Framework Mapping: Cisco Firewalls + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

The National Institute of Standards (NIST) Cybersecurity Framework (CSF) 2.0 is a voluntary set of guidelines developed to help organizations manage and reduce cybersecurity risks. While voluntary, its adoption can significantly improve an organization's security posture by offering a structured approach to risk management.

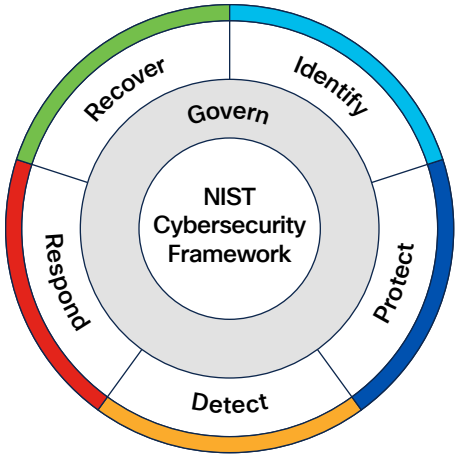
In February 2024, NIST released the CSF 2.0, updating version 1.1 from April 2018. This update incorporates feedback from various industries and stakeholders, enhancing the framework's flexibility, applicability, and relevance. The NIST CSF 2.0 continues to serve as a voluntary, risk-based framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, foster resilience, and align with best practices.

Purpose of the Framework

The NIST Cybersecurity Framework provides a structured yet flexible approach to improving an organization's cybersecurity posture. It is used for:

- **Assessing Risks:** Identifying, analyzing, and prioritizing cybersecurity risks
- **Guiding Cybersecurity Programs:** Establishing or improving cybersecurity strategies in alignment with organizational goals
- **Enhancing Communication:** Facilitating clear communication about cybersecurity risks and strategies among technical teams, leadership, and external stakeholders

The framework is particularly valuable for organizations that lack formalized cybersecurity programs or resources, though it is robust enough to benefit even the most mature organizations.



Key Components of the NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 maintains the foundational structure of the original framework while introducing several enhancements. Its key components are:

Core Functions

The Framework Core outlines six **high-level functions** that provide a strategic view of cybersecurity risk management.

These functions remain foundational in CSF 2.0 and are as follows:

- **Govern:** Establish and oversee policies, roles, processes, and accountability to align cybersecurity efforts with organizational objectives and regulatory requirements.

  Examples: Risk management policies, executive accountability, cybersecurity governance framework

- **Identify:** Develop an understanding of cybersecurity risks to systems, assets, data, and capabilities. This involves identifying critical resources, threats, and vulnerabilities.

  Examples: Asset management, governance, risk assessments

- **Protect:** Implement safeguards to ensure the delivery of critical services and mitigate risks.

  Examples: Access control, data protection, training, and maintenance

- **Detect:** Establish systems to identify cybersecurity events or anomalies in a timely manner.

  Examples: Continuous monitoring, intrusion detection, and threat intelligence

- **Respond:** Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

  Examples: Incident response planning, mitigation strategies, and communication

- **Recover:**
  Develop plans to restore operations and reduce the impact of cybersecurity incidents.

  Examples: Disaster recovery, business continuity planning, and lessons learned

Implementation Tiers

The framework includes **Implementation Tiers** to help organizations evaluate their current cybersecurity practices and set goals for improvement. These tiers reflect the degree to which an organization's cybersecurity practices are informed by risk management processes, integrated with business needs, and adaptive to evolving risks:

Tier 1 (Partial): Limited awareness and ad hoc implementation of cybersecurity practices

Tier 2 (Risk-Informed): Risk management practices are formally defined but not fully integrated

Tier 3 (Repeatable): Cybersecurity practices are consistently applied and documented across the organization

Tier 4 (Adaptive): Practices are continuously improved and proactively adapted to changing risks.

Profiles

The **Framework Profiles** allow organizations to align the framework to their specific goals, resources, and risk tolerance. A profile compares the current state of an organization's cybersecurity practices to its desired state, serving as a roadmap for improvement.

Why Use the NIST Cybersecurity Framework?

