Secure End-to-End Segmentation at Scale

with Cisco SD-WAN Security

Segmentation is a fundamental way to isolate and protect critical assets in an enterprise; but its implementation has always been complex. To address new security challenges, segmentation must be an integral part of a comprehensive security strategy. Cisco SD-WAN security makes it possible.

Unlike its predecessors, today's networks extend to anywhere and any device where work is taking place. In a flat networking architecture, an attacker, coming from just about anywhere, can get access to the business' sensitive data. With the ability to break the networks down into smaller, more logical pieces, organizations are able to control the access level to certain segments from unauthorized users, devices and applications. The traffic isolation that comes with segmentation prevents attacks from easily propagating across the entire network and turning into destructive breaches.

Although segmentation has been touted as a security tool for preventing access to sensitive corporate data, there are many other use cases for network segmentation that organizations use to meet their business needs.

Segmentation benefits:

Separating lines of business (LOB)

- Ensure only the finance teams get access to financial databases
- Multiple subsidiary companies of a parent company use the same WAN
- Provide selective access to business partners to specific portions of the network

Better monitoring

- Keep authenticated users separate from guest users
- Separate video surveillance traffic from transactional traffic

Improved performance

- Fewer users access a segment, which translates to less local traffic

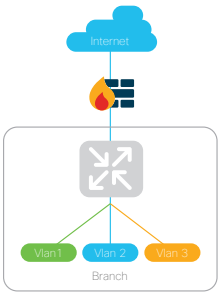
Better compliance

- Enfore regulatory compliance like HIPAA or PCI on a specific network or segment

Segmentation, Not a New Concept

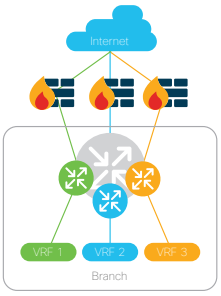
Traditional segmentation practices have focused on network-based segmentation which can be achieved through various physical or logical partitioning by configuring networking switches, routers, or firewalls. However, configuration of advanced routing and security per segment and per tenant, in modern environments, at scale, can be technically challenging. Over the years, many solutions for segmentation have been used but each has been insufficient for reasons like complexity, lack of security, manageability and scalability. One inherent limitation that makes the use of most segmentation solutions far less effective is their scope – they are limited to single devices or pairs of directly connected devices.

Here are a few examples of current solutions in the market:



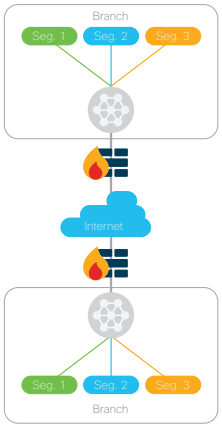
Virtual LANs (VLANs)

VLANs for layer 2 solutions have been used, for many years, to create private zones in order to guard the things in one zone from the things in other ones. The network can be logically segmented by VLANs on switches and the end-user communication between VLANs can be controlled by Access Control Lists (ACLs). Although these rudimentary solutions provide some security per segments, they are unable to provide greater visibility and granularity into users and applications. Lacking the required scalability – mostly due to their manual configuration process per device, site, or tenant – VLANs and ACLs are difficult to manage at enterprise scale. Besides, they are site-specific and unable to maintain an end-to-end network segmentation outside of their designated local network architecture.



Virtual Routing and Forwarding (VRF)

VRF for layer 3 solutions is more complex than VLAN configuration, and is a common technology that provides good security. With VRF, a network device can have multiple and distinct routing tables on the same switch or router and can't communicate with another device in a different VRF. The complexity of applying a defined grouping policy on a single device at every point of the network makes this solution non-scalable. There are simply too many points in an enterprise network to enforce a grouping policy. Without that enforcement, like VLANs, VRFs lose segmentation in the WAN environment; and it becomes unmanageably complex.



