CIS Cisco ACI Layer 2 Switch STIG Benchmark

v1.0.0 - 08-21-2025

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.

Table of Contents

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 for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

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

Remediation Procedure

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

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

The Rule Title from the STIG

Profile Definitions

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.

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.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Cisco ACI Layer 2 Switch

Recommendations

1 STIG RULES

Cisco Application Centric Infrastructure (ACI)

Cisco ACI Layer 2 Switch Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 27 May 2025

CLASSIFICATION unclassified

1.1 CACI-L2-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco ACI layer 2 switch must uniquely identify all network-connected endpoint devices before establishing any connection.

```
GROUP ID: V-272029
RULE ID: SV-272029r1114259
```

Rationale:

Controlling LAN access via 802.1x authentication can assist in preventing a malicious user from connecting an unauthorized PC to a switch port to inject or receive data from the network without detection.

In ACI, VLANs are used for traffic segmentation and identification, but their primary function is for identifying traffic, not directly configuring the leaf switch ports.

Audit:

Verify if the switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on those switch ports connected to devices that do not support an 802.1x supplicant.

1. Navigate to Fabric >> Port Profiles.
2. Select the port profile that is used for host-facing access ports.
3. Within the port profile configuration, locate the 802.1x settings and verify 802.1x is and MAB are enabled.
4. Navigate to the Endpoints section.
5. Choose the leaf nodes that host the host-facing ports and verify the port profile is applied.

If 802.1x authentication or MAB is not configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.

Remediation:

Enable 802.1X authentication on host-facing access ports in Cisco APIC and accommodate devices lacking 802.1X support, configure MAB (MAC Authentication Bypass). The following is an example.

Enable 802.1x on Port Profiles:

1. Navigate to Fabric >> Port Profiles.
2. Select the port profile that is used for host-facing access ports.
3. Within the port profile configuration, locate the 802.1x settings and enable it.
4. Specify the 802.1x authentication parameters are set.
5. Enable MAB and specify the MAC address range and relevant settings.
6. For Host Mode, select Single Host.
7. The MAC Auth should be EAP_FALLBACK_MAB.
8. In the Failed-auth VLAN field, select the VLAN to deploy to if authentication failed.
9. In the Failed-auth EPG field, choose the tenant, application profile, or EPG to deploy to if authentication failed.
10. Go to the Endpoints section.
11. Choose the leaf nodes that host the host-facing ports.
12. Apply the configured port profile to the host-facing ports.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.2 CACI-L2-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switches should authenticate all VLAN Trunk Protocol (VTP) messages with a hash function using the most secured cryptographic algorithm available.

```
GROUP ID: V-272030
RULE ID: SV-272030r1114331
```

Rationale:

VTP provides central management of VLAN domains, thus reducing administration in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP pruning preserves bandwidth by preventing VLAN traffic (unknown MAC, broadcast, multicast) from being sent down trunk links when not needed, that is, there are no access switch ports in neighboring switches belonging to such VLANs. An attack can force a digest change for the VTP domain enabling a rogue device to become the VTP server, which could allow unauthorized access to previously blocked VLANs or allow the addition of unauthorized switches into the domain. Authenticating VTP messages with a cryptographic hash function can reduce the risk of the VTP domains being compromised.

Audit:

Review the switch configuration to verify if VTP authentication is configured.

1. Navigate to Fabric >> Fabric Policies >> Policies >> Pod >> VLAN.
2. Verify that a VTP password is configured.

If a password is not configured, this is a finding.

Remediation:

Configure VLANs for VTP authentication by configuring the VLAN pool within the APIC and then associate it with the appropriate Endpoint Groups (EPGs). All switches in the VTP domain must have the same VTP domain name. All switches in the domain must have the same VTP password.

1. Navigate to Fabric >> Fabric Policies >> Policies >> Pod >> VLAN.
2. Specify the VTP domain name.
3. Set the VTP password.
4. Click "Apply" to save the changes.