Organizations adopt the NIST CSF 2.0 for several reasons:

Flexibility: Its non-prescriptive nature allows organizations to tailor it to their unique needs.

Widely Recognized: The framework is globally acknowledged as a standard for cybersecurity best practices.

Risk Management: It helps organizations prioritize risks and allocate resources effectively.

Compliance Alignment: While voluntary, the framework aligns with various regulatory requirements and standards, simplifying compliance efforts.

Mapping to Other Frameworks

The NIST National Online Informative References (OLIR) Program provides a framework for organizations to map cybersecurity standards, guidelines, and frameworks. By leveraging OLIR, Cisco can cross-reference the NIST Cybersecurity Framework (CSF) 2.0 with other standards like NIST SP 800-53, simplifying compliance and security alignment. This approach eliminates the need for separate mappings, saving time and effort while ensuring traceability across frameworks.

For Cisco®, this means that once its security solutions, such as Cisco Firewalls, are mapped to NIST CSF 2.0, these mappings can be extended through NIST OLIR to align with other frameworks. This capability is particularly beneficial for public sector and regulated industries, where compliance with multiple frameworks is often required. By using NIST CSF 2.0 as a common backbone, Cisco helps customers achieve compliance efficiently while demonstrating how its solutions align with best practices and regulatory mandates.

This cross-mapping capability strengthens Cisco's position as a strategic enabler of cybersecurity compliance, providing customers with a clear understanding of how its solutions fit into their broader compliance and risk management strategies.

Understanding Cisco Firewalls

As cyber threats evolve in complexity and scale, traditional firewalls may no longer be sufficient to safeguard organizations from sophisticated attacks. Cisco Secure Firewall is designed to address modern security challenges by providing advanced features that extend beyond traditional packet filtering and stateful inspection. By integrating a variety of security capabilities into a single platform, Cisco Secure Firewall help organizations achieve robust protection while maintaining operational efficiency.

What Are Next-Generation Firewalls?

A **Next-Generation Firewall** is a modern cybersecurity solution that combines traditional firewall capabilities with advanced features such as deep packet inspection, intrusion prevention, application awareness, and threat intelligence integration. Cisco Secure Firewall go a step further by leveraging automation, machine learning, and real-time threat intelligence to proactively defend against known and unknown threats.

Cisco's NGFWs are part of its Secure Firewall family, which includes models designed to meet the needs of small businesses, enterprises, and data centers. They are built to provide deep visibility, automated threat protection, and simplified management, all while ensuring high performance.

Benefits of Cisco NGFWs

Cisco Secure Firewall offer several advantages for organizations seeking to strengthen their cybersecurity posture:

Comprehensive Protection: By combining multiple security functions into one platform, Cisco Secure Firewall simplify the implementation of a layered defense strategy.

Proactive Threat Prevention: Real-time threat intelligence and advanced detection capabilities enable Cisco Secure Firewall to block threats before they cause harm.

Operational Efficiency: Automation and centralized management reduce the administrative burden on IT teams, allowing them to focus on strategic initiatives.

Enhanced Visibility: Deep insights into applications, users, and devices provide greater visibility into network activity, helping organizations identify and mitigate risks faster.

Future-Ready Security: Cisco Secure Firewall are designed to integrate seamlessly with Cisco's broader security portfolio, ensuring organizations can scale and adapt to new threats as their needs evolve.

Cisco NGFW Deployment Options

Cisco offers a range of NGFW models to accommodate diverse use cases and deployment scenarios:

Cisco Firepower NGFW: These appliances are designed for advanced threat protection and come in various models, from small branch office firewalls to high-performance enterprise-grade devices.

Cisco Secure Firewall Threat Defense Virtual (formerly FTDv): A virtualized version of Cisco Secure Firewall, enabling deployment in private, public, and hybrid cloud environments.

Cisco Meraki™ MX: A cloud-managed NGFW that is ideal for organizations looking for simplified deployment and management without sacrificing security.

