SW1(config-ext-nacl)#deny ip 169.254.0.0 0.0.255.255 any log-input
SW1(config-ext-nacl)#deny ip 172.16.0.0 0.15.255.255 any log-input
SW1(config-ext-nacl)#deny ip 192.0.0.0 0.0.0.255 any log-input
SW1(config-ext-nacl)#deny ip 192.0.2.0 0.0.0.255 any log-input
SW1(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255 any log-input
SW1(config-ext-nacl)#deny ip 198.18.0.0 0.1.255.255 any log-input
SW1(config-ext-nacl)#deny ip 198.51.100.0 0.0.0.255 any log-input
SW1(config-ext-nacl)#deny ip 203.0.113.0 0.0.0.255 any log-input
SW1(config-ext-nacl)#deny ip 224.0.0.0 31.255.255.255 any log-input
SW1(config-ext-nacl)#deny ip 240.0.0.0 15.255.255.255 any log-input
SW1(config-ext-nacl)#permit tcp any any established
SW1(config-ext-nacl)#permit icmp host x.12.1.9 host x.12.1.10 echo
SW1(config-ext-nacl)#permit icmp host x.12.1.9 host x.12.1.10 echo-reply
…
…
…
SW1(config-ext-nacl)#deny ip any any log-input
SW1(config-ext-nacl)#end
```

Step 2: Apply the ACL inbound on all external interfaces.

```
SW1(config)#int g0/0
SW1(config-if)#ip access-group FILTER_PERIMETER in
SW1(config-if)#end
```

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.22 CISC-RT-000310 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco perimeter switch must be configured to restrict it from accepting outbound IP packets that contain an illegitimate address in the source address field via egress filter or by enabling Unicast Reverse Path Forwarding (uRPF).

```
GROUP ID: V-220471
RULE ID: SV-220471r945858
```

Rationale:

A compromised host in an enclave can be used by a malicious platform to launch cyberattacks on third parties. This is a common practice in "botnets", which are a collection of compromised computers using malware to attack other computers or networks. DDoS attacks frequently leverage IP source address spoofing to send packets to multiple hosts that in turn will then send return traffic to the hosts with the IP addresses that were forged.

This can generate significant amounts of traffic. Therefore, protection measures to counteract IP source address spoofing must be taken. When uRPF is enabled in strict mode, the packet must be received on the interface that the device would use to forward the return packet, thereby mitigating IP source address spoofing.

Internal Only - General

Audit:

Review the switch configuration to verify that uRPF or an egress ACL has been configured on all internal interfaces to restrict the switch from accepting outbound IP packets that contain an illegitimate address in the source address field.
uRPF example:
interface GigabitEthernet0/1
description downstream link to LAN
ip address 10.1.25.5 255.255.255.0
ip verify unicast source reachable-via rx
Egress ACL example:
interface GigabitEthernet0/1
description downstream link to LAN
ip address 10.1.25.5 255.255.255.0
ip access-group EGRESS_FILTER in
…
…
…
ip access-list extended EGRESS_FILTER
permit udp 10.1.15.0 0.0.0.255 any eq domain
permit tcp 10.1.15.0 0.0.0.255 any eq ftp
permit tcp 10.1.15.0 0.0.0.255 any eq ftp-data
permit tcp 10.1.15.0 0.0.0.255 any eq www
permit icmp 10.1.15.0 0.0.0.255 any
permit icmp 10.1.15.0 0.0.0.255 any echo
deny ip any any
If uRPF or an egress ACL to restrict the switch from accepting outbound IP packets that contain an illegitimate address in the source address field has not been configured on all internal interfaces in an enclave, this is a finding.

Remediation:

Configure the switch to ensure that an egress ACL or uRPF is configured on internal interfaces to restrict the switch from accepting any outbound IP packet that contains an illegitimate address in the source field. The example below enables uRPF.
SW1(config)#int g0/1
SW1(config-if)#ip verify unicast source reachable-via rx

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

- NIST SP 800-53::SC-5 (1)
- NIST SP 800-53A::SC-5 (1).1
- NIST SP 800-53 Revision 4::SC-5 (1)
- NIST SP 800-53 Revision 5::SC-5 (1)

Internal Only - General

1.23 CISC-RT-000320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to filter traffic destined to the enclave in accordance with the guidelines contained in DoD Instruction 8551.1.

```
GROUP ID: V-220445
RULE ID: SV-220445r622190
```

Rationale:

Vulnerability assessments must be reviewed by the System Administrator, and protocols must be approved by the Information Assurance (IA) staff before entering the enclave.

Access control lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to reach a potential target within the security domain. The lists provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network that are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

If the perimeter is in a Deny-by-Default posture and what is allowed through the filter is in accordance with DoD Instruction 8551.1, and if the permit rule is explicitly defined with explicit ports and protocols allowed, then all requirements related to PPS being blocked would be satisfied.

Internal Only - General

Audit:

Review the switch configuration to verify that the ingress ACL is in accordance with DoD 8551.1.
Step 1: Verify that an inbound ACL is configured on all external interfaces.
interface GigabitEthernet0/2
ip address x.11.1.2 255.255.255.254
ip access-group EXTERNAL_ACL_INBOUND in
Step 2. Review the inbound ACL to verify that it is filtering traffic in accordance with DoD 8551.1.
ip access-list extended EXTERNAL_ACL_INBOUND
permit tcp any any established
permit icmp host x.11.1.1 host x.11.1.2 echo
permit icmp host x.11.1.1 host x.11.1.2 echo-reply
…
… < must be in accordance with DoD Instruction 8551.1>
…
deny ip any any log-input
If the switch does not filter traffic in accordance with the guidelines contained in DoD 8551.1, this is a finding.

Remediation:

Configure the switch to use an inbound ACL on all external interfaces as shown in the example below to restrict traffic in accordance with the guidelines contained in DoD Instruction 8551.1.
SW1(config)#ip access-list extended EXTERNAL_ACL_INBOUND
SW1(config-ext-nacl)#permit tcp any any established
SW1(config-ext-nacl)#permit icmp host x.11.1.1 host x.11.1.2 echo
SW1(config-ext-nacl)#permit icmp host x.11.1.1 host x.11.1.2 echo-reply
…
… < must be in accordance with DoD Instruction 8551.1>
…
SW1(config-ext-nacl)#deny ip any any log-input
SW1(config-ext-nacl)#exit
SW1(config)#int g0/2
SW1(config-if)#ip access-group EXTERNAL_ACL_INBOUND in

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.24 CISC-RT-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to filter ingress traffic at the external interface on an inbound direction.

```
GROUP ID: V-220446
RULE ID: SV-220446r622190
```

Rationale:

Access lists are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of switches makes use of access lists to restrict access to services on the switch itself as well as filter traffic passing through the switch.

Inbound versus Outbound: Some operating systems' default access lists are applied to the outbound queue. The more secure solution is to apply the access list to the inbound queue for three reasons:

- The switch can protect itself before damage is inflicted.
- The input port is still known and can be filtered on.
- It is more efficient to filter packets before routing them.

Audit:

Review the switch configuration to verify that an inbound ACL is configured on all external interfaces as shown in the example below:
interface GigabitEthernet0/2
ip address x.11.1.2 255.255.255.254
ip access-group EXTERNAL_ACL_INBOUND in
If the switch is not configured to filter traffic entering the network at all external interfaces in an inbound direction, this is a finding.

Remediation:

Configure the switch to use an inbound ACL on all external interfaces as shown in the example below:
SW1(config)#int g0/2
SW1(config-if)#ip access-group EXTERNAL_ACL_INBOUND in

Internal Only - General

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.25 CISC-RT-000340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to filter egress traffic at the internal interface on an inbound direction.

```
GROUP ID: V-220447
RULE ID: SV-220447r622190
```

Rationale:

Access lists are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of switches makes use of access lists to restrict access to services on the switch itself as well as filter traffic passing through the switch.

Inbound versus Outbound: Some operating systems' default access lists are applied to the outbound queue. The more secure solution is to apply the access list to the inbound queue for three reasons:

- The switch can protect itself before damage is inflicted.
- The input port is still known and can be filtered on.
- It is more efficient to filter packets before routing them.

Audit:

Review the switch configuration to verify that the egress access control list (ACL) is bound to the internal interface in an inbound direction.
interface interface GigabitEthernet0/2
description downstream link to LAN
ip address 10.1.25.5 255.255.255.0
ip access-group EGRESS_FILTER in
If the switch is not configured to filter traffic leaving the network at the internal interface in an inbound direction, this is a finding.

Remediation:

Configure the switch to use an inbound ACL on all internal interfaces as shown in the example below:
SW1(config)#int g0/2
SW1(config-if)#ip access-group EGRESS_FILTER in

Internal Only - General

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.26 CISC-RT-000350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to block all packets with any IP options.

