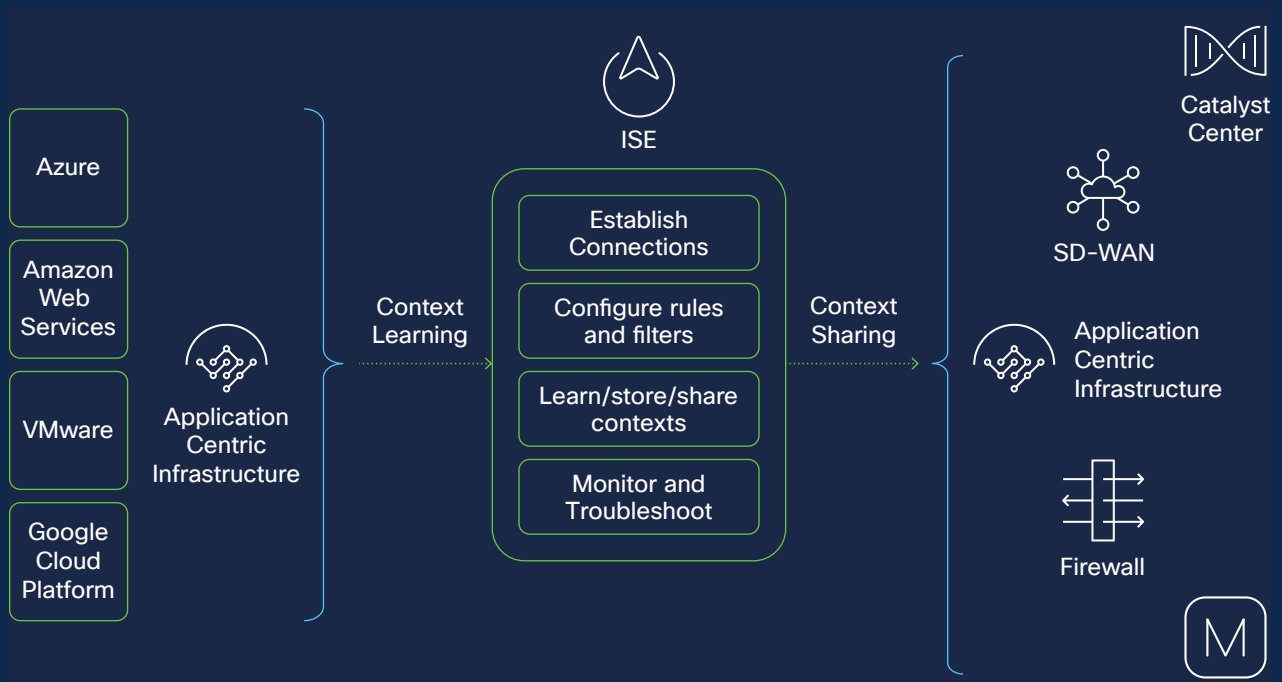
Cisco's Common Policy Framework

Benefits

1. **Create Once, Apply Everywhere:** Define shared policy conditions and building blocks that work across wired, wireless, and VPN access and multiple domains: Firewalls, Data Centers, and Cloud workloads.
2. **Eliminate Redundancy:** Centralize policy logic for more efficient management and reduced configuration errors.
3. **Unified Framework:** Cisco offers a unified policy framework that spans across various network environments, including on-premises, cloud, and hybrid. This allows for consistent policy application and management across diverse infrastructures.

Common Policy Capabilities in Identity Services Engine

Enabling consistent Zero Trust policies in a multidomain environment



Common Policy:

- **Introduces** a unified framework for managing security policies across diverse IT environments
- **Centralizes** context sharing and policy enforcement
- **Ensures** that security protocols automatically adapt to changes without requiring manual updates

Ensuring consistent policies across the distributed network

In today's rapidly evolving IT landscape, organizations encounter significant challenges in securing highly distributed, multi-domain networks. Ensuring consistent security policies across varied environments such as campuses, branches, data centers, and cloud platforms is vital. Cisco's Common Policy framework addresses these challenges by eliminating language barriers between network domains, enabling cohesive security policy enforcement, and supporting a robust Zero Trust strategy.

Security policies within enterprise networks are often applied inconsistently due to their heterogeneous nature. This inconsistency arises from the absence of standardized frameworks for managing access and security across multiple network domains. In addition, Zero-Trust access, whether it is remote or on-prem requires consistent access and segmentation policies between users, devices, and application workloads. This results in substantial operational and security challenges:

- **Productivity Issues:** Each domain utilizes unique policy constructs, leading to administrative complexity and slowing down IT operations.
- **Increased Risk:** Limited visibility into user, endpoint, and application access creates heightened vulnerability to cyber threats.
- **Reduced Agility:** The inability to share and enforce consistent policies across domains hinders the implementation of a comprehensive Zero Trust security model.

Today's fragmented IT environments further complicate the creation of uniform security policies. Administrators face challenges in integrating and managing policies when different domains cannot share context about users, devices, and applications. This fragmentation weakens security posture and obstructs efficient policy management.

Cisco's Common Policy Solution

Cisco's Common Policy solution introduces a unified framework for managing security policies across diverse IT environments. It enables centralized context sharing and policy enforcement, ensuring that security protocols automatically adapt to changes without requiring manual updates.