Technical Features

Cisco NGFWs are equipped with a broad range of features that enhance their ability to protect against modern threats. Below are some of the key capabilities:

Deep Packet Inspection (DPI)

Cisco Secure Firewall perform deep packet inspection to analyze the contents of network traffic beyond the header information. This enables the firewall to detect malicious payloads, prevent data exfiltration, and enforce granular security policies.

Application Awareness and Control

Traditional firewalls operate at the network layer, which limits their ability to differentiate between applications. Cisco Secure Firewall incorporate application-layer intelligence, allowing administrators to identify, monitor, and control specific applications (e.g., social media, SaaS platforms) based on organizational policies.

Advanced Threat Detection and Prevention

Cisco Secure Firewall include built-in **Intrusion Prevention Systems (IPS)** that can detect and block known vulnerabilities, exploits, and attacks. By leveraging Cisco Talos®, one of the largest commercial threat intelligence teams in the world, the NGFWs stay updated with real-time global threat intelligence to combat emerging threats.

URL Filtering

Cisco Secure Firewall provide URL filtering to block access to malicious or inappropriate websites. The solution uses Cisco's intelligence to categorize and evaluate URLs, preventing users from interacting with compromised or harmful domains.

Integrated Malware Protection

Cisco Secure Firewall are integrated with **Cisco Secure Endpoint** (formerly AMP for Endpoints) to deliver advanced malware protection. This feature allows for continuous monitoring, file analysis, and retrospective alerts to address threats that may bypass initial defenses.

Encrypted Traffic Inspection

With the growing use of encryption, attackers often hide malicious activity within encrypted traffic. Cisco NGFWs have the capability to inspect encrypted traffic (Secure Sockets Layer/Transport Layer Security) (SSL/TLS) without compromising performance or user privacy, ensuring that threats are not masked by encryption.

Automation and Orchestration

Cisco Secure Firewall integrate with other Cisco security products and third-party solutions through APIs. Automation features streamline incident response, policy updates, and threat remediation, reducing the workload for security teams.

Scalability and Performance

Cisco Secure Firewall portfolio includes options for every size and type of deployment, from branch offices to large-scale data centers. These firewalls are optimized for high throughput and low latency, ensuring performance remains consistent even under heavy loads.

Threat Intelligence

Cisco Secure Firewall leverage Cisco Talos to provide real-time threat intelligence. This ensures that the firewall can adapt to emerging threats and protect against zero-day attacks.

Centralized Management

Cisco has the following management solutions are available to manage Cisco Secure Firewalls depending on your mission and/or environment. This allows customers the ability to configure, monitor, and control multiple security devices and policies from a single, unified interface, simplifying administration and improving visibility across the entire network.

1. Firewall Management Center (FMC)

- Provides centralized management for Cisco Secure Firewalls.
- Can be deployed on-premises, as a virtual appliance, or in the cloud.
- Allows administrators to configure policies, monitor security events, and track compliance across the network.
- Designed for managing multiple firewalls from a single, unified interface.

2. Cisco Security Cloud Control (formerly Cisco Defense Orchestrator)

- Delivers cloud-based centralized management for Cisco Secure Firewalls.
- Unites management across multiple Cisco Security solutions, not just firewalls.
- Simplifies policy and configuration management through a single, cloud-hosted interface.
- Supports orchestration and automation across distributed environments.

3. Firewall Device Manager (FDM)

- Provides on-box, local management for individual Cisco Secure Firewalls.
- Allows direct management through the firewall's web interface.
- Enables administrators to configure policies, monitor events, and manage compliance on a single device.
- Ideal for smaller deployments or single-device environments.

