Secure Access Everywhere, with Cisco SD-WAN and Zero Trust

Adapting to the Evolving Security Landscape with Zero Trust

As organizations continue to evolve and expand, traditional business boundaries have become increasingly blurred. This has led to a lack of clear borders, making practically everyone an insider and significantly amplifying risks across every facet of the business. However, with the constant evolution of security threats in today's digital landscape, traditional security models that rely on perimeter-based defenses are no longer enough to protect against sophisticated attacks.

This has forced organizations to adopt a new security paradigm. This paradigm shift takes a zero-trust approach to security, where networking and security convergence are critical. The principles of zero trust—never assume trust, always verify, and enforce least privilege—should guide your security strategy to enforce secure access across borderless IT environments. Zero trust assumes that any entity attempting to access an organization's resources is potentially malicious until proven otherwise. To achieve secure access, organizations need a solution that helps build a zero-trust model tailored to their unique security needs.

Cisco® SD-WAN provides the necessary networking and security convergence to build a zero-trust model that helps ensure security across all facets of an organization's digital operations. The tight integration between Cisco SD-WAN and Cisco Identity Services Engine (ISE) enables IT to employ zero-trust security functions for the traffic that goes through the SD-WAN fabric.

Zero trust is often the starting point for enterprises that are beginning their Secure Access Service Edge (SASE) journey or dealing with hybrid work environments. To ensure the highest level of security in borderless IT environments, organizations need to adopt a zero-trust approach to security. Cisco SD-WAN provides a solution that can assist organizations at any stage of their transformation, allowing them to enable secure access to distributed applications for their workforce from anywhere.

Why zero trust is a must-have security approach

Organizations face a variety of challenges when it comes to securing their networks. Some of the key challenges include:

- **Businesses are competing as ecosystems:** Businesses today are increasingly competing as ecosystems, meaning that more parties are accessing company resources, making it harder to control access and monitor activity.
- **Every user is a potential insider:** As more people are considered insiders, including employees, contractors, and partners, the traditional network perimeter is no longer enough to ensure security against threats.
- **Hybrid work is here to stay:** With employees working from anywhere, on any device, including remotely, controlling and securing access to sensitive information and applications has become increasingly challenging.
- **Network complexity is increasing:** With the proliferation of cloud applications, mobile devices, and IoT devices, networks have become more complex, making it difficult to enforce consistent security policies.
- **Organizations lack visibility into network traffic:** Organizations struggle to gain complete visibility into network traffic, making it difficult to detect and respond to security threats.

Accelerate your journey to zero trust with Cisco SD-WAN

Cisco SD-WAN can help you implement a zero-trust model by delivering four functional requirements:

1. Establish trust for users, devices, and applications, driven by visibility and context.
2. Enforce trust-based access based on the principle of least privilege.
3. Continuously verify trust to detect any change in risk, even after initial access is granted.
4. Respond to change in trust by investigating and orchestrating responses to potential incidents.

Cisco SD-WAN includes several zero-trust capabilities that can help organizations implement a comprehensive security strategy. These capabilities include:

- Identity and device verification: Cisco SD-WAN can verify the identity and trustworthiness of users and devices before granting access to resources.
- Microsegmentation: Cisco SD-WAN can segment the network into smaller, more manageable segments, allowing organizations to enforce granular security policies.
- Secure Access Service Edge (SASE): Cisco SD-WAN can integrate with Security Service Edge (SSE) solutions to provide comprehensive security for cloud applications and remote workers.

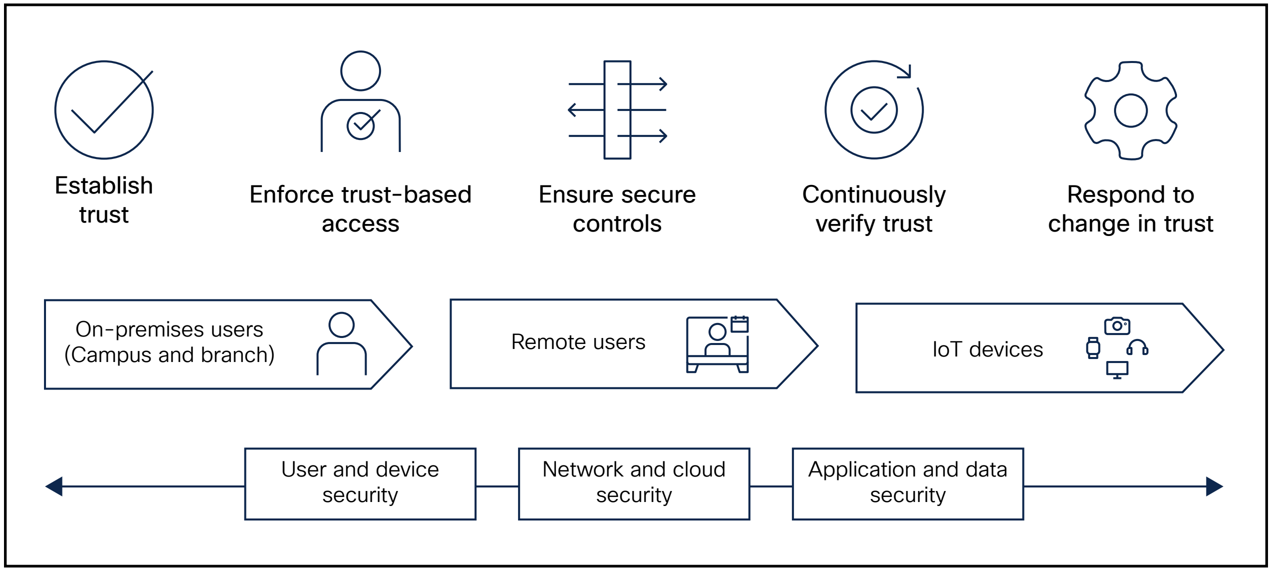
Establish trust
Enforce trust-based access
Ensure secure controls
Continuously verify trust
Respond to change in trust
On-premises users (Campus and branch)
Remote users
IoT devices
User and device security
Network and cloud security
Application and data security