```
GROUP ID: V-220472
RULE ID: SV-220472r945859
```

Rationale:

Packets with IP options are not fast switched and henceforth must be punted to the switch processor. Hackers who initiate denial-of-service (DoS) attacks on switches commonly send large streams of packets with IP options. Dropping the packets with IP options reduces the load of IP options packets on the switch. The end result is a reduction in the effects of the DoS attack on the switch and on downstream switches.

Audit:

Review the switch configuration to determine if it will block all packets with IP options.
ip access-list extended EXTERNAL_ACL
permit tcp any any established
deny ip any any option any-options
permit …
…
…
…
deny ip any any log-input
If the switch is not configured to drop all packets with IP options, this is a finding.

Remediation:

Configure the switch to drop all packets with IP options.
SW1(config)#ip access-list extended EXTERNAL_ACL
SW1(config-ext-nacl)#15 deny ip any any option any-options

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.27 CISC-RT-000360 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco perimeter switch must be configured to have Link Layer Discovery Protocol (LLDP) disabled on all external interfaces.

```
GROUP ID: V-220449
RULE ID: SV-220449r856240
```

Rationale:

LLDP is a neighbor discovery protocol used to advertise device capabilities, configuration information, and device identity. LLDP is media-and-protocol-independent as it runs over Layer 2; therefore, two network nodes that support different Layer 3 protocols can still learn about each other.

Allowing LLDP messages to reach external network nodes provides an attacker a method to obtain information of the network infrastructure that can be useful to plan an attack.

Audit:

Step 1: Verify LLDP is not enabled globally via the command.
lldp run
By default, LLDP is not enabled globally. If LLDP is enabled, proceed to Step 2.
Step 2: Verify LLDP is not enabled on any external interface as shown in the example below:
interface GigabitEthernet0/1
ip address x.1.12.1 255.255.255.252
no lldp transmit
Note: LLDP is enabled by default on all interfaces once it is enabled globally; hence the command "lldp transmit" will not be visible on the interface configuration.
If LLDP transmit is enabled on any external interface, this is a finding.

Remediation:

Disable LLDP transmit on all external interfaces as shown in the example below:
SW1(config)#int g0/1
SW1(config-if)#no lldp transmit

Internal Only - General

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.28 CISC-RT-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco perimeter switch must be configured to have Cisco Discovery Protocol (CDP) disabled on all external interfaces.

```
GROUP ID: V-220450
RULE ID: SV-220450r856241
```

Rationale:

CDP is a Cisco proprietary neighbor discovery protocol used to advertise device capabilities, configuration information, and device identity. CDP is media-and-protocol-independent as it runs over Layer 2; therefore, two network nodes that support different Layer 3 protocols can still learn about each other. Allowing CDP messages to reach external network nodes provides an attacker a method to obtain information of the network infrastructure that can be useful to plan an attack.

Audit:

Step 1: Verify if CDP is enabled globally as shown below:
cdp run
By default, CDP is not enabled globally or on any interface. If CDP is enabled globally, proceed to Step 2.
Step 2: Verify CDP is not enabled on any external interface as shown in the example below:
interface GigabitEthernet2
ip address z.1.24.4 255.255.255.252
…
…
…
cdp enable
If CDP is enabled on any external interface, this is a finding.

Remediation:

Disable CDP on all external interfaces via no cdp enable command or disable CDP globally via no cdp run command.

Internal Only - General

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.29 CISC-RT-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to have Proxy ARP disabled on all external interfaces.

```
GROUP ID: V-220451
RULE ID: SV-220451r856242
```

Rationale:

When Proxy ARP is enabled on a switch, it allows that switch to extend the network (at Layer 2) across multiple interfaces (LAN segments). Because proxy ARP allows hosts from different LAN segments to look like they are on the same segment, proxy ARP is only safe when used between trusted LAN segments.

Attackers can leverage the trusting nature of proxy ARP by spoofing a trusted host and then intercepting packets. Proxy ARP should always be disabled on switch interfaces that do not require it unless the switch is being used as a LAN bridge.

Audit:

Review the switch configuration to determine if IP Proxy ARP is disabled on all external interfaces as shown in the example below:
interface GigabitEthernet0/1
description link to DISN
ip address x.1.12.2 255.255.255.252
no ip proxy-arp
Note: By default, Proxy ARP is enabled on all interfaces; hence, if enabled, it will not be shown in the configuration.
If IP Proxy ARP is enabled on any external interface, this is a finding.

Remediation:

Disable Proxy ARP on all external interfaces as shown in the example below:
SW1(config)#int g0/1
SW1(config-if)#no ip proxy-arp

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.30 CISC-RT-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to block all outbound management traffic.

```
GROUP ID: V-220452
RULE ID: SV-220452r945857
```

Rationale:

For in-band management, the management network must have its own subnet in order to enforce control and access boundaries provided by Layer 3 network nodes, such as switches and firewalls. Management traffic between the managed network elements and the management network is routed via the same links and nodes as that used for production or operational traffic. Safeguards must be implemented to ensure that the management traffic does not leak past the perimeter of the managed network.

Audit:

Verify that the perimeter switch of the managed network is configured with an outbound ACL on the egress interface to block all management traffic as shown in the example below:
Step 1: Verify that all external interfaces has been configured with an outbound ACL as shown in the example below:
interface GigabitEthernet0/2
description link to DISN
ip address x.11.1.2 255.255.255.254
ip access-group EXTERNAL_ACL_OUTBOUND out
Step 2: Verify that the outbound ACL discards management traffic as shown in the example below:
ip access-list extended EXTERNAL_ACL_OUTBOUND
deny tcp any any eq tacacs log-input
deny tcp any any eq 22 log-input
deny udp any any eq snmp log-input
deny udp any any eq snmptrap log-input
deny udp any any eq syslog log-input
permit tcp any any eq www log-input
deny ip any any log-input
If management traffic is not blocked at the perimeter, this is a finding.

Internal Only - General

Remediation:

Configure the perimeter switch of the managed network with an outbound ACL on the egress interface to block all management traffic.
Step 1: Configure an ACL to block egress management traffic.

```
SW1(config)#ip access-list extended EXTERNAL_ACL_OUTBOUND
SW1(config-ext-nacl)#deny tcp any any eq tacacs log-input
SW1(config-ext-nacl)#deny tcp any any eq 22 log-input
SW1(config-ext-nacl)#deny udp any any eq snmp log-input
SW1(config-ext-nacl)#deny udp any any eq snmptrap log-input
SW1(config-ext-nacl)#deny udp any any eq syslog log-input
SW1(config-ext-nacl)#permit tcp any any eq www
SW1(config-ext-nacl)#deny ip any any log-input
SW1(config-ext-nacl)#exit
```

Note: Permit commands would be configured to allow applicable outbound traffic. The example above is allowing web traffic.
Step 2: Configure the external interfaces with the outbound ACL.

```
SW1(config)#int g0/2
SW1(config-if)#ip access-group EXTERNAL_ACL_OUTBOUND out
```

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.31 CISC-RT-000391 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to suppress Router Advertisements on all external IPv6-enabled interfaces.

```
GROUP ID: V-237758
RULE ID: SV-237758r648791
```

Rationale:

Many of the known attacks in stateless autoconfiguration are defined in RFC 3756 were present in IPv4 ARP attacks. To mitigate these vulnerabilities, links that have no hosts connected such as the interface connecting to external gateways must be configured to suppress router advertisements.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to verify that Router Advertisements are suppressed on all external IPv6-enabled interfaces as shown in the example below.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 nd ra suppress
If the switch is not configured to suppress Router Advertisements on all external IPv6-enabled interfaces, this is a finding.

Remediation:

Configure the switch to suppress Router Advertisements on all external IPv6-enabled interfaces as shown in the example below.
SW1(config)#int g1/0
SW1(config-if)#ipv6 nd ra suppress
SW1(config-if)#end

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.32 CISC-RT-000392 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 undetermined transport packets.

