Framework Mapping: Cisco Secure Firewall + CISA Zero Trust Model

© 2025 Cisco and/or its affiliates. All rights reserved.

Background

U.S. Public Sector organizations are embarking on a Zero Trust roadmap—a structured and phased approach to transition its cybersecurity framework toward a more mature and resilient Zero Trust Architecture (ZTA). This roadmap aligns with best practices outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-207 and the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM).

By leveraging these frameworks, U.S. Public Sector Organizations can adopt a comprehensive strategy to strengthen its security posture across all five CISA Zero Trust pillars—**Identity, Device, Network/Environment, Application Workload,** and **Data**.

1. **Identity:** Focuses on verifying and managing the identities of users, processes, and systems, ensuring access is granted only to authenticated and authorized entities based on least privilege principles.
2. **Device:** Ensures that all devices accessing the network are identified, monitored, and meet security compliance standards to reduce potential attack surfaces.
3. **Network/Environment:** Emphasizes secure network segmentation, dynamic access controls, and monitoring of traffic flows to limit lateral movement and protect resources within hybrid, cloud, and on-premises environments.
4. **Application Workload:** Protects applications and workloads by enforcing secure access, implementing runtime monitoring, and ensuring that interactions between applications are trusted and compliant.
5. **Data:** Focuses on protecting sensitive information through classification, encryption, monitoring, and policies that prevent unauthorized access or exfiltration.

The CISA Zero Trust Model also builds on the foundational capabilities of the cross-cutting pillars with **Visibility and Analytics**,[1] **Automation and Orchestration**,[2] and **Governance**[3] which support (acts as the Pillar Base) and enhance the maturity of each core pillar.

Cisco® provides proven solutions for accelerating Zero Trust adoption. In this document we discuss how Cisco Secure Firewall meets the CISA ZTMM standards.

[1] Visibility and Analytics enable organizations to monitor and analyze behavior and events across the five pillars. This foundation capability provides the data-driven insights necessary to identify anomalies, detect threats, and enforce Zero Trust polices.

[2] Automation and Orchestration ensure that Zero Trust principles are implemented consistently and efficiently across the five pillars. By automating security tasks and orchestrating responses, organizations can reduce human error and improve reaction times to potential threats.

[3] Governance ensures that security policies, processes, and compliance requirements are well-defined and constantly applied across all pillars. It provides the overarching framework for decision-making, accountability, and adherence to organizational goals and regulatory mandates.

© 2025 Cisco and/or its affiliates. All rights reserved.

