CISCO APPLICATION CENTRIC INFRASTRUCTURE (ACI) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

27 May 2025

Developed by DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Cisco Application Centric Infrastructure (ACI) Security Technical Implementation Guide (STIG) provides technical security configuration and assessment controls for Cisco ACI fabric and components. The ACI fabric appears as a single switch, capable of bridging and routing; thus, guidance consists of a package of three STIGs that together ensure the secure implementation of management, control, and data planes of the switch.

The DOD enterprise consists of hundreds of physical and virtual endpoints, requiring a complex set of policies and configurations. The ACI can be leveraged to provide centralized data center management, simplify policy distribution, and integrate analytics and forensic applications across the infrastructure. The ACI can also segment the architecture and distribute external routes from a border leaf to other leaf switches. This approach allows the data center network to grow without the risk of creating a failure domain that is too large.

The STIGs' primary scope is the management of network traffic within the data center, the associated functions of application-centric policies, and the automation of application connectivity. In addition to the layer 2 switching functions, layer 3 connectivity to external networks through the L3Out configuration is also assessed. However, acting as a traditional perimeter or edge router is out of scope. Custom applications that can be installed from various vendors to extend functionality are also out of scope.

ACI consists of three key components: the Application Policy Infrastructure Controller (APIC), the leaf switches, and the spine switches.

The APIC is a centralized controller that manages all aspects of the ACI fabric. It is a software-defined networking (SDN) solution that provides a policy-based software controller that centralizes access to all fabric information. The APIC interacts with leaf and spine switches to push configurations and enforce application policies. It also creates a fabric-based architecture that can support single-site or multi-site topologies, including multi-cloud and multi-tenant deployment models.

ACI uses Multi-Protocol Border Gateway Protocol (MP-BGP) with VPNv4 in the ACI infra-Virtual Routing and Forwarding (VRF) to distribute external routes from a border leaf to other leaf switches. All traffic in the ACI fabric is normalized as Virtual Extensible LAN (VXLAN) packets. VXLAN decouples layer 2 domains from the underlying layer 3 network infrastructure.

The spine-leaf network framework can be implemented as a two- or three-tier architecture using physical switches and/or virtual switches that combine into a virtual fabric using policies controlled by one or more APICs. Each leaf switch connects to one or more spine switches forming a mesh.

- Leaf switches: These devices have ports connected to classic Ethernet devices, such as servers, firewalls, and router ports. Leaf switches are at the edge of the fabric. The leaf switches are responsible for routing or bridging tenant packets and applying network policies.

- Spine switches: These devices interconnect leaf switches. They can also be used to build a Cisco ACI Multi-Pod fabric by connecting a Cisco ACI pod to an IP network or to a supported WAN device. Spine switches store all the endpoints-to-virtual tunnel endpoint (VTEP) mapping entries (spine switch proxies).

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a

STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.

2. ASSESSMENT CONSIDERATIONS

The Cisco ACI fabric consists of discrete components connected in a spine and leaf switch topology provisioned and managed as a single entity. The wide variations in architecture will be a challenge when completing checks and fixes. Example configurations are provided; however, the exact method and commands required for compliance with a given requirement may vary based on the architectural choices such as multi-tenants, multi-pods options, or the role of the fabric in the architecture. Some controls can be applied globally to the fabric versus directly to a leaf or VRF. Thus, the STIG package consists of multiple STIGs working together to secure the components of the fabric.

Custom applications that can be installed from various vendors to extend functionality are not covered by the STIG but should be assessed using the Application SRG.

2.1 Security Assessment Information

A security assessment of the Cisco ACI must consist of a security review of both the management backplane and the ACI security functions. The following STIGs are required as part of all assessments:

- Cisco ACI Network Device Management (NDM) STIG: Contains requirements applicable to secure administrative access, AAA logging, least privilege, account of last resort, and system control plane configuration. Some settings are also globally applicable.
- Cisco ACI Layer 2 Switch (L2S) STIG: Contains requirements applicable to securing layer 2 switch assessment.
- Cisco ACI Router (RTR) STIG: Contains requirements applicable to securing layer 3 switch assessment.