Framework Mapping:
Cisco Secure Firewalls and Firewall Management Center + CIS Controls v8.1

Background

Cisco Secure Firewalls and Firewall Management Center (FMC) give organizations a practical way to connect CIS Critical Security Controls v8.1 requirements to security controls they can deploy, operate, monitor, and document. Secure Firewalls provide the enforcement and inspection layer: boundary protection, segmentation, secure access, application control, URL filtering, intrusion prevention, malware and file inspection, encrypted traffic visibility, and detailed security-event telemetry. FMC adds centralized policy administration, monitoring, reporting, device health visibility, workflow evidence, and operational consistency across distributed firewall deployments.

For organizations using CIS as a security framework roadmap, the combined platform is particularly relevant where safeguards depend on network infrastructure management, network monitoring and defense, audit log management, malware defense, email and web protection, access control management, segmentation, and selected data-protection outcomes. In those areas, firewall enforcement, traffic inspection, policy control, logging, and event analysis can provide both operational protection and evidence that supports compliance discussions.

The mapping is intentionally scoped to what Cisco Firewalls and FMC can reasonably provide. Some CIS safeguards require enterprise governance, endpoint management, identity administration, user training, service-provider oversight, backup operations, or software development security programs. In those areas, Cisco Firewalls and FMC may still provide meaningful supporting evidence or compensating technical control value, but customers should pair that evidence with the appropriate process owner and adjacent security platforms.

CIS Controls v8.1 Overview

The CIS Critical Security Controls v8.1 are a prioritized set of safeguards for defending systems and networks against prevalent cyber attacks. For Cisco customers, the framework is useful because it turns broad security outcomes into specific safeguards that can be mapped to technology capabilities, operational ownership, and evidence.

CIS Controls v8.1 updates v8 with current alignment to industry standards and frameworks, revised asset classes and safeguard wording, and the Govern security function introduced in NIST Cybersecurity Framework 2.0. CIS publishes mapping resources and the CIS Controls Navigator so teams can see how CIS safeguards relate to other security standards and to the broader programs they already manage.

This crosswalk value matters in a multi-framework environment. CIS publishes individual mappings to frameworks such as NIST CSF 2.0, NIST SP 800-53 Rev. 5, NIST SP 800-171, ISO/IEC 27001, PCI DSS, SOC 2, and additional regulatory or industry frameworks. A CIS mapping can therefore help Cisco customers explain how firewall enforcement, monitoring, logging, segmentation, and policy-management evidence supports more than one compliance conversation.

Implementation Groups

Implementation Groups (IGs) are CIS's recommended prioritization model. IG1 is essential cyber hygiene: the baseline set of safeguards every enterprise should consider first because they address common attacks with practical, foundational controls. IG2 builds on IG1 for organizations with more complex environments, greater regulatory exposure, or higher operational risk. IG3 includes the full CIS Controls safeguard set and is designed for organizations with mature security programs,

significant risk exposure, or a need for the most comprehensive coverage.

In the mapping tables, the IG1/IG2/IG3 columns show where each safeguard sits in that adoption path. This lets a customer use the same Cisco firewall and FMC mapping for a phased roadmap: start with IG1 priorities, expand into IG2 as the program matures, and use IG3 where the organization requires full CIS coverage.

Major Controls at a Glance

The CIS Controls v8.1 provide a prioritized set of 18 cybersecurity best practices designed to help organizations strengthen their security posture, reduce cyber risk, and improve resilience against modern threats. The controls are organized around key areas of security governance, asset management, vulnerability management, access control, monitoring, and incident response. Together, they offer a practical, risk-based framework that helps organizations establish foundational security capabilities while aligning security resources to the most effective defensive measures. The following table summarizes the 18 CIS Controls at a high level. Detailed descriptions for each control are provided in subsequent sections of this document.