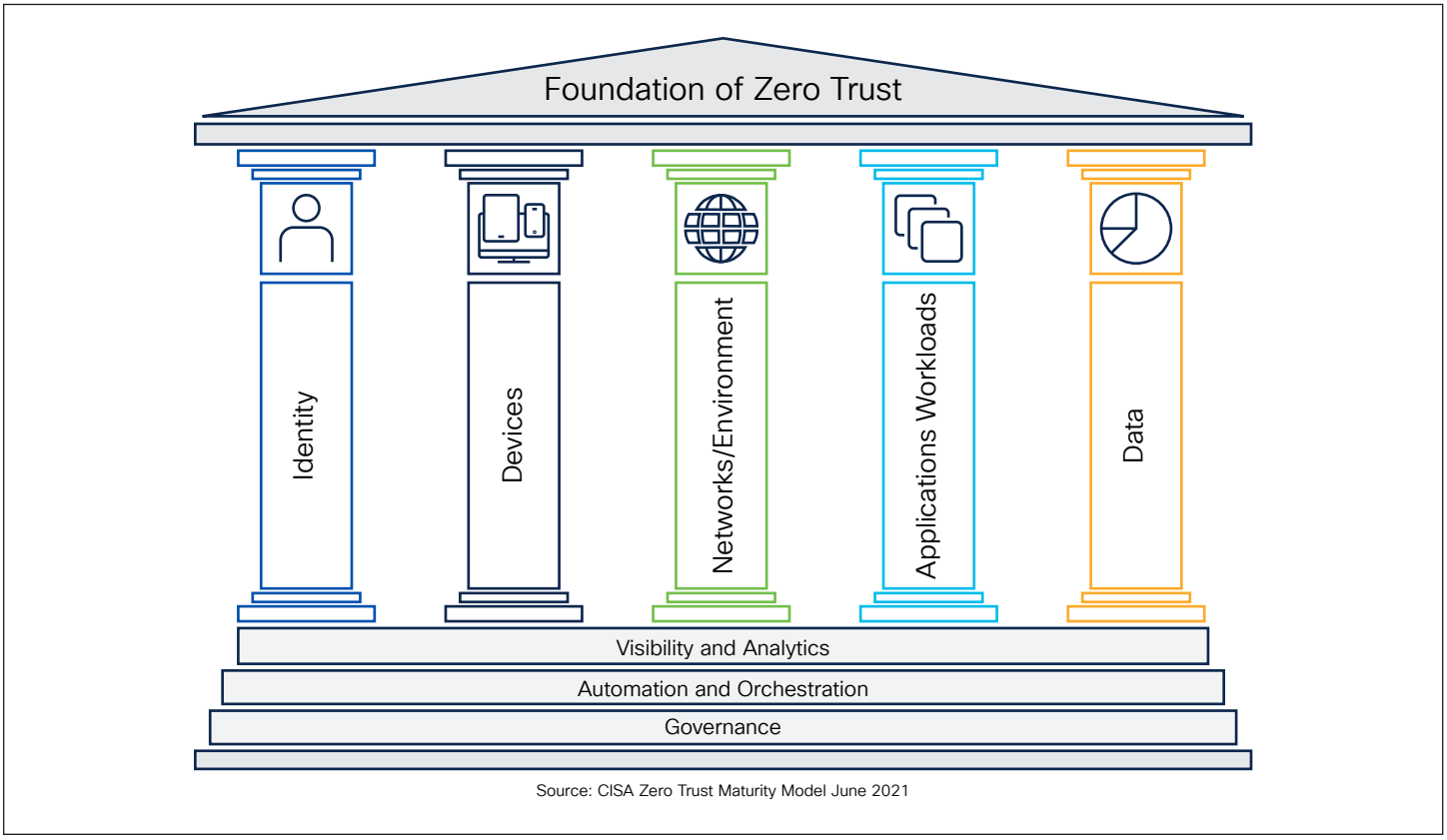

Figure 1. CISA Zero Trust Maturity Model

Cisco Secure Firewall is a key enabler of an organizations Zero Trust strategy, excelling in the **Device**, **Network**, and **Automation and Orchestration** pillars of the CISA model. It provides **real-time device inspection**, **secure access controls**, and **dynamic segmentation**, ensuring that network traffic is securely managed and unauthorized movement is restricted. By leveraging automated policy management and enforcement, Secure Firewall dynamically adapts to evolving threats, enabling HHS to maintain consistent security across its network infrastructure. These capabilities are critical for addressing the complexity of modern healthcare environments, where real-time protection and adaptability are essential.

In addition to its primary strengths, Cisco Secure Firewall also contributes significantly to the **Data** pillar by supporting **data encryption and rights management**, ensuring sensitive information is protected as it moves across the network. While its role in the **Identity** and **Application Workload** pillars is more indirect, it complements other Zero Trust tools by enforcing consistent security policies and enabling secure access to applications and services. By integrating seamlessly with other Cisco solutions, Secure Firewall ensures comprehensive enforcement of Zero Trust principles across the HHS environment. As a foundational component of an organizations Zero Trust roadmap, Cisco Secure Firewall empowers the organization to protect its operations, mitigate risks, and align its cybersecurity strategy with national standards and best practices.

© 2025 Cisco and/or its affiliates. All rights reserved.

Mapping to the CISA Zero Trust Five Pillars

Below is a detailed mapping of Cisco Secure Firewall capabilities to the CISA Zero Trust Five Pillars and their corresponding functions. This table provides a clear alignment between Secure Firewall's features and the foundational components of a Zero Trust architecture, illustrating how its capabilities support each pillar and enhance overall security. By breaking down each pillar, function, and capability, the table offers valuable context for understanding how Secure Firewall enables government organizations to advance their Zero Trust maturity.

Table 1. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Identity Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Identity	Enterprise Identity and Access Management		Cisco Secure Firewall does not directly manage identities but supports identity-based policies for controlling access to resources.
	Multi-Factor Authentication		Next-Generation Firewall (NGFW) is not a direct MFA solution but can be integrated with identity solutions to enable identity-based firewall rules.
	Privileged Access Management		Indirectly supports privileged access by enforcing identity policies to restrict unauthorized access to sensitive systems or applications. It additionally supports user, device, and context-based policies.
	Least Privileged Access		Indirectly supports least privileged access by enforcing identity policies to restrict unauthorized access to sensitive systems or applications. It additionally supports user, device, and context-based policies.

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 2. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Device Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Device	Device Inventory	Device Detection	Cisco Secure Firewall has functionality to create an asset inventory of devices passing through the firewall attempting to communicate on the network.
	Device Security Posture	Device Detection and Compliance	Verifies device compliance with security policies before allowing access to network resources. NGFW can enforce specific compliance checks (e.g., Remote Access VPN [RAVPN] and Zero Trust Network Access [ZTNA]).
	Device Trust	Device Authorization with Real-Time Inspection	Authorizes devices dynamically based on real-time posture and inspection for security compliance (e.g., connection checks with RAVPN and ZTNA).
	Secure Remote Access	Remote Access	Provides secure access for remote users and devices by inspecting traffic and enforcing security policies.