Mapping Cisco Firewalls to NIST CSF 2.0

Cisco NGFW for Government Capability Mapping to NIST CSF 2.0 and NIST 800-53

Function	Category	Cisco NGFW NIST CSF 2.0 Mapping (Meets)	Cisco NGFW NIST CSF 2.0 Mapping (Supports)	Cisco NGFW NIST 800-53 Mapping (Meets)	Cisco NGFW NIST 800-53 Mapping (Suports)
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)		ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-08		CM-08, PM-05, AC-20, SA-05, SA-09, AC-04, CA-03, CA-09, PL-02, PL-08, PM-07, SR-02, CM-09, CM-13, MA-02, MA-06, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
	Risk Assettment (ID.RA)	ID.RA-02, ID.RA-09	ID.RA-01	SI-05, PM-15, PM-16, SA-04, SA-05, SA-10, SA-11, SA-15, SA-17, SI-07, SR-05, SR-06, SR-10, SR-11	CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05
	Improvement (ID.IM)	Non-technical controls			
Protect (PR)	Identity, Management, Authentication, and Access Control (PR.AA)	PR.AA-01, PR.AA-03, PR.AA-04, PR.AA-05		AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11, IA-13, AC-03, AC-05, AC-06, AC-07, AC-10, AC-12, IA-13, AC-16, AC-17, AC-18, AC-19, AC-24	
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)	PR.DS-01, PR.DS-02, PR.DS-11		CA-03, CP-09, MP-08, SC-04, SC-07, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-03, SI-04, SI-07, AU-16, CA-03, SC-08, SC-11, SC-16, SC-40, CP-06	
	Platfrom Security (PR.PS)	PR.PS-01, PR.PS-04, PR.PS-05	PR.PS-02, PR.PS-06	CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, SC-34	CM-11, MA-03(06), SI-02, SI-07, SA-03, SA-08, SA-10, SA-11, SA-15, SA-17
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01, PR.IR-03	PR.IR-02, PR.IR-04	AC-03, AC-04, SC-04, SC-05, SC-07, CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13	CP-02, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-23, CP-06, CP-07, CP-08, PM-03, PM-09
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM-01, DE.CM-06	DE.CM-03, DE.CM-09	AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04, PS-07, SA-04, SA-09	AC-02, AU-12, AU-13, CA-07, CM-10, CM-11, AC-04, AC-09, AU-12, CM-03, CM-06, SC-34, SC-35, SI-04, SI-07
	Adverse Event Analysis (DE.AE)	DE.AE-02, DE.AE-03, DE.AE-06, DE.AE-07, DE.AE-08	DE.AE-04	AU-06, CA-07, IR-04, SI-04, AU-06, CA-07, PM-16, IR-04, IR-05, IR-08, SI-04, IR-04, PM-15, PM-16, RA-03, RA-10, PM-16, RA-03, RA-10, IR-04, IR-08	PM-09, PM-11, PM-18, PM-28, PM-30
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)	RS.AN-08	RS.AN-03, RS.AN-07	IR-04, IR-08, RA-03, RA-07	AU-07, IR-04, AU-07, IR-04, IR-06
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls			
	Incident Mitigation (RS.MI)		RS.MI-01, RS.MI-02		IR-04
Recover (RC)	Incident Recovery Plan Execution (RC.RP)		RC.RP-03, RC.RP-05		CP-02, CP-04, CP-09, CP-10
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Conclusion

The NIST Cybersecurity Framework 2.0 builds on the strengths of the original framework while addressing the dynamic nature of cybersecurity challenges. By providing a flexible, scalable, and comprehensive approach to risk management, the framework empowers organizations to enhance their cybersecurity posture, improve resilience, and ensure the continuity of critical operations. Whether an organization is just beginning its cybersecurity journey or looking to refine an established program, CSF 2.0 serves as a robust guide for navigating today's complex threat landscape.

Cisco Secure Firewalls provide a powerful, all-encompassing solution to address the ever-growing cybersecurity challenges faced by modern organizations. By combining advanced threat prevention, application awareness, and centralized management with real-time threat intelligence, Cisco Secure Firewalls enable organizations to protect their networks, assets, and users against both known and emerging threats. Whether deployed on-premises, in the cloud, or in hybrid environments, Cisco Secure Firewalls offer the scalability, performance, and flexibility organizations need to maintain a strong security posture in today's dynamic threat landscape.

By aligning with the NIST CSF 2.0, Cisco Secure Firewalls not only help organizations manage their cybersecurity risks but also streamline regulatory compliance and improve communication between technical teams and leadership. Their scalability, performance, and ease of management make them an asset for organizations seeking to implement the NIST CSF 2.0 effectively, whether they are just beginning their cybersecurity journey or optimizing a mature program.

C11-5299696-00 07/25