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

1.3 CACI-L2-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must authenticate all network-connected endpoint devices before establishing any connection.

```
GROUP ID: V-272032
RULE ID: SV-272032r1114076
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

For distributed architectures (e.g., service-oriented architectures [SOA]), the decisions regarding the validation of authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide authentication decisions (as opposed to the actual authenticators) to the services that need to act on those decisions.

This requirement applies to applications that connect either locally, remotely, or through a network to an endpoint device (including, but not limited to, workstations, printers, servers (outside a datacenter), VoIP Phones, and VTC CODECs). Gateways and SOA applications are examples of where this requirement would apply.

Device authentication is a solution enabling an organization to manage devices. It is an additional layer of authentication ensuring only specific pre-authorized devices can access the system.

Audit:

Verify the switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on those switch ports connected to devices that do not support an 802.1x supplicant.

Verify the 802.1X Port Authentication policy is configured correctly:

1. On the menu bar, click Fabric >> External Access Policies >> Policies >> Interface >> 802.1X Port Authentication.
2. Right-click "802.1X Port Authentication" and review each 802.1X Port Authentication Policy.
    - In the Host Mode field, verify "Single Host" is selected.
    - In the MAC Auth field, verify "EAP_FALLBACK_MAB" is selected.

Verify 802.1X Node Authentication is associated with the 802.1X Port Authentication Policy to a Fabric Access Group:

1. On the menu bar, click Fabric >> External Access Policies >> Policies >> Switch >> 802.1X Node Authentication.
2. Right-click "802.1X Node Authentication" and review each 802.1X Node Authentication Policy.
    - In the Failed-auth EPG field, verify the tenant, application profile, and EPG to deploy to in the case of failed authentication is configured.
    - In the Failed-auth VLAN. verify the VLAN to deploy to in the case of failed authentication is selected.

Verify the 802.1X Node Authentication Policy is applied to each Leaf Switch Policy Group:

1. Navigate to Fabric >> External Access Policies >> Switches >> Leaf Switches >> Policy Groups.
2. Right-click "Policy Groups" to inspect each Access Switch Policy Group.

Verify the 802.1X Node Authentication Policy to a Leaf Interface Profile:

1. Navigate to Fabric >> External Access Policies >> Interfaces >> Leaf Interfaces >> Profiles.
2. Right-click "Profiles" and select Leaf Interface Profile.
3. Expand the Interface Selectors table to review the Access Port Selector(s).

If 802.1x authentication or MAB is not configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.

Remediation:

Configure 802.1 x authentications on all host-facing access switch ports. To authenticate those devices that do not support 802.1x, MAB must be configured. When configuring the interface for a leaf switch, the port security policy can be chosen from the list of available port security policies.

Create an 802.1X Port Authentication Policy:

1. On the menu bar, click Fabric >> External Access Policies >> Policies >> Interface >> 802.1X Port Authentication.
2. Right-click "802.1X Port Authentication" to open Create 802.1X Port Authentication Policy and fill out the form.
    - In the Host Mode field, select "Single Host—For allowing only one host per port".
    - In the MAC Auth field, select "EAP_FALLBACK_MAB".
    - Click "Submit".

Configure 802.1X Node Authentication.
Associate the 802.1X Port Authentication Policy to a Fabric Access Group:

1. On the menu bar, click Fabric >> External Access Policies >> Policies >> Switch >> 802.1X Node Authentication.
    - Right-click "802.1X Node Authentication" to open Create 802.1X Node Authentication Policy.
    - In the Failed-auth EPG field, select the tenant, application profile, and EPG to deploy to in the case of failed authentication.
    - In the Failed-auth VLAN, select the VLAN to deploy to in the case of failed authentication.
2. To associate the 802.1X Node Authentication Policy to a Leaf Switch Policy Group, navigate to Fabric >> External Access Policies >> Switches >> Leaf Switches >> Policy Groups.
    - Right-click "Policy Groups" to open Create Access Switch Policy Group.
    - In the 802.1X Node Authentication Policy field, select the previously created policy.
    - Click "Submit".
3. To associate the 802.1X Node Authentication Policy to a Leaf Interface Profile, navigate to Fabric >> External Access Policies >> Interfaces >> Leaf Interfaces >> Profiles.
    - Right-click "Profiles" to open Create Leaf Interface Profile.
    - Expand the Interface Selectors table to open the Create Access Port Selector dialog box and fill out the form.
    - In the Interface Policy Group field, select the previously created policy and click "OK".
    - Click "Submit".

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

1.4 CACI-L2-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must have Unknown Unicast Flood Blocking (UUFB) set to "Hardware Proxy".