SD-WAN solutions

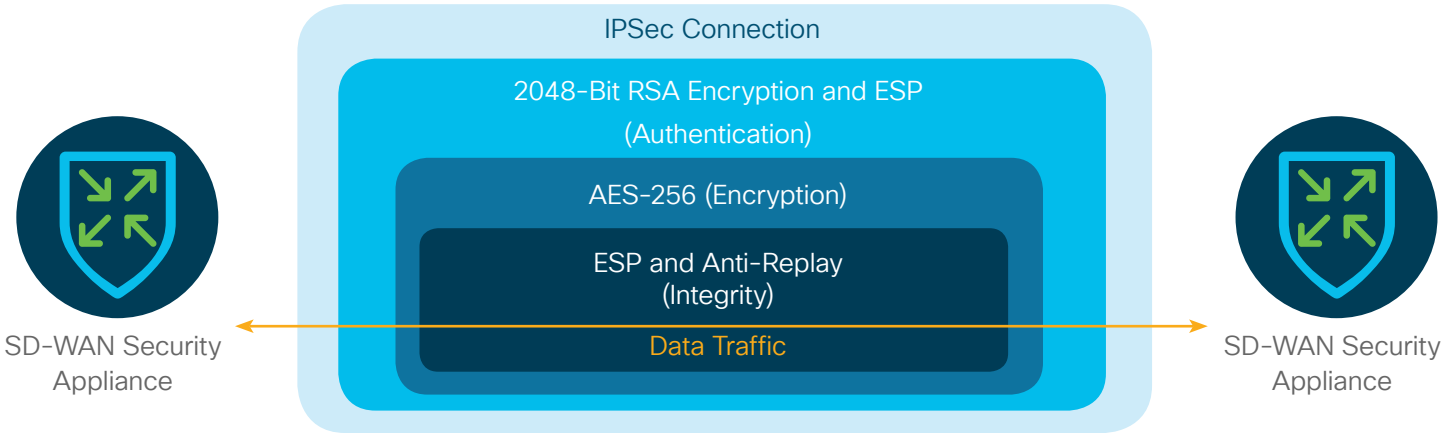
SD-WANs can segment traffic at the edge of the network and maintain separation through all relevant points in the network. To achieve this, a typical SD-WAN builds a single overlay across all enterprise links based on an encryption protocol like an IPsec, and maps VLANs or IP address ranges to those defined tunnels at each location. Segmentation with SD-WAN allows for complete visibility and control into each network segment. With its centralized management and orchestration, an SD-WAN solution optimizes the use of link and bandwidth through the enforcement of network-specific or segment-specific policies in an end-to-end segmentation.

SD-WAN network segmentation is based on layer 3 and is only able to restrict access based on the types of devices, users, and applications. Once a device or an application gets compromised by a malicious code, SD-WAN can't prevent an attacker from accessing a system on a different segment and malware can quickly spread across an organization.

Cisco SD-WAN Security: A Differentiated Segmentation Solution

The approach that organizations take to network segmentation as a security strategy hasn't kept abreast of the complexity and unpredictability of today's cyberattacks. Cisco SD-WAN security is taking the segmentation to an all new level by providing a comprehensive layer 3 to layer 7 security, including direct cloud security, per tenant in each segment. This creates an end-to-end secure network and secure network applications without modifying any devices in its path without modifying any devices in its path.

At its core, Cisco SD-WAN technology provides key security components of authentication and encryption capabilities for data packets traveling within the secure layer 3 IPsec connection. Cisco SD-WAN ensures the privacy of traffic crossing the network by all devices being fully and securely authenticated with 2048-bit encryption keys, and by having the underlying traffic encrypted using the AES-256 cipher.



Cisco SD-WAN security extends branch segmentation into the data center and cloud by carrying the relevant identifying segmentation information to all relevant points in the network. By integrating security and networking into one platform, Cisco SD-WAN makes it easy to set and monitor automated security policies within each segment in an entire network from a single pane of glass. In addition to its simple deployment in multi-tenant and multi-segments environment, Cisco SD-WAN can provide the following unique benefits per tenant and per segment:

Full Stack Security

Embedded enterprise Firewall, IPS, and URL filtering capabilities directly into SD-WAN appliance

Cloud Security

Easily configure and leverage Cisco Umbrella as a Secure Internet Gateway for direct access breakouts

Automated Management

Security and networking management interface to enforce application-aware and security policies

Scalable Deployment

Zero touch deployment and automatic provisioning of an end-to-end segmentation

Real-time Orchestration

Optimizing link and bandwidth through enforcement of network-specific or segment-specific policies