```
GROUP ID: V-237761
RULE ID: SV-237761r950991
```

Rationale:

One of the fragmentation weaknesses known in IPv6 is the undetermined transport packet. This packet contains an undetermined protocol due to fragmentation. Depending on the length of the IPv6 extension header chain, the initial fragment may not contain the layer four port information of the packet.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to determine if it is configured to drop IPv6 undetermined transport packets.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops undetermined transport packets as shown in the example below.
ipv6 access-list FILTER_IPV6
deny ipv6 any any log undetermined-transport
permit ipv6 …
…
…
…
deny ipv6 any any log
If the switch is not configured to drop IPv6 undetermined transport packets, this is a finding.

Internal Only - General

Remediation:

Configure the switch to drop IPv6 undetermined transport packets as shown in the example below.
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny ipv6 any any undetermined-transport log
SW1(config-ipv6-acl)#permit ipv6 …
…
…
…
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6 in

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.33 CISC-RT-000393 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured drop IPv6 packets with a Routing Header type 0, 1, or 3-255.

```
GROUP ID: V-237763
RULE ID: SV-237763r856665
```

Rationale:

The routing header can be used maliciously to send a packet through a path where less robust security is in place, rather than through the presumably preferred path of routing protocols. Use of the routing extension header has few legitimate uses other than as implemented by Mobile IPv6.

The Type 0 Routing Header (RFC 5095) is dangerous because it allows attackers to spoof source addresses and obtain traffic in response, rather than the real owner of the address. Secondly, a packet with an allowed destination address could be sent through a Firewall using the Routing Header functionality, only to bounce to a different node once inside. The Type 1 Routing Header is defined by a specification called "Nimrod Routing", a discontinued project funded by DARPA. Assuming that most implementations will not recognize the Type 1 Routing Header, it must be dropped. The Type 3–255 Routing Header values in the routing type field are currently undefined and should be dropped inbound and outbound.

Internal Only - General

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to determine if it is configured to drop IPv6 packets containing a Routing Header of type 0, 1, or 3-255.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets with a Routing Header type 0, 1, or 3-255
as shown in the example below.
ipv6 access-list FILTER_IPV6
permit ipv6 any host 2001:DB8::1:1:1234 routing-type 2
deny ipv6 any any log routing
permit ipv6 …
…
…
…
deny ipv6 any any log
Note: The example above allows routing-type 2 in the event Mobility IPv6 is deployed.
If the switch is not configured to drop IPv6 packets containing a Routing Header of type 0, 1, or 3-255, this is a finding.

Remediation:

Configure the switch to drop IPv6 packets with Routing Header of type 0, 1, or 3-255 as shown in the example below.
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#permit ipv6 any host 2001:DB8::0:1:1:1234 routing-type 2
SW1(config-ipv6-acl)#deny ipv6 any any routing log
SW1(config-ipv6-acl)#permit …
…
…
…
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.34 CISC-RT-000394 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values.

```
GROUP ID: V-237765
RULE ID: SV-237765r856667
```

Rationale:

These options are intended to be for the Destination Options header only. The optional and extensible natures of the IPv6 extension headers require higher scrutiny since many implementations do not always drop packets with headers that it cannot recognize and hence could cause a Denial-of-Service on the target device. In addition, the type, length, value (TLV) formatting provides the ability for headers to be very large.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to determine if it is compliant with this requirement.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets containing a Hop-by-Hop header with option type values of 0x04 (Tunnel Encapsulation Limit), 0xC9 (Home Address Destination), or 0xC3 (NSAP Address) as shown in the example below.
ipv6 access-list FILTER_IPV6
deny hbh any any dest-option-type 4 log
deny hbh any any dest-option-type 195 log
deny hbh any any dest-option-type home-address log
permit ipv6 …
…
…
…
deny ipv6 any any log
If the switch is not configured to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values, this is a finding.

Internal Only - General

Remediation:

Configure the switch to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values as shown in the example below.

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny hbh any any dest-option-type 4 log
SW1(config-ipv6-acl)#deny hbh any any dest-option-type 195 log
SW1(config-ipv6-acl)#deny hbh any any dest-option-type home-address log
SW1(config-ipv6-acl)# permit ipv6 …
…
…
…
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
SW1(config-if)#end
```

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.35 CISC-RT-000395 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 packets containing a Destination Option header with invalid option type values.

```
GROUP ID: V-237771
RULE ID: SV-237771r856669
```

Rationale:

These options are intended to be for the Hop-by-Hop header only. The optional and extensible natures of the IPv6 extension headers require higher scrutiny since many implementations do not always drop packets with headers that it cannot recognize. Hence, this could cause a Denial-of-Service on the target device. In addition, the type, length, value (TLV) formatting provides the ability for headers to be very large.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to determine if it is compliant with this requirement.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets containing a Destination Option header with option type values of 0x05 (Switch Alert) or 0xC2 (Jumbo Payload) as shown in the example below.
ipv6 access-list FILTER_IPV6
deny 60 any any dest-option-type 5 log
deny 60 any any dest-option-type 194 log
permit ipv6 …
…
…
…
deny ipv6 any any log
If the switch is not configured to drop IPv6 packets containing a Destination Option header with option type values of 0x05 (Switch Alert) or 0xC2 (Jumbo Payload), this is a finding.

Internal Only - General

Remediation:

Configure the switch to drop IPv6 packets containing a Destination Option header with option type values of 0x05 (Switch Alert) or 0xC2 (Jumbo Payload) as shown in the example below.

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny 60 any any dest-option-type 5 log
SW1(config-ipv6-acl)#deny 60 any any dest-option-type 194 log
SW1(config-ipv6-acl)#permit …
…
…
…
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
SW1(config-if)#end
```

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.36 CISC-RT-000396 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 packets containing an extension header with the Endpoint Identification option.

```
GROUP ID: V-237773
RULE ID: SV-237773r856671
```

Rationale:

The optional and extensible natures of the IPv6 extension headers require higher scrutiny since many implementations do not always drop packets with headers that it cannot recognize, and hence could cause a Denial-of-Service on the target device. In addition, the type, length, value (TLV) formatting provides the ability for headers to be very large. This option type is associated with the Nimrod Routing system and has no defining RFC document.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration to determine if it is compliant with this requirement.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets containing an extension header with the Endpoint Identification option as shown in the example below.
ipv6 access-list FILTER_IPV6
deny any any dest-option-type 138 log
permit ipv6 …
…
…
…
deny ipv6 any any log
If the switch is not configured to drop IPv6 packets containing an extension header with the Endpoint Identification option, this is a finding.

Internal Only - General

Remediation:

Configure the switch to drop IPv6 packets containing an option type values of 0x8A (Endpoint Identification) regardless of whether it appears in a Hop-by-Hop or Destination Option header as shown in the example below.

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny any any dest-option-type 138 log
SW1(config-ipv6-acl)#permit ipv6 …
…
…
…
SW1(config-ipv6-acl)# deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
SW1(config-if)#end
```

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.37 CISC-RT-000397 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 packets containing the NSAP address option within Destination Option header.

```
GROUP ID: V-237775
RULE ID: SV-237775r856673
```

Rationale:

The optional and extensible natures of the IPv6 extension headers require higher scrutiny since many implementations do not always drop packets with headers that it cannot recognize, and hence could cause a Denial-of-Service on the target device. In addition, the type, length, value (TLV) formatting provides the ability for headers to be very large. This option type from RFC 1888 (OSI NSAPs and IPv6) has been deprecated by RFC 4048.

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration and determine if filters are bound to the applicable interfaces to drop IPv6 packets containing a Destination Option header with option type value of 0xC3 (NSAP address).
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets containing the NSAP address option within Destination Option header as shown in the example below.
ipv6 access-list FILTER_IPV6
deny 60 any any dest-option-type 195 log
permit ipv6 …
…
…
…
deny ipv6 any any log
If the switch is not configured to drop IPv6 packets containing the NSAP address option within Destination Option header, this is a finding.