```
GROUP ID: V-272033
RULE ID: SV-272033r1114238
```

Rationale:

Access layer switches use the Content Addressable Memory (CAM) table to direct traffic to specific ports based on the VLAN number and the destination MAC address of the frame. When a router has an Address Resolution Protocol (ARP) entry for a destination host and forwards it to the access layer switch and there is no entry corresponding to the frame's destination MAC address in the incoming VLAN, the frame will be sent to all forwarding ports within the respective VLAN, which causes flooding. Large amounts of flooded traffic can saturate low bandwidth links, causing network performance issues or complete connectivity outage to the connected devices. Unknown unicast flooding has been a problem in networks that have asymmetric routing and default timers. To mitigate the risk of a connectivity outage, the Unknown Unicast Flood Blocking (UUFB) feature must be implemented on all access layer switches. The UUFB feature will block unknown unicast traffic flooding and only permit egress traffic with MAC addresses that are known to exit on the port.

For Cisco ACI, L2 Unknown Unicast decides whether the bridge domain should flood packets that are destined to an unknown MAC address (Flood) or should send it to a spine node for COOP database lookup (Hardware Proxy).

Audit:

Verify each Bridge Domain used is configured to block unknown unicast traffic.

1. Navigate to Tenant>> Networking >> Bridge Domains >> Policy >> General and inspect each Tenant's Bridge Domain configuration.
2. Expand Networking and right-click each Bridge Domain.
    - Verify the L2 Unknown Unicast box is set to "Hardware Proxy".

If any user-facing or untrusted access switch ports do not have UUFB set to "Hardware Proxy", this is a finding.

Remediation:

Configure each Bridge Domain to handle unknown unicast flood blocking.

1. Navigate to Tenant >> Networking >> Bridge Domains >> Policy >> General.
2. Expand Networking and right-click "Create Bridge Domain" to open the dialog box and fill out the form.
    - In the L2 Unknown Unicast box, select "Hardware Proxy".
3. Click "NEXT".
4. Complete the Bridge Domain configuration and click "Finish".

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

1.5 CACI-L2-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must enable port security.

```
GROUP ID: V-272037
RULE ID: SV-272037r1113943
```

Rationale:

The port security feature protects the ACI fabric from being flooded with unknown MAC addresses by limiting the number of MAC addresses learned per port. The port security feature support is available for physical ports, port channels, and virtual port channels.

Audit:

Review the port security policies for compliance:

1. In the GUI menu bar, click Fabric >> Access Policies.
2. In the Navigation pane, expand Policies >> Interface >> Port Security.
3. Select each port security policy used and verify the following:
    - Port Security Timeout is set to "600 seconds".
    - Violation Action is set to "Protect mode".
    - Maximum Endpoints is set to "1".

Verify port security is active on all appropriate host-facing interfaces:

1. In the Navigation pane, click Fabric >> Inventory >> Topology.
2. Verify that each leaf has been configured to use a correctly configured port security policy.

If port security is not configured and enabled, this is a finding.

Remediation:

Create a port security policy. The port security policy can be created new or chosen from the list of available port security policies.

1. In the GUI menu bar, click Fabric >> Access Policies.
2. In the Navigation pane, expand Policies >> Interface >> Port Security.
3. Right-click "Port Security" and click "Create Port Security Policy".
4. In the Create Port Security Policy dialog box:
    - In the Port Security Timeout field, enter "600" before reenabling MAC learning on an interface.
    - In the Maximum Endpoints field, enter "1" for the maximum number of endpoints that can be learned on an interface.
    - In the Violation Action field, select "Protect".
5. Click "Submit".

Configure each host-facing interface for the leaf switches:

1. In the Navigation pane, click Fabric >> Inventory >> Topology, and navigate to the desired leaf switch.
2. Choose the appropriate port to configure the interface.
3. From the port security policy drop-down list, choose the desired port security policy to associate.

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

1.6 CACI-L2-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco ACI layer 2 switch must have Storm Control configured on all host-facing switch ports.