Table 3. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Network/Environment Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Network/Environment	Segmentation of Network	Macro-Segmentation	Enables macro-segmentation by grouping and isolating network resources based on roles, zones, or access policies.
		Micro-Segmentation	Implements micro-segmentation by applying granular policies to individual users, devices, or applications to minimize lateral movement (e.g., utilizing Security Group Tags [SGTs]).
	Secure Network Access		Ensures secure access to the network by enforcing access policies at the perimeter, within zones, and between segments.
	Encrypted Network Traffic (VPN)		Provides encrypted traffic with encrypted tunnels with site-to-site and remote access VPN tunnels. Cisco Secure Firewall includes several methods of key management.

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 4. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Application Workload Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Application Workload	Enterprise Application Inventory		While Cisco Secure Firewall does not maintain application inventories, it monitors application traffic to enforce security policies. Cisco Secure Firewall also profiles applications to provide threat risk scores.
	Secure Application Access		Provides secure gateway access to applications with ZTNA. Cisco Secure Firewall also ensures secure application access by inspecting application-layer traffic and enforcing security policies.

Table 5. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Data Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Data	Data Classification		Cisco Secure Firewall does not classify data but protects data flows by enforcing segmentation and access control.
	Data Discovery		Data discovery is not a direct capability but is supported by monitoring traffic flows to identify data movement and patterns.
	Encrypt Data at Rest and in Transit	Data Encryption	Ensures encrypted data is securely transmitted across the network by enforcing access controls and secure pathways. Cisco Secure Firewall utilizes self-encrypting drives, and all traffic is encrypted to the system management interface.
	Prevent Data Exfiltration	Data Encryption and Rights Management	Helps prevent data exfiltration by monitoring and inspecting traffic for unauthorized access or data flows. It also implements sensitive data protection (SS#s and credit cards/ Personally Identifiable Information [PII] info).

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 6. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Automation and Orchestration Supporting Pillar

CISA Zero Trust Pillar Base	CISA Functions	Cisco Capabilities	Notes
Automation and Orchestration	Automated Threat Detection and Response	Policy Decision Point (PDP) and Policy Orchestration	Cisco Secure Firewall dynamically adjusts policies based on real-time analysis and integrates with orchestration tools for automated responses.
		Machine Learning	Leverages machine learning to detect anomalies, optimize policies, and proactively defend against emerging threats (SnortML and AI Assistant).

Table 7. Mapping Cisco Secure Firewall Capabilities to the CISA Zero Trust Visibility and Analytics Supporting Pillar

CISA Zero Trust Pillar Base	CISA Functions	Cisco Capabilities	Notes
Visibility and Analytics	Security Monitoring and Visibility	Common Security and Risk Analytics	Cisco Secure Firewall has a plethora of monitoring, visibility, and reporting features. AI policy analytics are also incorporated. Cisco Secure Firewall also integrates with other Cisco or third-party tools for visibility and analytics.

© 2025 Cisco and/or its affiliates. All rights reserved.

Key observations

1. Core Strengths in Device and Network Security:

- Cisco Secure Firewall aligns strongly with the **Device** pillar by supporting **device detection**, **real-time inspection**, and **secure remote access**.
- It also contributes significantly to the **Network** pillar with **macro-segmentation**, **micro-segmentation**, and **secure access control**, minimizing lateral movement within the network.

2. Support for Data Security:

- Within the **Data** pillar, Cisco Secure Firewall supports **data encryption** and **rights management**, preventing unauthorized access to sensitive data and ensuring secure data flows.

3. Automation and Orchestration:

- Cisco Secure Firewall's **Policy Decision Point (PDP)** and **Policy Orchestration** capabilities align with Zero Trust automation requirements, enabling automated and dynamic policy adjustments.
- The inclusion of **machine learning** allows for proactive defense mechanisms and optimization of security policies.

4. Indirect Contributions to Identity and Application Workload:

- While Cisco Secure Firewall does not directly manage identities or application workloads, it secures access to applications and enforces identity-based policies.
- It supports application security by inspecting traffic and enforcing granular controls for secure application access.

5. Visibility and Analytics:

- Although not explicitly listed in the provided capabilities, Cisco Secure Firewall integrates with Cisco's broader security ecosystem (e.g., Secure Network Analytics and Cisco Extended Detection and Response [XDR]) to enhance **monitoring** and **visibility**, which indirectly supports the **Visibility and Analytics** pillar.

Summary

Cisco Secure Firewall excels in the Device, Network, and Automation and Orchestration pillars of the CISA Zero Trust model, providing robust capabilities for segmentation, real-time device inspection, secure access, and automated policy management. Its contributions to the Data pillar are also significant, particularly in encryption and rights management. While it plays a more indirect role in the Identity and Application Workload pillars, it complements other tools to enforce Zero Trust principles comprehensively.

Resources

Cisco Secure Firewall

Cisco Secure Firewall At-a-Glance

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)