Internal Only - General

Remediation:

Configure the switch to to drop IPv6 packets containing the NSAP address option within Destination Option header as shown in the example below.
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny 60 any any dest-option-type 195 log
SW1(config-ipv6-acl)#permit …
…
…
…
SW1(config-ipv6-acl)# deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
SW1(config-if)#end

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.38 CISC-RT-000398 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco perimeter switch must be configured to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type.

```
GROUP ID: V-237777
RULE ID: SV-237777r856675
```

Rationale:

The optional and extensible natures of the IPv6 extension headers require higher scrutiny since many implementations do not always drop packets with headers that it cannot recognize, and hence could cause a Denial-of-Service on the target device. In addition, the type, length, value (TLV) formatting provides the ability for headers to be very large.

Internal Only - General

Audit:

This requirement is not applicable for the DODIN Backbone.
Review the switch configuration and determine if filters are bound to the applicable interfaces to drop all inbound IPv6 packets containing an undefined option type value regardless of whether they appear in a Hop-by-Hop or Destination Option header. Undefined values are 0x02, 0x03, 0x06, 0x9 – 0xE, 0x10 – 0x22, 0x24, 0x25, 0x27 – 0x2F, and 0x31 – 0xFF.
Step 1: Verify that an inbound IPv6 ACL has been configured on the external interface.
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 traffic-filter FILTER_IPV6 in
Step 2: Verify that the ACL drops IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type as shown in the example below.
ipv6 access-list FILTER_IPV6
deny any any dest-option-type 2
deny any any dest-option-type 3
deny any any dest-option-type 6
deny any any dest-option-type 9
deny any any dest-option-type 10
deny any any dest-option-type 11
deny any any dest-option-type 12
deny any any dest-option-type 13
deny any any dest-option-type 14
deny any any dest-option-type 16
…
deny any any dest-option-type 34
deny any any dest-option-type 36
deny any any dest-option-type 37
deny any any dest-option-type 39
…
deny any any dest-option-type 47
deny any any dest-option-type 49
…
deny any any dest-option-type 255
permit …
…
…
…
deny ipv6 any any log
Note: Because hop-by-hop and destination options have the same exact header format, they can be combined under the dest-option-type keyword. Since Hop-by-Hop and Destination Option headers have non-overlapping types, you can use dest-option-type to match either.
If the switch is not configured to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type, this is a finding.

Internal Only - General

Remediation:

Configure the switch to drop all inbound IPv6 packets containing an undefined option type value regardless of whether they appear in a Hop-by-Hop or Destination Option header as shown in the example below.

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny any any dest-option-type 2
SW1(config-ipv6-acl)#deny any any dest-option-type 3
SW1(config-ipv6-acl)#deny any any dest-option-type 6
SW1(config-ipv6-acl)#deny any any dest-option-type 9
SW1(config-ipv6-acl)#deny any any dest-option-type 10
SW1(config-ipv6-acl)#deny any any dest-option-type 11
SW1(config-ipv6-acl)#deny any any dest-option-type 12
SW1(config-ipv6-acl)#deny any any dest-option-type 13
SW1(config-ipv6-acl)#deny any any dest-option-type 14
SW1(config-ipv6-acl)#deny any any dest-option-type 16
…
SW1(config-ipv6-acl)#deny any any dest-option-type 34
SW1(config-ipv6-acl)#deny any any dest-option-type 36
SW1(config-ipv6-acl)#deny any any dest-option-type 37
SW1(config-ipv6-acl)#deny any any dest-option-type 39
…
SW1(config-ipv6-acl)#deny any any dest-option-type 47
SW1(config-ipv6-acl)#deny any any dest-option-type 49
…
SW1(config-ipv6-acl)#deny any any dest-option-type 255
SW1(config-ipv6-acl)#permit …
…
…
…
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.39 CISC-RT-000450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to only permit management traffic that ingresses and egresses the out-of-band management (OOBM) interface.

```
GROUP ID: V-220453
RULE ID: SV-220453r991873
```

Rationale:

The OOBM access switch will connect to the management interface of the managed network elements. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network element will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic, thereby providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device.

If the device does not have an OOBM port, the interface functioning as the management interface must be configured so that management traffic does not leak into the managed network and production traffic does not leak into the management network.

Internal Only - General

Audit:

This requirement is only applicable where management access to the switch is via an OOBM interface, which is not a true OOBM interface.
Step 1: Verify that the managed interface has an inbound and outbound access control list (ACL) configured.
interface GigabitEthernet0/7
no switchport
description link to OOBM access switch
ip address 10.11.1.22 255.255.255.0
ip access-group INGRESS_MANAGEMENT_ACL in
ip access-group EGRESS_MANAGEMENT_ACL in
Step 2: Verify that the ingress ACL only allows management and ICMP traffic.
ip access-list extended INGRESS_MANAGEMENT_ACL
permit tcp any host 10.11.1.22 eq tacacs
permit tcp any host 10.11.1.22 eq 22
permit udp any host 10.11.1.22 eq snmp
permit udp any host 10.11.1.22 eq snmptrap
permit udp any host 10.11.1.22 eq ntp
permit icmp any host 10.11.1.22
deny ip any any log-input
Step 3: Verify that the egress ACL blocks any transit traffic.
ip access-list extended EGRESS_MANAGEMENT_ACL
deny ip any any log-input
Note: On Cisco switches, local generated packets are not inspected by outgoing interface access lists. Hence, the above configuration would drop any packets not generated by the switch, blocking any transit traffic.
If the switch does not restrict traffic that ingresses and egresses the management interface, this is a finding.

Internal Only - General

Remediation:

If the management interface is not a dedicated OOBM interface, it must be configured with both an ingress and egress ACL.
Step 1: Configure an ingress ACL as shown in the example below:
SW1(config)#ip access-list extended INGRESS_MANAGEMENT_ACL
SW1(config-ext-nacl)#permit tcp any host 10.11.1.22 eq tacacs
SW1(config-ext-nacl)#permit tcp any host 10.11.1.22 eq 22
SW1(config-ext-nacl)#permit udp any host 10.11.1.22 eq snmp
SW1(config-ext-nacl)#permit udp any host 10.11.1.22 eq snmptrap
SW1(config-ext-nacl)#permit udp any host 10.11.1.22 eq ntp
SW1(config-ext-nacl)#permit icmp any host 10.11.1.22
SW1(config-ext-nacl)#deny ip any any log-input
SW1(config-ext-nacl)#exit
Step 2: Configure an egress ACL as shown in the example below:
SW1(config)#ip access-list extended EGRESS_MANAGEMENT_ACL
SW1(config-ext-nacl)#deny ip any any log-input
SW1(config-ext-nacl)#exit
Step 3: Apply the ACLs to the OOBM interfaces.
SW1(config)#int g0/7
SW1(config-if)#ip access-group INGRESS_MANAGEMENT_ACL in
SW1(config-if)#ip access-group EGRESS_MANAGEMENT_ACL out

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

Internal Only - General

1.40 CISC-RT-000660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco PE switch providing MPLS Layer 2 Virtual Private Network (L2VPN) services must be configured to authenticate targeted Label Distribution Protocol (LDP) sessions used to exchange virtual circuit (VC) information using a FIPS-approved message authentication code algorithm.

```
GROUP ID: V-220454
RULE ID: SV-220454r864159
```

Rationale:

LDP provides the signaling required for setting up and tearing down pseudowires (virtual circuits used to transport Layer 2 frames) across an MPLS IP core network. Using a targeted LDP session, each PE switch advertises a virtual circuit label mapping that is used as part of the label stack imposed on the frames by the ingress PE switch during packet forwarding. Authentication provides protection against spoofed TCP segments that can be introduced into the LDP sessions.

Audit:

The Cisco switch is not compliant with this requirement; hence, it is a finding. However, the severity level can be downgraded to a CAT III if the switch is configured to authenticate targeted LDP sessions using MD5 as shown in the configuration example below:
mpls ldp neighbor 10.1.1.2 password xxxxxxx
mpls label protocol ldp
If the switch is not configured to authenticate targeted LDP sessions using MD5, the finding will remain as a CAT II.