```
GROUP ID: V-272038
RULE ID: SV-272038r1114350
```

Rationale:

A traffic storm occurs when packets flood a LAN, creating excessive traffic and degrading network performance. Traffic storm control prevents network disruption by suppressing ingress traffic when the number of packets reaches configured threshold levels. Traffic storm control monitors ingress traffic levels on a port and drops traffic when the number of packets reaches the configured threshold level during any one-second interval.

Audit:

Review the switch configuration to verify that storm control is enabled on all host-facing interfaces as shown in the example below.

1. Navigate to Fabric >> Access Policies >> Policies >> Interface >> Storm Control.
2. Review each Storm Control policy.
3. Navigate to the Application Profile containing the EPGs to be protected.
4. Select each EPG and go to the "Policies" tab to verify that a storm control policy that is configured for to protect broadcast, at a minimum, has been applied.

If storm control is not enabled for host-facing interfaces for broadcast traffic at a, minimum, for broadcast traffic, this is a finding.

Remediation:

Configure one or more storm control policies for all host-facing interfaces and external interfaces and apply the policy to an ESG.

1. Navigate to Fabric >> Access Policies >> Policies >> Interface >> Storm Control.
2. Click "Add" to create a new policy and define the following parameters:
    - Give the policy a descriptive name.
    - Choose "Broadcast" as the type of traffic to control and other types as needed (e.g., Multicast, Unknown Unicast).
    - Set the threshold for the traffic type. (Refer to note below.)
    - Specify "log" as the action to take when the threshold is exceeded (e.g., drop, log).
    - Enable monitoring to track storm control events.

Apply the Storm Control Policy to an EPG:

1. Navigate to the Application Profile containing the EPGs to be protected.
2. Select the EPG and navigate to the "Policies" tab.
3. Under "Interface", select the newly created "Storm Control" policy.
4. Click "Apply".

Note: The acceptable range is 10000000-1000000000 for a gigabit Ethernet interface, and 100000000-10000000000 for a ten gigabit interface. Storm control is not supported on most FastEthernet interfaces.

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

1.7 CACI-L2-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco ACI layer 2 switch must have Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) snooping configured on all VLANs.

```
GROUP ID: V-272039
RULE ID: SV-272039r1113945
```

Rationale:

IGMP and MLD snooping provides a way to constrain multicast traffic at layer 2. By monitoring the IGMP or MLD membership reports sent by hosts within a VLAN, the snooping application can set up Layer 2 multicast forwarding tables to deliver specific multicast traffic only to interfaces connected to hosts interested in receiving the traffic, thereby significantly reducing the volume of multicast traffic that would otherwise flood the VLAN.

Audit:

Verify the switch configuration enables IGMP or MLD snooping for IPv4 and IPv6 multicast traffic. Below is an example of the steps to verify that IGMP snooping is enabled for each VLAN:

```
apic1(config-tenant-template-ip-igmp-snooping)# show run all
```

If the switch is not configured to implement IGMP or MLD snooping for each VLAN, this is a finding.

Remediation:

Configure IGMP or MLD snooping for IPv4 and IPv6 multicast traffic respectively globally.

Example:

```
apic1(config-tenant)# template ip igmp snooping policy <policy name>
```

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

1.8 CACI-L2-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must have all disabled switch ports assigned to an unused VLAN.

```
GROUP ID: V-272042
RULE ID: SV-272042r1114329
```

Rationale:

It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.

Audit:

If the switchport is configured for 802.1X, this is not applicable.

1. In the ACI GUI, navigate to Fabric >> Inventory >> Pod number.
2. Click the "Topology" tab to view the fabric topology.
3. Double-click the leaf switch or spine switch to view port-level connectivity.
4. Navigate to the VLAN section.
5. Review the switch configuration for the VLAN designated as the inactive VLAN. No applications or endpoints assigned.

Review the disabled ports.

1. Navigate to Fabric >> Inventory >> Pod number, then navigate to the desired switch.
2. Navigate to the port profile and verify it is assigned to the designated unused VLAN.
3. Each access switch identified as not in use should have membership to a designated unused VLAN.

If there are any access switch ports not in use and not in an inactive VLAN, this is a finding.

Remediation:

Identify ports that are unused. Assign all switch ports not in use to an inactive VLAN.

Create an Unused VLAN.

1. In the ACI GUI, Navigate to Fabric >> Inventory >> Pod number.
2. Click on the "Topology" tab to view the fabric topology.
3. Double-click the leaf switch or spine switch to view port-level connectivity.
4. Navigate to the VLAN section and create a new VLAN profile but do not assign any applications or endpoints.

Assign Ports to the Unused VLAN.

1. Navigate to Fabric >> Inventory >> Pod number, then navigate to the desired switch.
2. Select the specific port you want to disable (or not use) and assign to the unused VLAN.
3. Navigate to the port profile and select the unused VLAN.
4. Disable the port as needed.

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

1.9 CACI-L2-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must have all user-facing or untrusted ports configured as access switch ports.