Table 1. CIS Controls v8.1

Control Number	Control Title
Control 1	Inventory and Control of Enterprise Assets
Control 2	Inventory and Control of Software Assets
Control 3	Data Protection
Control 4	Secure Configuration of Enterprise Assets and Software
Control 5	Account Management
Control 6	Access Control Management
Control 7	Continuous Vulnerability Management
Control 8	Audit Log Management
Control 9	Email and Web Browser Protections
Control 10	Malware Defenses
Control 11	Data Recovery
Control 12	Network Infrastructure Management
Control 13	Network Monitoring and Defense
Control 14	Security Awareness and Skills Training
Control 15	Service Provider Management
Control 16	Application Software Security
Control 17	Incident Response Management
Control 18	Penetration Testing

Cisco Product Overview

Cisco Secure Firewall

Cisco Secure Firewall helps organizations protect their users, applications, data, and critical infrastructure across on-premises, cloud, hybrid, branch, industrial, and IoT environments. By providing broad visibility and control over network traffic, Secure Firewall helps enable security teams to reduce risk, enforce security policies consistently, and strengthen their overall security posture.

Within the context of the CIS Controls v8.1, Cisco Secure Firewall plays a key role in helping organizations implement network security practices through capabilities such as network segmentation, access control enforcement, application visibility and control, intrusion prevention, malware and file inspection, URL filtering, encrypted traffic analysis, remote-access security, and security-event logging. These capabilities help organizations limit attack surfaces, detect and block malicious activity, and maintain greater visibility into network communications.

Powered by Cisco Talos threat intelligence and advanced Snort® detection technology, Cisco Secure Firewall helps customers identify emerging threats and respond more effectively to security events. Its integration with identity, analytics, logging, security operations, and extended detection and response (XDR) platforms further enables organizations to support CIS Controls related to network management, threat detection, malware defense, access control, audit logging, and continuous monitoring.

.

Firewall Management Center (FMC)

Cisco Firewall Management Center (FMC) provides a centralized platform for managing, monitoring, and optimizing Cisco Secure Firewall deployments across the enterprise. FMC helps organizations streamline security operations by enabling consistent policy administration, comprehensive visibility, and simplified management from a single interface.

For organizations with multiple firewalls deployed across campus, branch, data center, cloud, or hybrid environments, FMC provides the operational framework needed to maintain standardized security controls and support consistent policy enforcement. Security teams can centrally manage access control, intrusion prevention, malware protection, URL filtering, application control, and segmentation policies while maintaining visibility into security events and network activity.

From a CIS Controls perspective, FMC enhances an organization's ability to implement and operationalize security controls by providing centralized policy management, network discovery, device health monitoring, event correlation, reporting, alerting, and investigation workflows. These capabilities support ongoing monitoring, audit readiness, threat detection, incident investigation, and security operations efficiency. Available in physical, virtual, and cloud-delivered deployment models, FMC enables organizations to extend consistent security management practices across diverse environments while scaling to meet evolving business and security requirements.

How to Interpret the Mapping

The CIS Controls mappings in this document evaluate the combined contributions of Cisco Secure Firewall and Firewall Management Center (FMC). While Secure Firewall provides security enforcement and threat-prevention capabilities at the network layer, FMC delivers the centralized management, visibility, reporting, and operational workflows needed to deploy, monitor, and maintain those controls consistently across the environment.

The following capability areas provide a useful framework for understanding how each solution contributes to CIS Controls implementation.

Table 2. CIS alignment value

Capability Area	Cisco Secure Firewall Benefits	Cisco Firewall Management Center (FMC) Benefits
Network Security Enforcement	Network segmentation, access control, VPN services, application visibility and control, and policy enforcement across network boundaries.	Centralized policy creation, deployment, validation, change management, and policy consistency across firewall deployments.
Threat Prevention and Detection	Intrusion prevention, Snort-based threat detection, malware and file inspection, URL filtering, and encrypted traffic visibility.	Centralized management of intrusion, malware, file, URL, and application policies, along with event aggregation and correlation.
Visibility, Monitoring, and Reporting	Collection of connection, intrusion, malware, URL, VPN, and policy events that provide operational security visibility.	Dashboards, reporting, event analysis, device health monitoring, audit data, and integrations with SIEM, logging, and security operations platforms.
Incident Response and Operations	Supports containment and mitigation actions through policy enforcement, traffic blocking, and security integrations.	Provides investigation workflows, operational context, policy deployment capabilities, reporting, and integration-driven response support.