Remediation:

The severity level can be downgraded to a CAT III if the switch is configured to authenticate targeted LDP sessions using MD5 as shown in the example below:
SW1(config)#mpls ldp neighbor 10.1.1.2 password xxxxxxxx

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

Internal Only - General

1.41 CISC-RT-000730 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco PE switch must be configured to block any traffic that is destined to the IP core infrastructure.

```
GROUP ID: V-220455
RULE ID: SV-220455r622190
```

Rationale:

IP addresses can be guessed. Core network elements must not be accessible from any external host. Protecting the core from any attack is vital for the integrity and privacy of customer traffic as well as the availability of transit services. A compromise of the IP core can result in an outage or, at a minimum, non-optimized forwarding of customer traffic. Protecting the core from an outside attack also prevents attackers from using the core to attack any customer. Hence, it is imperative that all switches at the edge deny traffic destined to any address belonging to the IP core infrastructure.

Audit:

Step 1: Review the switch configuration to verify that an ingress ACL is applied to all external or CE-facing interfaces.
interface GigabitEthernet0/2
no switchport
ip address x.1.12.2 255.255.255.252
ip access-group BLOCK_TO_CORE in
Step 2: Verify that the ingress ACL discards and logs packets destined to the IP core address space.
ip access-list extended BLOCK_TO_CORE
deny ip any 10.1.x.0 0.0.255.255 log-input
permit ip any any
!
If the PE switch is not configured to block any traffic with a destination address assigned to the IP core infrastructure, this is a finding.
Note: Internet Control Message Protocol (ICMP) echo requests and traceroutes will be allowed to the edge from external adjacent neighbors.

Internal Only - General

Remediation:

Configure protection for the IP core to be implemented at the edges by blocking any traffic with a destination address assigned to the IP core infrastructure.
Step 1: Configure an ingress ACL to discard and log packets destined to the IP core address space.
SW2(config)#ip access-list extended BLOCK_TO_CORE
SW2(config-ext-nacl)#deny ip any 10.1.x.0 0.0.255.255 log-input
SW2(config-ext-nacl)#exit
Step 2: Apply the ACL inbound to all external or CE-facing interfaces.
SW2(config)#int SW1(config)#int g0/2
SW2(config-if)#ip access-group BLOCK_TO_CORE in
SW2(config-if)#end

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.42 CISC-RT-000740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco PE switch must be configured with Unicast Reverse Path Forwarding (uRPF) loose mode enabled on all CE-facing interfaces.

```
GROUP ID: V-220456
RULE ID: SV-220456r622190
```

Rationale:

The uRPF feature is a defense against spoofing and denial-of-service (DoS) attacks by verifying if the source address of any ingress packet is reachable. To mitigate attacks that rely on forged source addresses, all provider edge switches must enable uRPF loose mode to guarantee that all packets received from a CE switch contain source addresses that are in the route table.

Audit:

Review the switch configuration to determine if uRPF loose mode is enabled on all CE-facing interfaces.
interface GigabitEthernet0/2
no switchport
ip address x.1.12.2 255.255.255.252
ip access-group BLOCK_TO_CORE in
ip verify unicast source reachable-via any
If uRPF loose mode is not enabled on all CE-facing interfaces, this is a finding.

Remediation:

Configure uRPF loose mode on all CE-facing interfaces as shown in the example below:
SW2(config)#int SW1(config)#int g0/2
SW2(config-if)#ip verify unicast source reachable-via any
SW2(config-if)#end

Additional Information:

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

Internal Only - General

1.43 CISC-RT-000750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco PE switch must be configured to ignore or drop all packets with any IP options.

```
GROUP ID: V-220473
RULE ID: SV-220473r945860
```

Rationale:

Packets with IP options are not fast-switched and therefore must be punted to the switch processor. Hackers who initiate denial-of-service (DoS) attacks on switches commonly send large streams of packets with IP options. Dropping the packets with IP options reduces the load of IP options packets on the switch. The end result is a reduction in the effects of the DoS attack on the switch and on downstream switches.

Audit:

Review the switch configuration to determine if it will ignore or drop all packets with IP options as shown in the examples below:
ip options drop
or
ip options ignore
If the switch is not configured to drop or block all packets with IP options, this is a finding.

Remediation:

Configure the switch to ignore or drop all packets with IP options as shown in the examples below:
SW1(config)#ip options ignore
or
SW1(config)#ip options drop

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.44 CISC-RT-000760 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco PE switch must be configured to enforce a Quality-of-Service (QoS) policy to provide preferred treatment for mission-critical applications.

```
GROUP ID: V-220458
RULE ID: SV-220458r917423
```

Rationale:

Different applications have unique requirements and toleration levels for delay, jitter, bandwidth, packet loss, and availability. To manage the multitude of applications and services, a network requires a QoS framework to differentiate traffic and provide a method to manage network congestion. The Differentiated Services Model (DiffServ) is based on per-hop behavior by categorizing traffic into different classes and enabling each node to enforce a forwarding treatment to each packet as dictated by a policy.

Packet markings such as IP Precedence and its successor, Differentiated Services Code Points (DSCP), were defined along with specific per-hop behaviors for key traffic types to enable a scalable QoS solution. DiffServ QoS categorizes network traffic, prioritizes it according to its relative importance, and provides priority treatment based on the classification. It is imperative that end-to-end QoS is implemented within the IP core network to provide preferred treatment for mission-critical applications.

Internal Only - General

Audit:

Review the switch configuration and verify that a QoS policy has been configured to provide preferred treatment for mission-critical applications.
Step 1: Verify that the class-maps are configured to match on DSCP values as shown in the configuration example below:

```
class-map match-all C2_VOICE
match ip dscp af47
class-map match-all VOICE
match ip dscp ef
class-map match-all VIDEO
match ip dscp af41
class-map match-all CONTROL_PLANE
match ip dscp cs6
class-map match-all PREFERRED_DATA
match ip dscp af33
```

Step 2: Verify that the policy map reserves the bandwidth for each traffic type as shown in the example below:

```
policy-map QOS_POLICY
class C2_VOICE
priority percent 10
class VOICE
priority percent 15
class VIDEO
bandwidth percent 25
class CONTROL_PLANE
priority percent 10
class PREFERRED_DATA
bandwidth percent 25
class class-default
bandwidth percent 15
```

Step 3: Verify that an output service policy is bound to all interfaces as shown in the configuration example below:

```
interface GigabitEthernet1/1
no switchport
ip address 10.1.15.1 255.255.255.252
service-policy output QOS_POLICY
!
```


Internal Only - General

interface GigabitEthernet1/2
no switchport
ip address 10.1.15.4 255.255.255.252
service-policy output QOS_POLICY
Note: Enclaves must mark or re-mark their traffic to be consistent with the DODIN backbone admission criteria to gain the appropriate level of service. A general DiffServ principle is to mark or trust traffic as close to the source as administratively and technically possible. However, certain traffic types might need to be re-marked before handoff to the DODIN backbone to gain admission to the correct class. If such re-marking is required, it is recommended that the re-marking be performed at the CE egress edge.
Note: The GTP QOS document (GTP-0009) can be downloaded via the following link: https://intellipedia.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG_GTPs/GTP_Development_List
If the switch is not configured to enforce a QoS policy in accordance with the QoS GIG Technical Profile, this is a finding.