```
GROUP ID: V-272043
RULE ID: SV-272043r1113949
```

Rationale:

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address, and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Audit:

Review the switch configuration and examine all user-facing or untrusted switchports. Display information for all Ethernet interfaces, including access and trunk interfaces.

Example:

```
[apic1] configure terminal
[apic1(config)#] show interface switchport
```

If any of the user-facing switch ports are configured as a trunk, this is a finding.

Remediation:

Disable trunking on all user-facing or untrusted switch ports. To disable trunking on all user-facing or untrusted switch ports on a Cisco APIC, use the command "switchport mode access" on each relevant interface within the APIC configuration, effectively setting each port to "access mode", which only allows traffic for a single VLAN, preventing trunking functionality. Identify which physical ports on the APIC are considered "user-facing" or "untrusted" as those will need to be configured as access ports.

```
[apic1] configure terminal
[apic1(config)#] interface <interface name>
[apic1(config-if)#] switchport mode access
[apic1(config-if)#] switchport access vlan <vlan-id>
```

or

To prevent any accidental trunking negotiation, use the "switchport nonegotiate" command on the interface.

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

1.10 CACI-L2-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch, for all 802.1q trunk links, must have the native VLAN assigned to an ID other than the default VLAN.

```
GROUP ID: V-272044
RULE ID: SV-272044r1113950
```

Rationale:

VLAN hopping can be initiated by an attacker who has access to a switch port belonging to the same VLAN as the native VLAN of the trunk link connecting to another switch that the victim is connected to. If the attacker knows the victim's MAC address, it can forge a frame with two 802.1q tags and a layer 2 header with the destination address of the victim. Since the frame will ingress the switch from a port belonging to its native VLAN, the trunk port connecting to the victim's switch will simply remove the outer tag because native VLAN traffic is to be untagged. The switch will forward the frame on to the trunk link unaware of the inner tag with a VLAN ID of which the victim's switch port is a member.

Audit:

Review the switch configurations and examine all trunk links. Verify the native VLAN has been configured to a VLAN ID other than the ID of the default VLAN (i.e., VLAN 1) as shown in the example below:

```
[apic1(config)#] show vlan dot1q tag native
```

or

```
[apic1(config)#] show interface
```

If the native VLAN has the same VLAN ID as the default VLAN, this is a finding.

Remediation:

To ensure the integrity of the trunk link and prevent unauthorized access, the ID of the native VLAN of the trunk port must be changed from the default VLAN (i.e., VLAN 1) to its own unique VLAN ID.

```
[apic1] configure terminal
[apic1(config)#] interface <interface name>
[apic1(config-if)#] vlan dot1q tag native
```

or

```
[apic1] configure terminal
[apic1(config)#] interface {interface name}
[apic1(config-if)#] switchport trunk native vlan <vlan-id>
```

Note: An alternative to configuring a dedicated native VLAN is to ensure all native VLAN traffic is tagged. This will mitigate the risk of VLAN hopping because there will always be an outer tag for native traffic as it traverses an 802.1q trunk link.

Note: The native VLAN ID must be the same on both ends of the trunk link; otherwise, traffic could accidentally leak between broadcast domains.

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

1.11 CACI-L2-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must employ a first-hop-security (FHS) policy to protect against denial-of-service (DoS) attacks.

```
GROUP ID: V-272045
RULE ID: SV-272045r1114353
```

Rationale:

DoS events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth.

FHS features enable a better IPv4 and IPv6 link security and management over the layer 2 links. In a service provider environment, these features closely control address assignment and derived operations. Setting include the following DOD required configurations:

- Unknown Unicast Flood Blocking (UUFB) enabled.
- DHCP snooping enabled for all user VLANs to validate DHCP messages from untrusted sources.
- IP Source Guard enabled on all user-facing or untrusted access switch ports.
- Dynamic Address Resolution Protocol (ARP) Inspection enabled on all user VLANs.

Satisfies: SRG-NET-000362-L2S-000025, SRG-NET-000362-L2S-000026, SRG-NET-000362-L2S-000027

Audit:

Verify the FHS policy is configured.

Note: This is an example. The exact configuration may vary with the site's architecture.