Key Features

Cisco's Common Policy solution offers a comprehensive suite of features provide organizations with the tools needed to maintain a secure and efficient network infrastructure:

Centralized Context Sharing: Using Cisco Identity Services Engine (ISE) as the exchange hub, Common Policy creates context information closer to the domain where it resides, in the access layer for users and devices, and in the data center or cloud for application workloads. Common Policy then shares context to various domains enables security administrators to create consistent access and segmentation policy irrespective of which domain they choose to enforce policy. User, device, and application contexts are normalized into Security Group Tags (SGTs), ensuring interoperability across network domains.

- **Unified Policy Enforcement:** Policies are applied consistently, regardless of whether users access the network from campuses, branches, data centers, or cloud environments.
- **Policy Automation:** Policies dynamically adjust based on network changes, reducing administrative burden.
- **Dynamic Policy Adaptation:**Security protocols evolve in real time, reflecting changing user behaviors and network conditions.

Policy Enforcement Techniques

Policy enforcement techniques are essential for maintaining network security and ensuring consistent access control across various environments. These techniques encompass:

- Device-level enforcement - where policies are applied through wired, wireless, and VPN access points to secure endpoints, thereby safeguarding devices from unauthorized access and potential threats.
- Software-Defined Networking (SDN) enables policy enforcement across the entire network by leveraging dynamic security profiles, which allows for adaptable and efficient management of security measures as network conditions change.
- Micro-segmentation plays a crucial role in protecting sensitive workloads by implementing granular, flexible security policies. This approach allows for precise control over network traffic, ensuring that sensitive data remains secure and isolated from potential threats.

Together, these techniques provide a comprehensive strategy for effective policy enforcement and robust network security.

Expanded Network & Security Ecosystem

Common Policy extends Zero Trust security by integrating with industry leading providers

Unified policy constructs facilitate seamless policy management across all network environments, ensuring consistent security. Enhanced context sharing provides detailed information that supports more precise access control and segmentation. Cross-domain integration allows for centralized context sharing, enabling administrators to manage security policies across various domains using a single, unified framework.

Why Cisco Common Policy?

Cisco offers a differentiated Common Policy solution through several key aspects:

1. **Integration with Cisco Ecosystem:**As part of Cisco's extensive portfolio, the Common Policy solution integrates seamlessly with other Cisco products and solutions, such as Cisco Catalyst Center, Cisco Application Centric Infrastructure (ACI), Cisco Software-Defined Access (SD-Access) and Cisco Secure Access, providing a comprehensive and cohesive network management experience.
2. **Advanced Security Features:** Cisco's solution includes robust security capabilities, leveraging its expertise in network security to provide features like automated threat detection and response, identity-based access control, and micro-segmentation.
3. **Scalability and Flexibility:**Cisco's policy solution is designed to scale with growing network demands and can be customized to fit the unique requirements of different organizations. This flexibility is a significant advantage for enterprises with complex and evolving networks.
4. **AI and Machine Learning:** Cisco incorporates AI and machine learning to enhance policy automation, optimize network performance, and predictively address potential issues before they impact operations.

5. **Comprehensive Visibility and Analytics:** Cisco provides deep visibility into network operations and user behavior, powered by advanced analytics. This helps organizations make informed decisions and ensure optimal performance and security.
6. **Strong Support and Services:** Cisco's global support network and professional services offer customers robust assistance in deploying, managing, and optimizing their policy solutions.

These differentiators make Cisco's Common Policy solution a compelling choice for organizations looking for a reliable, integrated, and secure policy management platform.

How it works

Common Policy provides the solution to the network administrator's problem. Context information is created closer to the domain where it resides: the access layer for users and devices and in the data center or cloud for application workloads. This context is normalized to a group construct, namely a Security Group Tag (SGT), that is understood across all of the domains. The normalized user, device, and app workload context is sent to each domain using Cisco ISE as the exchange hub.

This enables security administrators to create consistent access and segmentation policies regardless of which domain they choose to enforce policy.

Business Benefits

The business benefits of implementing these strategies are significant. Improved security posture is achieved through consistent policies that minimize security gaps and reduce the risk of breaches. Operational efficiency is enhanced by automated policy management, which streamlines IT operations and reduces administrative overhead. Zero trust enablement is facilitated by continuous trust verification and least-privilege enforcement, which bolster digital transformation efforts. Additionally, scalable security ensures that security policies grow with the organization, maintaining robust protection as the organization expands.

Conclusion

Common Policy serves as a universal translator for network security, facilitating seamless policy implementation across IT environments. By sharing unified context through Cisco Identity Services Engine (ISE), organizations can build a strong Zero Trust foundation, enhance IT agility, reduce operational complexity, and effectively mitigate cybersecurity risks. This solution not only simplifies policy management but also empowers organizations to proactively adapt to evolving security landscapes, ensuring resilient and secure network operations in the face of emerging threats.

Ensure your business is protected with common policies across the network. For more information, please visit these other sites:

[Cisco Identity Services Engine (ISE)]

[Cisco Catalyst Center]

[Cisco Secure Access]

[Cisco Application Centric Infrastructure (ACI)]

[Cisco Software-Defined Access]

P0518190610 03/25