Optimized Performance

Ensure optimized performance for every tenant, in any segment, regardless of their location

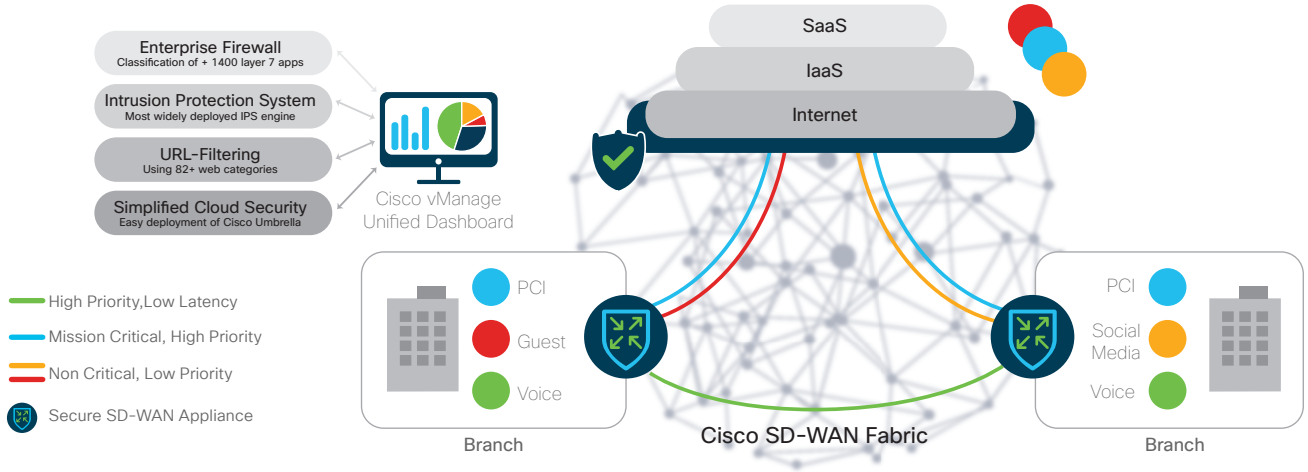
Secure Segmentation Use Case with Cisco SD-WAN

Restricting network access to just the network segments for specific users or a line of business within a company is a common best practice in all types of organizations. Some compelling examples are excluding guest Wi-Fi access from an internal network or providing access to customer data to only a specific department. Securing the overall network traffics, once the segment is created is a big challenge. Sophisticated security threats and the ability of malicious traffic to cross over from one segment to another necessitate a complete traffic separation between segments as well as increasing security layers within and between segments throughout a network infrastructure.

Cisco SD-WAN allows for the creation of segmentation policies based on device types, application characteristics, network topologies, and user locations and profiles to simplify the provisioning of network access, as well as improve the performance of the overall network. With its embedded enterprise security controls, while maintaining isolation between segments, Cisco SD-WAN is able to elevate security within the organizational infrastructure and allow customers, guests, and internal employees to accomplish their tasks. With its automated and dynamic policies, Cisco SD-WAN security is able to automatically enforce segmentation-based policies based on user and device type discovery and apply different per-application policies to each segment. It also routes the applications in real-time along the optimum path or selected transport to the destination.

Figure 1 shows how a mission-critical traffic from the PCI segment steers over a high priority secure route from a branch to the PCI network in order to protect critical data and meet compliance requirements, while a high priority voice application between branches takes an optimal and low latency path. Finally, traffic from guest users is sent directly to the Internet over a non-critical and low cost broadband link.

Figure 1: Segmentation-based policy with Cisco SD-WAN



As for security, Cisco's secure SD-WAN platform ensures complete isolation and security of traffic among segments as well as protection of data within each segment by a set of natively integrated security capabilities such as enterprise firewall, URL filtering, intrusion prevention and DNS monitoring. Additionally, Cisco vManage unified management dashboard is able to create, control and monitor the segmentation-based policies, at scale, from a single centralized console and enforce those polices across the entire network.

With its integrated routing, security, centralized policy and orchestration, Cisco SD-WAN security enables organizations to implement end-to-end segmentation strategies that can stop breach propagation, enforce regulatory compliance, and promote network - and application - layer security.