```
leaf4# show fhs bt all
```

The following settings must be enabled at a minimum:

- ip-inspection-admin-status enabled-both
- source-guard-admin-status enabled-both
- router-advertisement-guard-admin-status enabled
- router-advertisement-guard
- managed-config-check
- managed-config-flag
- other-config-check
- other-config-flag
- maximum-router-preference low
- minimum-hop-limit 10
- maximum-hop-limit 100

Trust-control tcpolicy settings:

- arp
- dhcpv4-server
- dhcpv6-server
- ipv6-router
- router-advertisement
- neighbor-discovery

If an FHS policy is not configured with all required settings, this is a finding.

Remediation:

Configure the FHS policy.

Note: This is an example. The exact configuration may vary with the site's architecture.

Example:

```
apic1(config)# tenant <tenant name>
apic1(config-tenant)# first-hop-security
apic1(config-tenant-fhs)# security-policy secpol1
apic1(config-tenant-fhs-secpol)#
apic1(config-tenant-fhs-secpol)# ip-inspection-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# source-guard-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# router-advertisement-guard-admin-status
enabled
apic1(config-tenant-fhs-secpol)# router-advertisement-guard
apic1(config-tenant-fhs-raguard)#
apic1(config-tenant-fhs-raguard)# managed-config-check
apic1(config-tenant-fhs-raguard)# managed-config-flag
apic1(config-tenant-fhs-raguard)# other-config-check
apic1(config-tenant-fhs-raguard)# other-config-flag
apic1(config-tenant-fhs-raguard)# maximum-router-preference low
apic1(config-tenant-fhs-raguard)# minimum-hop-limit 10
apic1(config-tenant-fhs-raguard)# maximum-hop-limit 100
apic1(config-tenant-fhs-raguard)# exit
apic1(config-tenant-fhs-secpol1)# exit
apic1(config-tenant-fhs)# trust-control tcpol1
apic1(config-tenant-fhs-trustctrl)# arp
apic1(config-tenant-fhs-trustctrl)# dhcpv4-server
apic1(config-tenant-fhs-trustctrl)# dhcpv6-server
apic1(config-tenant-fhs-trustctrl)# ipv6-router
apic1(config-tenant-fhs-trustctrl)#  router-advertisement
apic1(config-tenant-fhs-trustctrl)# neighbor-discovery
apic1(config-tenant-fhs-trustctrl)# exit
apic1(config-tenant-fhs)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# first-hop-security security-policy pol1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application ap1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# first-hop-security trust-control tcpol1
```

Additional Information:

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

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

1.12 CACI-L2-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

```
GROUP ID: V-272046
RULE ID: SV-272046r1114355
```

Rationale:

Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.

Cisco ACI provides numerous features to cover different use cases to restrict traffic between EPGs to help organizations in the segmentation and micro-segmentation journey. This includes features such as:

- Inter-VRF and Intra-VRF Contracts.
- Policy-based Redirection and layer 4 to layer 7 Services Insertion.
- Intra-EPG Isolation and Intra-EPG Contracts.
- vzAny Contracts.
- Endpoint Security Groups (ESG).

Organizations must make use of one or more of these Cisco ACI contracts and segmentation capabilities to provide segmentation within the data center for east-west traffic flows, as well as for north-south traffic flows, combined in this former case with other security devices or solutions to implement a defense-in-depth strategy.

Audit:

Verify one or more Cisco ACI contracts and/or segmentation capabilities to provide segmentation within the data center for east-west traffic and north-south traffic flows, combined in this former case with other security devices or solutions to implement a defense-in-depth strategy. The following is an example of deploying an EPG through an interface policy group to multiple interfaces to provide separation and isolation of traffic.

Associate the target EPG with the interface policy group. The sample command sequence specifies an interface policy group pg3 associated with VLAN domain, domain1, and with VLAN 1261. The application EPG, epg47 is deployed to all interfaces associated with this policy group. Check the target ports to verify deployment of the policies of the interface policy group associated with application EPG. The output of the sample "show command" sequence indicates that policy group pg3 is deployed on Ethernet port 1/20 on leaf switch 1017.