Internal Only - General

Remediation:

Configure to enforce a QoS policy to provide preferred treatment for mission-critical applications.
Step 1: Configure class-maps to match on DSCP values as shown in the configuration example below:

```
SW1(config)#class-map match-all PREFERRED_DATA
SW1(config-cmap)#match ip dscp af33
SW1(config-cmap)#class-map match-all CONTROL_PLANE
SW1(config-cmap)#match ip dscp cs6
SW1(config-cmap)#class-map match-all VIDEO
SW1(config-cmap)#match ip dscp af41
SW1(config-cmap)#class-map match-all VOICE
SW1(config-cmap)#match ip dscp ef
SW1(config-cmap)#class-map match-all C2_VOICE
SW1(config-cmap)#match ip dscp 47
SW1(config-cmap)#exit
```

Step 2: Configure a policy map to be applied to the core-layer-facing interface that reserves the bandwidth for each traffic type as shown in the example below:

```
SW1(config)#policy-map QOS_POLICY
SW1(config-pmap)#class CONTROL_PLANE
SW1(config-pmap-c)#priority percent 10
SW1(config-pmap-c)#class C2_VOICE
SW1(config-pmap-c)#priority percent 10
SW1(config-pmap-c)#class VOICE
SW1(config-pmap-c)#priority percent 15
SW1(config-pmap-c)#class VIDEO
SW1(config-pmap-c)#bandwidth percent 25
SW1(config-pmap-c)#class PREFERRED_DATA
SW1(config-pmap-c)#bandwidth percent 25
SW1(config-pmap-c)#class class-default
SW1(config-pmap-c)#bandwidth percent 15
SW1(config-pmap-c)#exit
SW1(config-pmap)#exit
```

Step 3: Apply the output service policy to all interfaces as shown in the configuration example below:

```
SW1(config)#int g1/1
SW1(config-if)#service-policy output QOS_POLICY
SW1(config-if)#exit
SW1(config)#int g1/2
SW1(config-if)#service-policy output QOS_POLICY
SW1(config-if)#end
```


Internal Only - General

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

Internal Only - General

1.45 CISC-RT-000770 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco P switch must be configured to enforce a Quality-of-Service (QoS) policy to provide preferred treatment for mission-critical applications.

```
GROUP ID: V-220459
RULE ID: SV-220459r917426
```

Rationale:

Different applications have unique requirements and toleration levels for delay, jitter, bandwidth, packet loss, and availability. To manage the multitude of applications and services, a network requires a QoS framework to differentiate traffic and provide a method to manage network congestion. The Differentiated Services Model (DiffServ) is based on per-hop behavior by categorizing traffic into different classes and enabling each node to enforce a forwarding treatment to each packet as dictated by a policy.

Packet markings such as IP Precedence and its successor, Differentiated Services Code Points (DSCP), were defined along with specific per-hop behaviors for key traffic types to enable a scalable QoS solution. DiffServ QoS categorizes network traffic, prioritizes it according to its relative importance, and provides priority treatment based on the classification. It is imperative that end-to-end QoS is implemented within the IP core network to provide preferred treatment for mission-critical applications.

Internal Only - General

Audit:

Review the switch configuration and verify that a QoS policy has been configured to provide preferred treatment for mission-critical applications.
Step 1: Verify that the class-maps are configured to match on DSCP values as shown in the configuration example below:
class-map match-all PREFERRED_DATA
match ip dscp af33
class-map match-all CONTROL_PLANE
match ip dscp cs6
class-map match-all VIDEO
match ip dscp af41
class-map match-all VOICE
match ip dscp ef
class-map match-all C2_VOICE
match ip dscp 47
Step 2: Verify that the policy map reserves the bandwidth for each traffic type as shown in the example below:
policy-map QOS_POLICY
class CONTROL_PLANE
priority percent 10
class C2_VOICE
priority percent 10
class VOICE
priority percent 15
class VIDEO
bandwidth percent 25
class PREFERRED_DATA
bandwidth percent 25
class class-default
bandwidth percent 15
Step 3: Verify that an output service policy is bound to all interfaces as shown in the configuration example below:
interface GigabitEthernet1/1
no switchport
ip address 10.1.15.5 255.255.255.252
service-policy output QOS_POLICY
!
interface GigabitEthernet1/2
no switchport
ip address 10.1.15.8 255.255.255.252
service-policy output QOS_POLICY
Note: The GTP QOS document (GTP-0009) can be downloaded via the following link: https://intellipedia.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG_GTPs/GTP_Development_List
If the switch is not configured to enforce a QoS policy in accordance with the QoS GIG Technical Profile, this is a finding.

Internal Only - General

Remediation:

Configure to enforce a QoS policy to provide preferred treatment for mission-critical applications.
Step 1: Configure class-maps to match on DSCP values as shown in the configuration example below:

```
SW1(config)#class-map match-all PREFERRED_DATA
SW1(config-cmap)#match ip dscp af33
SW1(config-cmap)#class-map match-all CONTROL_PLANE
SW1(config-cmap)#match ip dscp cs6
SW1(config-cmap)#class-map match-all VIDEO
SW1(config-cmap)#match ip dscp af41
SW1(config-cmap)#class-map match-all VOICE
SW1(config-cmap)#match ip dscp ef
SW1(config-cmap)#class-map match-all C2_VOICE
SW1(config-cmap)#match ip dscp 47
SW1(config-cmap)#exit
```

Step 2: Configure a policy map to be applied to the core-layer-facing interface that reserves the bandwidth for each traffic type as shown in the example below:

```
SW1(config)#policy-map QOS_POLICY
SW1(config-pmap)#class CONTROL_PLANE
SW1(config-pmap-c)#priority percent 10
SW1(config-pmap-c)#class C2_VOICE
SW1(config-pmap-c)#priority percent 10
SW1(config-pmap-c)#class VOICE
SW1(config-pmap-c)#priority percent 15
SW1(config-pmap-c)#class VIDEO
SW1(config-pmap-c)#bandwidth percent 25
SW1(config-pmap-c)#class PREFERRED_DATA
SW1(config-pmap-c)#bandwidth percent 25
SW1(config-pmap-c)#class class-default
SW1(config-pmap-c)#bandwidth percent 15
SW1(config-pmap-c)#exit
SW1(config-pmap)#exit
```

Step 3: Apply the output service policy to all interfaces as shown in the configuration example below:

```
SW1(config)#int g1/1
SW1(config-if)#service-policy output QOS_POLICY
SW1(config-if)#exit
SW1(config)#int g1/2
SW1(config-if)#service-policy output QOS_POLICY
SW1(config-if)#end
```


Internal Only - General

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

Internal Only - General

1.46 CISC-RT-000780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce a Quality-of-Service (QoS) policy to limit the effects of packet flooding denial-of-service (DoS) attacks.

```
GROUP ID: V-220460
RULE ID: SV-220460r622190
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. Packet flooding distributed denial-of-service (DDoS) attacks are referred to as volumetric attacks and have the objective of overloading a network or circuit to deny or seriously degrade performance, which denies access to the services that normally traverse the network or circuit. Volumetric attacks have become relatively easy to launch using readily available tools such as Low Orbit Ion Cannon or botnets.

Measures to mitigate the effects of a successful volumetric attack must be taken to ensure that sufficient capacity is available for mission-critical traffic. Managing capacity may include, for example, establishing selected network usage priorities or quotas and enforcing them using rate limiting, Quality of Service (QoS), or other resource reservation control methods. These measures may also mitigate the effects of sudden decreases in network capacity that are the result of accidental or intentional physical damage to telecommunications facilities (such as cable cuts or weather-related outages).

Internal Only - General

Audit:

Review the switch configuration to determine if it is configured to enforce a QoS policy to limit the effects of packet flooding DoS attacks.
Step 1: Verify that a class-map has been configured for the Scavenger class as shown in the example below:
class-map match-all SCAVENGER
match ip dscp cs1
Step 2: Verify that the policy-map includes the SCAVENGER class with low priority as shown in the example below:
policy-map QOS_POLICY
class CONTROL_PLANE
priority percent 10
class C2_VOICE
priority percent 10
class VOICE
priority percent 15
class VIDEO
bandwidth percent 25
class PREFERRED_DATA
bandwidth percent 25
class SCAVENGER
bandwidth percent 5
class class-default
bandwidth percent 10
Note: Traffic out of profile must be marked at the customer access layer or CE egress edge.
If the switch is not configured to enforce a QoS policy to limit the effects of packet flooding DoS attacks, this is a finding.

Remediation:

Step 1: Configure a class-map for the SCAVENGER class.
SW1(config)#class-map match-all SCAVENGER
SW1(config-cmap)#match ip dscp cs1
Step 2: Add the SCAVENGER class to the policy-map as shown in the example below:
SW1(config)#policy-map QOS_POLICY
SW1(config-pmap-c)#no class class-default
SW1(config-pmap)#class SCAVENGER
SW1(config-pmap-c)#bandwidth percent 5
SW1(config-pmap-c)#class class-default
SW1(config-pmap-c)#bandwidth percent 10
SW1(config-pmap-c)#end

Internal Only - General

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

Internal Only - General

1.47 CISC-RT-000790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco multicast switch must be configured to disable Protocol Independent Multicast (PIM) on all interfaces that are not required to support multicast routing.