Detailed CIS Controls Mapping Tables

The following sections map Cisco Secure Firewall and Firewall Management Center (FMC) capabilities to CIS Controls v8.1. Each control and its safeguards are evaluated to show how Secure Firewall and FMC meet or support control requirements, helping organizations understand their role in supporting CIS Control objectives within a defense-in-depth security strategy. Mapping tables identify the applicable Implementation Group (IG1, IG2, and IG3), asset types, and security functions (Identify, Protect, Detect, Respond, and Recover). Safeguards are categorized as either:

- **Meets** – Cisco Secure Firewall or FMC directly provides capabilities that satisfy the intent of the safeguard.
- **Supports** – Cisco Secure Firewall or FMC contributes to the implementation of the safeguard but may require complementary technologies, processes, or organizational controls to fully address the requirement.

Not all CIS Controls and safeguards are directly addressed by network security technologies. Where a control focuses primarily on areas such as governance, policy, risk management, or workforce training, a mapping table may not be included. These controls remain important components of a comprehensive cybersecurity program and are therefore included for completeness, along with a description of their purpose and relevance within the CIS Controls framework.

Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	Identify	X	X	X		Supports		Supports
1.2	Address Unauthorized Assets	Devices	Respond	X	X	X		Supports		Supports
1.3	Utilize an Active Discovery Tool	Devices	Detect		X	X		Supports		Supports
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices	Identify		X	X		Supports		Supports
1.5	Use a Passive Asset Discovery Tool	Devices	Detect			X		Supports	Meets	

Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
2.1	Establish and Maintain a Software Inventory	Software	Identify	X	X	X		Supports		Supports
2.2	Ensure Authorized Software is Currently Supported	Software	Identify	X	X	X		Supports		Supports
2.3	Address Unauthorized Software	Software	Respond	X	X	X		Supports		Supports
2.4	Utilize Automated Software Inventory Tools	Software	Detect		X	X		Supports		Supports
2.5	Allowlist Authorized Software	Software	Protect		X	X		Supports		Supports
2.6	Allowlist Authorized Libraries	Software	Protect		X	X		Supports		Supports
2.7	Allowlist Authorized Scripts	Software	Protect			X		Supports		Supports

Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
3.1	Establish and Maintain a Data Management Process	Data	Govern	X	X	X		Supports		Supports
3.2	Establish and Maintain a Data Inventory	Data	Identify	X	X	X		Supports		Supports
3.3	Configure Data Access Control Lists	Data	Protect	X	X	X	Meets			Supports
3.4	Enforce Data Retention	Data	Protect	X	X	X		Supports		Supports
3.7	Establish and Maintain a Data Classification Scheme	Devices	Identify		X	X		Supports		Supports
3.8	Document Data Flows	Data	Identify		X	X		Supports		Supports
3.10	Encrypt Sensitive Data in Transit	Data	Protect		X	X		Supports		Supports
3.12	Segment Data Processing and Storage-Based on Sensitivity	Data	Protect		X	X		Supports		Supports
3.13	Deploy a Data Loss Prevention Solution	Data	Protect			X		Supports		Supports
3.13	Deploy a Data Loss Prevention Solution	Data	Protect			X		Supports		Supports
3.14	Log Sensitive Data Access	Data	Detect			X		Supports		Supports

Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
4.1	Establish and Maintain a Secure Configuration Process	Documentation	Govern	X	X	X		Supports		Supports
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Documentation	Govern	X	X	X		Supports		Supports
4.3	Configure Automatic Session Locking on Enterprise Assets	Devices	Protect	X	X	X		Supports		Supports
4.6	Securely Manage Enterprise Assets and Software	Devices	Protect	X	X	X		Supports		Supports
4.7	Manage Default Accounts on Enterprise Assets and Software	Users	Protect	X	X	X		Supports		Supports
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Devices	Protect		X	X		Supports		Supports
4.9	Configure Trusted DNS Servers on Enterprise Assets	Devices	Protect		X	X		Supports		Supports

Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
5.1	Establish and Maintain an Inventory of Accounts	Users	Identify	X	X	X		Supports		Supports
5.2	Use Unique Passwords	Users	Protect	X	X	X		Supports		Supports
5.3	Disable Dormant Accounts	Users	Protect	X	X	X		Supports		Supports
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	Protect	X	X	X		Supports		Supports
5.5	Establish and Maintain an Inventory of Service Accounts	Users	Identify		X	X		Supports		Supports
5.6	Centralize Account Management	Users	Protect		X	X		Supports	Meets	

Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
6.1	Establish an Access Granting Process	Documentation	Govern	X	X	X		Supports		Supports
6.2	Establish an Access Revoking Process	Documentation	Govern	X	X	X		Supports		Supports
6.3	Require MFA for Externally-Exposed Applications	Users	Protect	X	X	X		Supports		Supports
6.4	Require MFA for Remote Network Access	Users	Protect	X	X	X		Supports		Supports
6.5	Require MFA for Administrative Access	Users	Protect	X	X	X		Supports		Supports
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Software	Identify		X	X		Supports		Supports
6.7	Centralize Access Control	Users	Protect		X	X		Supports		Supports
6.8	Define and Maintain Role-Based Access Control	Users	Govern			X		Supports	Meets	

Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
7.1	Establish and Maintain a Vulnerability Management Process	Documentation	Govern	X	X	X		Supports		Supports
7.2	Establish and Maintain a Remediation Process	Documentation	Govern	X	X	X		Supports		Supports
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Software	Identify		X	X		Supports		Supports
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Software	Identify		X	X		Supports		Supports
7.7	Remediate Detected Vulnerabilities	Software	Respond		X	X		Supports		Supports

Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
8.1	Establish and Maintain an Audit Log Management Process	Documentation	Govern	X	X	X		Supports		Supports
8.2	Collect Audit Logs	Data	Detect	X	X	X		Supports	Meets	
8.3	Ensure Adequate Audit Log Storage	Data	Protect	X	X	X		Supports		Supports
8.4	Standardize Time Synchronization	Network	Protect		X	X		Supports		Supports
8.5	Collect Detailed Audit Logs	Data	Detect		X	X		Supports	Meets	
8.6	Collect DNS Query Audit Logs	Data	Detect		X	X		Supports		Supports
8.7	Collect URL Request Audit Logs	Data	Detect		X	X	Meets			Supports
8.8	Collect Command-Line Audit Logs	Data	Detect		X	X		Supports		Supports
8.9	Centralize Audit Logs	Data	Detect		X	X		Supports	Meets	
8.10	Retain Audit Logs	Data	Protect		X	X		Supports		Supports
8.11	Conduct Audit Log Reviews	Data	Detect		X	X		Supports		Supports
8.12	Collect Service Provider Logs	Data	Detect			X		Supports		Supports

Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
9.2	Use DNS Filtering Services	Devices	Protect	X	X	X		Supports		Supports
9.3	Maintain and Enforce Network-Based URL Filters	Network	Protect		X	X	Meets			Supports
9.6	Block Unnecessary File Types	Network	Protect		X	X		Supports		Supports

Control 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
10.1	Deploy and Maintain Anti-Malware Software	Devices	Detect	X	X	X		Supports		Supports
10.2	Configure Automatic Anti-Malware Signature Updates	Devices	Protect	X	X	X		Supports		Supports
10.5	Enable Anti-Exploitation Features	Devices	Protect		X	X		Supports		Supports
10.6	Centrally Manage Anti-Malware Software	Devices	Protect		X	X		Supports		Supports
10.7	Use Behavior-Based Anti-Malware Software	Devices	Detect		X	X		Supports		Supports

Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
11.2	Perform Automated Backups	Data	Recover	X	X	X				Supports
11.3	Protect Recovery Data	Data	Protect	X	X	X				Supports
11.5	Test Data Recovery	Data	Recover		X	X				Supports

Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
12.1	Ensure Network Infrastructure is Up-to-Date	Network	Protect	X	X	X		Supports		Supports
12.2	Establish and Maintain a Secure Network Architecture	Network	Protect		X	X		Supports		Supports
12.3	Securely Manage Network Infrastructure	Network	Protect		X	X		Supports		Supports
12.4	Establish and Maintain Architecture Diagram(s)	Documentation	Govern		X	X		Supports		Supports
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	Network	Protect		X	X		Supports		Supports

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
12.6	Use of Secure Network Management and Communication Protocols	Network	Protect		X	X		Supports		Supports
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Devices	Protect		X	X	Meets			Supports
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Devices	Protect			X		Supports		Supports

Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
13.1	Centralize Security Event Alerting	Network	Detect		X	X		Supports	Meets	
13.2	Deploy a Host-Based Intrusion Detection Solution	Devices	Detect		X	X		Supports		Supports
13.3	Deploy a Network Intrusion Detection Solution	Network	Detect		X	X	Meets			Supports
13.4	Perform Traffic Filtering Between Network Segments	Network	Protect		X	X	Meets			Supports
13.5	Manage Access Control for Remote Assets	Devices	Protect		X	X		Supports		Supports
13.6	Collect Network Traffic Flow Logs	Network	Detect		X	X	Meets		Meets	
13.7	Deploy a Host-Based Intrusion Prevention Solution	Devices	Protect			X		Supports		Supports
13.8	Deploy a Network Intrusion Prevention Solution	Network	Protect			X	Meets			Supports
13.9	Deploy Port-Level Access Control	Network	Protect			X		Supports		Supports
13.10	Perform Application Layer Filtering	Network	Protect			X	Meets			Supports
13.11	Tune Security Event Alerting Thresholds	Network	Detect			X		Supports	Meets	

Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

This control is primarily addressed through organizational policies, processes, and employee education programs. While Cisco Secure Firewall and Firewall Management Center (FMC) are not designed to directly implement security awareness and training activities, they serve as important components of a defense-in-depth security strategy by helping organizations enforce security policies, monitor network activity, and reduce exposure to cyber threats addressed through workforce awareness initiatives.

Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
15.4	Ensure Service Provider Contracts Include Security Requirements	Documentation	Govern		X	X		Supports		Supports
15.5	Assess Service Providers	Users	Govern			X		Supports		Supports
15.6	Monitor Service Providers	Data	Govern			X		Supports		Supports

Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	Software	Protect		X	X		Supports		Supports
16.8	Separate Production and Non-Production Systems	Network	Protect		X	X		Supports		Supports
16.10	Apply Secure Design Principles in Application Architectures	Software	Protect		X	X		Supports		Supports
16.13	Conduct Application Penetration Testing	Software	Govern			X		Supports		Supports
16.14	Conduct Threat Modeling	Software	Protect			X		Supports		Supports

Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
17.1	Designate Personnel to Manage Incident Handling	Users	Respond	X	X	X		Supports		Supports
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Documentation	Govern	X	X	X		Supports		Supports
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Documentation	Govern	X	X	X		Supports		Supports
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Documentation	Govern		X	X		Supports		Supports
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Documentation	Govern		X	X		Supports		Supports
17.4	Establish and Maintain an Incident Response Process	Documentation	Govern		X	X		Supports		Supports
17.5	Assign Key Roles and Responsibilities	Users	Respond		X	X		Supports		Supports
17.6	Define Mechanisms for Communicating During Incident Response	Users	Respond		X	X		Supports		Supports
17.7	Conduct Routine Incident Response Exercises	Users	Recover		X	X		Supports		Supports
17.8	Conduct Post-Incident Reviews	Users	Recover		X	X		Supports		Supports
17.9	Establish and Maintain Security Incident Thresholds	Documentation	Recover			X		Supports		Supports

Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Firewalls Meet	Firewalls Supports	FMC Meet	FMC Supports
18.1	Establish and Maintain a Penetration Testing Program	Documentation	Govern		X	X		Supports		Supports
18.2	Perform Periodic External Penetration Tests	Network	Detect		X	X		Supports		Supports
18.3	Remediate Penetration Test Findings	Network	Protect		X	X		Supports		Supports
18.4	Validate Security Measures	Network	Protect			X		Supports		Supports
18.5	Perform Periodic Internal Penetration Tests	Network	Detect			X		Supports		Supports

Key Observations

1. Strong Alignment to Network Security and Defense:

- Cisco Secure Firewall and Firewall Management Center align strongly with CIS safeguards focused on network infrastructure management, network monitoring, access control enforcement, intrusion prevention, and threat detection.

- Together, the platform helps customers strengthen control areas such as secure network architecture, traffic inspection, segmentation, policy enforcement, and response to suspicious or unauthorized activity.

2. Centralized Policy Management and Operational Consistency:

- FMC provides centralized management for firewall policy, events, configuration, reporting, and operational oversight, helping customers apply security controls consistently across distributed environments.
-
- This is especially valuable for CIS safeguards that require repeatable processes, documented control operation, audit visibility, and ongoing management of network security controls.

3. Meaningful Support for Visibility, Logging, and Audit Evidence:

- Cisco Secure Firewall and FMC support CIS compliance by generating and centralizing security events, connection data, intrusion events, malware events, and policy activity that can be used for audit, investigation, and reporting.

- These capabilities are particularly relevant to CIS controls related to audit log management, network monitoring and defense, malware defenses, incident response, and continuous security operations.

4. Threat Prevention and Response Value:

- Cisco Secure Firewall supports proactive defense through capabilities such as intrusion prevention, malware protection, URL filtering, application visibility and control, encrypted traffic handling, and threat intelligence from Cisco Talos.

- FMC strengthens response workflows by helping customers correlate events, review security activity, tune policies, and document actions taken during investigation or remediation.

5. Complementary Role in Broader CIS Compliance:

- Cisco Secure Firewall and FMC provide technical support for network-centered CIS safeguards, but some controls require complementary tools, processes, or ownership outside the firewall platform.

Areas such as workforce training, identity lifecycle management, endpoint configuration, backup and recovery, software development, and service-provider governance should be addressed through the broader security program, with firewall and FMC evidence used where it supports those outcomes.

Summary

Cisco Secure Firewalls and FMC support customers' efforts to map selected Cisco capabilities to CIS Controls v8.1 by combining enforcement, telemetry, centralized policy, and operational evidence. Secure Firewalls provide the network security enforcement layer: they enforce access controls, segment traffic, inspect applications, filter URLs, analyze files and malware, detect intrusions, support secure remote access, and generate high-value security events. FMC provides the management and visibility plane: it helps deploy consistent controls, tune policies, monitor device health, analyze events, and preserve evidence for compliance and response workflows.

The combined value is strongest where CIS safeguards depend on network visibility, boundary defense, traffic inspection, centralized logging, monitoring, policy consistency, and response support. For safeguards that require enterprise-wide governance, endpoint configuration, user training, service-provider management, software development lifecycle control, or data lifecycle ownership, Cisco Firewalls and FMC are positioned as supporting technical controls that should be paired with the appropriate process owner and adjacent security platforms.

Resources

For more information, please refer to the following:

- CIS Critical Security Controls v8.1
- CIS Critical Security Controls Implementation Groups
- CIS Controls Navigator and framework mappings
- Cisco Secure Firewall product page
- Cisco Secure Firewall Management Center product page
- Framework Mapping: Cisco Secure Firewall + NIST CSF 2.0