```
apic1# show run leaf 1017 int eth 1/20
# Command: show running-config leaf 1017 int eth 1/20
# Time: Mon Jun 27 22:12:10 2016
  leaf 1017
    interface ethernet 1/20
      policy-group pg3
```

If physical or logical separation of subnetworks to isolate organization-defined critical system components and functions has not been implemented, this is a finding.

Remediation:

Configure one or more Cisco ACI contracts and/or segmentation capabilities to provide segmentation within the data center for east-west traffic and north-south traffic flows, combined in this former case with other security devices or solutions to implement a defense-in-depth strategy. The following is an example of deploying an EPG through an interface policy group to multiple interfaces in order to provide separation and isolation of traffic.

Before beginning, ensure the following:

- The target application EPG is created.
- The VLAN pools have been created containing the range of VLANs to use for EPG deployment on the AEP.
- The physical domain has been created and linked to the VLAN Pool and AEP.
- The target attached entity profile is created and associated with the ports on which the application EPG will be deployed.

1. Associate the target EPG with the interface policy group. The sample command sequence specifies an interface policy group pg3 associated with VLAN domain, domain1, and with VLAN 1261. The application EPG, epg47 is deployed to all interfaces associated with this policy group.

```
apic1# configure terminal
apic1(config)# template policy-group pg3
```

Deploying an EPG through an Interface Policy Group to Multiple Interfaces

```
apic1(config-pol-grp-if)# vlan-domain member domain1
apic1(config-pol-grp-if)# switchport trunk allowed vlan 1261 tenant tn10
application pod1-AP
      epg epg47
```

2. Check the target ports to ensure deployment of the policies of the interface policy group associated with application EPG. The output of the sample "show command" sequence indicates that policy group pg3 is deployed on Ethernet port 1/20 on leaf switch 1017.

```
apic1# show run leaf 1017 int eth 1/20
# Command: show running-config leaf 1017 int eth 1/20
# Time: Mon Jun 27 22:12:10 2016
  leaf 1017
    interface ethernet 1/20
      policy-group pg3
      exit
    exit
ifav28-ifc1#
```

Additional Information:

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)

1.13 CACI-L2-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco ACI layer 2 switch must establish organization-defined alternate communication paths for system operations organizational command and control.

```
GROUP ID: V-272047
RULE ID: SV-272047r1113953
```

Rationale:

An incident, whether adversarial- or nonadversarial-based, can disrupt established communication paths used for system operations and organizational command and control. Alternate communication paths reduce the risk of all communication paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communication path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communication paths for command and control purposes, including designating alternative decision makers if primary decision makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization's ability to continue to operate and take appropriate actions during an incident.

To establish alternate communication paths for system operations and organizational command and control within a Cisco ACI cluster using the CLI, configure a multi-pod ACI architecture with separate APIC clusters, ensuring redundancy across pods by using external IP-routed networks (Inter-Pod Network) to maintain connectivity even if one pod experiences a failure. This effectively creates diverse communication pathways for management and control functions.

Audit:

If the connection type is remotely attached through a layer 3 network, this is not applicable.

Verify the cluster status.

```
apic1# cluster_health
```

If the status of the clustered nodes is not "OK", this is a finding.

Remediation:

Configure a multi-pod ACI architecture with separate APIC clusters with redundancy across pods using external IP-routed networks (Interpod Network) to connect them, allowing management access even if one pod experiences a failure.

Deploy at least two separate APIC clusters (pods).

```
apic1# conf t
apic1(config)# pod <pod_name>
apic1(config)# ip address <management_ip> <subnet_mask>
apic1(config)# ip route <destination_network> <next_hop_ip>
```

Additional Information:

CCI-004931 Establish organization-defined alternate communications paths for system operations organizational command and control.

- NIST SP 800-53 Revision 5::SC-47

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	CACI-L2-000001 (Manual)	☐	☐
1.2	CACI-L2-000002 (Manual)	☐	☐
1.3	CACI-L2-000004 (Manual)	☐	☐
1.4	CACI-L2-000005 (Manual)	☐	☐
1.5	CACI-L2-000009 (Manual)	☐	☐
1.6	CACI-L2-000010 (Manual)	☐	☐
1.7	CACI-L2-000011 (Manual)	☐	☐
1.8	CACI-L2-000014 (Manual)	☐	☐
1.9	CACI-L2-000015 (Manual)	☐	☐
1.10	CACI-L2-000016 (Manual)	☐	☐
1.11	CACI-L2-000017 (Manual)	☐	☐
1.12	CACI-L2-000018 (Manual)	☐	☐
1.13	CACI-L2-000019 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 21, 2025	1.0.0	Initial CIS Release