```
GROUP ID: V-220461
RULE ID: SV-220461r622190
```

Rationale:

If multicast traffic is forwarded beyond the intended boundary, it is possible that it can be intercepted by unauthorized or unintended personnel. Limiting where, within the network, a given multicast group's data is permitted to flow is an important first step in improving multicast security.

A scope zone is an instance of a connected region of a given scope. Zones of the same scope cannot overlap, while zones of a smaller scope will fit completely within a zone of a larger scope. For example, Admin-local scope is smaller than Site-local scope, so the administratively configured boundary fits within the bounds of a site. According to RFC 4007 IPv6 Scoped Address Architecture (section 5), scope zones are also required to be "convex from a routing perspective"; that is, packets routed within a zone must not pass through any links that are outside of the zone. This requirement forces each zone to be one contiguous island rather than a series of separate islands.

As stated in the DoD IPv6 IA Guidance for MO3, "One should be able to identify all interfaces of a zone by drawing a closed loop on their network diagram, engulfing some switches and passing through some switches to include only some of their interfaces." Therefore, it is imperative that the network engineers have documented their multicast topology and know which interfaces are enabled for multicast. Once this is done, the zones can be scoped as required.

Audit:

Step 1: Review the network's multicast topology diagram.
Step 2: Review the switch configuration to verify that only the PIM interfaces as shown in the multicast topology diagram are enabled for PIM as shown in the example below:
interface GigabitEthernet1/1
no switchport
ip address 10.1.3.3 255.255.255.0
ip pim sparse-mode
If an interface is not required to support multicast routing and it is enabled, this is a finding.

Internal Only - General

Remediation:

Document all enabled interfaces for PIM in the network's multicast topology diagram. Disable support for PIM on interfaces that are not required to support it.
SW1(config)#int g1/1
SW1(config-if)#no ip pim sparse-mode

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.48 CISC-RT-000800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco multicast switch must be configured to bind a Protocol Independent Multicast (PIM) neighbor filter to interfaces that have PIM enabled.

```
GROUP ID: V-220462
RULE ID: SV-220462r622190
```

Rationale:

PIM is a routing protocol used to build multicast distribution trees for forwarding multicast traffic across the network infrastructure. PIM traffic must be limited to only known PIM neighbors by configuring and binding a PIM neighbor filter to interfaces that have PIM enabled.

If a PIM neighbor filter is not applied to interfaces that have PIM enabled, unauthorized switches can join the PIM domain, discover and use the rendezvous points, and advertise their rendezvous points into the domain. This can result in a denial of service by traffic flooding or in the unauthorized transfer of data.

Audit:

Step 1: Verify that all interfaces enabled for PIM have a neighbor access control list (ACL) bound to the interface as shown in the example below:
interface GigabitEthernet1/1
no switchport
ip address 10.1.2.2 255.255.255.0
ip pim neighbor-filter PIM_NEIGHBORS
ip pim sparse-mode
Step 2: Review the configured ACL for filtering PIM neighbors as shown in the example below:
ip access-list standard PIM_NEIGHBORS
permit 10.1.2.6
If PIM neighbor ACLs are not bound to all interfaces that have PIM enabled, this is a finding.

Internal Only - General

Remediation:

Configure neighbor ACLs to only accept PIM control plane traffic from documented PIM neighbors. Bind neighbor ACLs to all PIM-enabled interfaces.
Step 1: Configure ACL for PIM neighbors.
SW2(config)#ip access-list standard PIM_NEIGHBORS
SW2(config-std-nacl)#permit 10.1.2.6
SW2(config-std-nacl)#exit
Step 2: Apply the ACL to all interfaces enabled for PIM.
SW2(config)#int g1/1
SW2(config-if)#ip pim neighbor-filter PIM_NEIGHBORS

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.49 CISC-RT-000810 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco multicast edge switch must be configured to establish boundaries for administratively scoped multicast traffic.

```
GROUP ID: V-220463
RULE ID: SV-220463r622190
```

Rationale:

If multicast traffic is forwarded beyond the intended boundary, it is possible that it can be intercepted by unauthorized or unintended personnel.

Administrative scoped multicast addresses are locally assigned and are to be used exclusively by the enterprise network or enclave. Administrative scoped multicast traffic must not cross the enclave perimeter in either direction. Restricting multicast traffic makes it more difficult for a malicious user to access sensitive traffic.

Admin-Local scope is encouraged for any multicast traffic within a network intended for network management, as well as for control plane traffic that must reach beyond link-local destinations.

Audit:

Review the switch configuration and verify that admin-scope multicast traffic is blocked at the external edge as shown in the example below:
interface GigabitEthernet1/2
no switchport
ip address x.1.12.2 255.255.255.252
ip pim sparse-mode
ip multicast boundary MULTICAST_SCOPE
…
…
…
ip access-list standard MULTICAST_SCOPE
deny 239.0.0.0 0.255.255.255
permit any
If the switch is not configured to establish boundaries for administratively scoped multicast traffic, this is a finding.

Internal Only - General

Remediation:

Step 1: Configure the ACL to deny packets with multicast administratively scoped destination addresses as shown in the example below:
SW2(config)#ip access-list standard MULTICAST_SCOPE
SW2(config-std-nacl)#deny 239.0.0.0 0.255.255.255
SW2(config-std-nacl)#permit any
SW2(config-std-nacl)#exit
Step 2: Apply the multicast boundary at the appropriate interfaces as shown in the example below:
SW2(config)#int g1/2
SW2(config-if)#ip multicast boundary MULTICAST_SCOPE
SW2(config-if)#end

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

Internal Only - General

1.50 CISC-RT-000860 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco multicast Designated switch (DR) must be configured to filter the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Report messages to allow hosts to join only multicast groups that have been approved by the organization.

```
GROUP ID: V-220464
RULE ID: SV-220464r864160
```

Rationale:

Real-time multicast traffic can entail multiple large flows of data. Large unicast flows tend to be fairly isolated (i.e., someone doing a file download here or there), whereas multicast can have broader impact on bandwidth consumption, resulting in extreme network congestion. Hence, it is imperative that there is multicast admission control to restrict which multicast group's hosts are allowed to join via IGMP or MLD.

Audit:

Review the configuration of the DR to verify that it is filtering IGMP or MLD Membership Report messages, allowing hosts to join only groups that have been approved.
Step 1: Verify that all host-facing Layer 3 and VLAN interfaces are configured to filter IGMP Membership Report messages (IGMP joins) as shown in the example below:
interface Vlan3
ip address 10.3.3.3 255.255.255.0
ip pim sparse-mode
ip igmp access-group IGMP_JOIN_FILTER
ip igmp version 3
Step 2: Verify that the ACL denies unauthorized groups or permits only authorized groups. The example below denies all groups from 239.8.0.0/16 range.
ip access-list standard IGMP_JOIN_FILTER
deny 239.8.0.0 0.0.255.255
permit any
Note: This requirement is only applicable to Source Specific Multicast (SSM) implementation. This requirement is not applicable to Any Source Multicast (ASM) since the filtering is being performed by the Rendezvous Point switch.
If the DR is not filtering IGMP or MLD Membership Report messages, this is a finding.

Internal Only - General

Remediation:

Configure the DR to filter the IGMP or MLD Membership Report messages to allow hosts to join only multicast groups that have been approved.
Step 1: Configure the ACL to filter IGMP Membership Report messages as shown in the example below:
SW2(config)#ip access-list standard IGMP_JOIN_FILTER
SW2(config-std-nacl)#deny 239.8.0.0 0.0.255.255
SW2(config-std-nacl)#permit any
SW2(config-std-nacl)#exit
Step 2: Apply the filter to all host-facing Layer 3 and VLAN interfaces.
SW2(config)#int vlan3
SW2(config-if)#ip igmp access-group IGMP_JOIN_FILTER

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.51 CISC-RT-000870 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco multicast Designated switch (DR) must be configured to filter the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Report messages to allow hosts to join a multicast group only from sources that have been approved by the organization.