Figure 1. Zero-trust architecture

The integration of Cisco SD-WAN and Cisco ISE offers a comprehensive set of security features that enable IT teams to implement zero-trust security for traffic passing through an SD-WAN fabric. This integration enables Cisco ISE to support the configuration of security posture policies in the SD-WAN fabric to evaluate the posture of devices and IoT endpoints when they connect to the network based on the configured policy. Security Group Tags (SGTs) and session attributes are shared between the two, allowing IT teams to create identity groups and associate security policies in Cisco vManage for specific user groups to access applications over the SD-WAN fabric. The periodic reassessment of device posture is also supported, allowing changes in authorization and security policies at the SD-WAN edge. This approach helps ensure a seamless integration of network and endpoints to provide zero-trust capabilities. Furthermore, the use of software-defined remote access extends zero-trust principles to remote users, providing enhanced security.

The bridge to possible

Use cases for Cisco SD-WAN with zero-trust capabilities

- Secure access to applications.
- Achieve granular access control to private applications across data center and public clouds.
- User security posture.
- Establish access control and secure policy based on posture, followed by periodic evaluation of posture.
- User location agnostic.
- Support posture-based user-to-application policies for both on-premises and remote users.
- IoT devices.
- Support vulnerability assessment-based access policies for IoT devices.
- Complete visibility.
- Visualize the user-to-application traffic journey and generate reports for security operations center engineers and CISOs.

Stay ahead in a dynamic threat landscape with Cisco SD-WAN and zero trust

Cisco SD-WAN with zero trust brings several benefits that help organizations stay secure and resilient against security threats.

- **Identity verification and secure access to distributed applications:** With its zero-trust model, Cisco SD-WAN helps ensure that every user, device, and application is verified before being granted access to resources. This not only improves security but also enhances user experience and productivity.
- **Scalable and distributed security enforcement:** Scalable and distributed security enforcement close to endpoints helps ensure maximum bandwidth utilization and no central choke points. This is critical for organizations embracing the SASE architecture, which requires security to be distributed across a global network.
- **Enhanced security posture:** Cisco SD-WAN's zero-trust capabilities enhance security posture by eliminating the assumption of trust and providing secure connectivity for applications and users. The integration with Cisco ISE provides policy-based access control, enforcing strict authentication and authorization measures. This helps ensure that only authorized users and devices can access the network, thus reducing the risk of security breaches and improving overall network security.
- **Simplified IT management:** The improved workflow simplifies IT management by allowing policies to be defined using usernames, user groups, and SGTs, providing a more identity-based policy management system that allows for constant policies. This approach improves efficiency and reduces complexity, making it easier for IT teams to manage network security as compared to traditional IP address-based policies.
- **Increased visibility and control:** With Cisco SD-WAN's zero-trust capabilities, IT teams gain increased visibility and control over the network, applications, and devices. This is crucial in a distributed environment where multiple devices and applications are accessing the network from various locations.
- **Improved flexibility:** With Cisco SD-WAN's zero-trust capabilities, organizations gain the flexibility to deploy secure access across any device or location, enabling their workforce to work from anywhere without compromising security. This improves agility, enabling organizations to respond to changing business needs quickly.

With the constantly evolving threat landscape, organizations need to prioritize security resilience to protect their digital assets. Cisco SD-WAN's comprehensive security capabilities make it possible to implement zero-trust functions across SD-WAN traffic, helping ensure network and device security in a scalable, efficient, and cost-effective manner. By adopting Cisco SD-WAN and zero-trust capabilities, your organization can achieve a zero-trust transformation, enabling you to stay secure and resilient against security threats. Don't wait, start your journey to a more secure future today with Cisco SD-WAN and zero trust.

Learn more:

- SD-WAN security
- Cisco SD-WAN
- Zero Trust, Zero Compromises: Secure Your Network with Cisco SD-WAN
- Enforcing Zero TrustAccess with Cisco SD-WAN