```
GROUP ID: V-220465
RULE ID: SV-220465r864161
```

Rationale:

Real-time multicast traffic can entail multiple large flows of data. Large unicast flows tend to be fairly isolated (i.e., someone doing a file download here or there), whereas multicast can have broader impact on bandwidth consumption, resulting in extreme network congestion. Hence, it is imperative that there is multicast admission control to restrict which multicast groups hosts are allowed to join via IGMP or MLD.

Audit:

Review the configuration of the DR to verify that it is filtering IGMP or MLD report messages, allowing hosts to only join multicast groups from sources that have been approved.
Step 1: Verify that all host-facing Layer 3 and VLAN interfaces are configured to filter IGMP Membership Report messages (IGMP joins) as shown in the example below:
interface Vlan3
ip address 10.3.3.3 255.255.255.0
ip pim sparse-mode
ip igmp access-group IGMP_JOIN_FILTER
ip igmp version 3
Step 2: Verify that the ACL denies unauthorized sources or allows only authorized sources. The example below denies all groups from the 232.8.0.0/16 range and permits sources only from the x.0.0.0/8 network.
ip access-list extended IGMP_JOIN_FILTER
deny ip any 232.8.0.0 0.0.255.255
permit ip x.0.0.0 0.255.255.255 any
deny ip any any
Note: This requirement is only applicable to Source Specific Multicast (SSM) implementation.
If the DR is not filtering IGMP or MLD report messages, this is a finding.

Internal Only - General

Remediation:

Configure the DR to filter the IGMP and MLD report messages to allow hosts to join only multicast groups from sources that have been approved as shown in the example below:
SW2(config)#ip access-list extended IGMP_JOIN_FILTER
SW2(config-ext-nacl)#deny ip any 232.8.0.0 0.0.255.255
SW2(config-ext-nacl)#permit ip x.0.0.0 0.255.255.255 any
SW2(config-ext-nacl)#deny ip any any
SW2(config-ext-nacl)#exit
Step 2: Apply the filter to all host-facing Layer 3 and VLAN interfaces.
SW2(config)#int vlan3
SW2(config-if)#ip igmp access-group IGMP_JOIN_FILTER

Additional Information:

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

Internal Only - General

1.52 CISC-RT-000880 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco multicast Designated switch (DR) must be configured to limit the number of mroute states resulting from Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Host Membership Reports.

```
GROUP ID: V-220466
RULE ID: SV-220466r856246
```

Rationale:

The current multicast paradigm can let any host join any multicast group at any time by sending an IGMP or MLD membership report to the DR. In a Protocol Independent Multicast (PIM) Sparse Mode network, the DR will send a PIM Join message for the group to the RP.

Without any form of admission control, this can pose a security risk to the entire multicast domain, specifically the multicast switches along the shared tree from the DR to the RP that must maintain the mroute state information for each group join request. Hence, it is imperative that the DR is configured to limit the number of mroute state information that must be maintained to mitigate the risk of IGMP or MLD flooding.

Audit:

Review the DR configuration to verify that it is limiting the number of mroute states via IGMP or MLD.
Verify IGMP limits have been configured globally or on each host-facing Layer 3 and VLAN interface via the ip igmp limit command as shown in the example below:
interface Vlan3
ip address 10.3.3.3 255.255.255.0
…
…
…
ip igmp limit nn
If the DR is not limiting multicast join requests via IGMP or MLD on a global or interfaces basis, this is a finding.

Remediation:

Configure the DR on a global or interface basis to limit the number of mroute states resulting from IGMP or MLD membership reports.
SW2(config)#int vlan3
SW2(config-if)#ip igmp limit 2

Internal Only - General

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.53 CISC-RT-000890 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco multicast Designated switch (DR) must be configured to set the shortest-path tree (SPT) threshold to infinity to minimalize source-group (S, G) state within the multicast topology where Any Source Multicast (ASM) is deployed.

```
GROUP ID: V-220467
RULE ID: SV-220467r945856
```

Rationale:

ASM can have many sources for the same groups (many-to-many). For many receivers, the path via the RP may not be ideal compared with the shortest path from the source to the receiver. By default, the last-hop switch will initiate a switch from the shared tree to a source-specific SPT to obtain lower latencies. This is accomplished by the last-hop switch sending an (S, G) Protocol Independent Multicast (PIM) Join toward S (the source).

When the last-hop switch begins to receive traffic for the group from the source via the SPT, it will send a PIM Prune message to the RP for the (S, G). The RP will then send a Prune message toward the source. The SPT switchover becomes a scaling issue for large multicast topologies that have many receivers and many sources for many groups because (S, G) entries require more memory than (*, G). Hence, it is imperative to minimize the amount of (S, G) state to be maintained by increasing the threshold that determines when the SPT switchover occurs.

Audit:

Review the DR configuration to verify that the SPT switchover threshold is increased (default is "0") or set to infinity (never switch over).
ip pim rp-address 10.2.2.2
ip pim spt-threshold infinity
If the DR is not configured to increase the SPT threshold or set to infinity to minimalize (S, G) state, this is a finding.

Remediation:

Configure the DR to increase the SPT threshold or set it to infinity to minimalize (S, G) state within the multicast topology where ASM is deployed.
SW2(config)#ip pim spt-threshold infinity

Internal Only - General

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	CISC-RT-000010 (Manual)	☐	☐
1.2	CISC-RT-000050 (Manual)	☐	☐
1.3	CISC-RT-000060 (Manual)	☐	☐
1.4	CISC-RT-000090 (Manual)	☐	☐
1.5	CISC-RT-000120 (Manual)	☐	☐
1.6	CISC-RT-000150 (Manual)	☐	☐
1.7	CISC-RT-000160 (Manual)	☐	☐
1.8	CISC-RT-000170 (Manual)	☐	☐
1.9	CISC-RT-000180 (Manual)	☐	☐
1.10	CISC-RT-000190 (Manual)	☐	☐
1.11	CISC-RT-000200 (Manual)	☐	☐
1.12	CISC-RT-000210 (Manual)	☐	☐
1.13	CISC-RT-000220 (Manual)	☐	☐
1.14	CISC-RT-000230 (Manual)	☐	☐
1.15	CISC-RT-000235 (Manual)	☐	☐
1.16	CISC-RT-000236 (Manual)	☐	☐
1.17	CISC-RT-000237 (Manual)	☐	☐
1.18	CISC-RT-000240 (Manual)	☐	☐
1.19	CISC-RT-000250 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	CISC-RT-000260 (Manual)	☐	☐
1.21	CISC-RT-000270 (Manual)	☐	☐
1.22	CISC-RT-000310 (Manual)	☐	☐
1.23	CISC-RT-000320 (Manual)	☐	☐
1.24	CISC-RT-000330 (Manual)	☐	☐
1.25	CISC-RT-000340 (Manual)	☐	☐
1.26	CISC-RT-000350 (Manual)	☐	☐
1.27	CISC-RT-000360 (Manual)	☐	☐
1.28	CISC-RT-000370 (Manual)	☐	☐
1.29	CISC-RT-000380 (Manual)	☐	☐
1.30	CISC-RT-000390 (Manual)	☐	☐
1.31	CISC-RT-000391 (Manual)	☐	☐
1.32	CISC-RT-000392 (Manual)	☐	☐
1.33	CISC-RT-000393 (Manual)	☐	☐
1.34	CISC-RT-000394 (Manual)	☐	☐
1.35	CISC-RT-000395 (Manual)	☐	☐
1.36	CISC-RT-000396 (Manual)	☐	☐
1.37	CISC-RT-000397 (Manual)	☐	☐
1.38	CISC-RT-000398 (Manual)	☐	☐
1.39	CISC-RT-000450 (Manual)	☐	☐
1.40	CISC-RT-000660 (Manual)	☐	☐
1.41	CISC-RT-000730 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	CISC-RT-000740 (Manual)	☐	☐
1.43	CISC-RT-000750 (Manual)	☐	☐
1.44	CISC-RT-000760 (Manual)	☐	☐
1.45	CISC-RT-000770 (Manual)	☐	☐
1.46	CISC-RT-000780 (Manual)	☐	☐
1.47	CISC-RT-000790 (Manual)	☐	☐
1.48	CISC-RT-000800 (Manual)	☐	☐
1.49	CISC-RT-000810 (Manual)	☐	☐
1.50	CISC-RT-000860 (Manual)	☐	☐
1.51	CISC-RT-000870 (Manual)	☐	☐
1.52	CISC-RT-000880 (Manual)	☐	☐
1.53	CISC-RT-000890 (Manual)	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
Aug 25, 2025	1.0.0	Initial CIS Release

Internal Only - General