SD-WAN security options

Let's look at SD-WAN security and partnerships with suppliers, including Aruba, Cisco, Riverbed and Silver Peak.

Let's look at SD-WAN security and partnerships with suppliers, including Aruba, Cisco, Riverbed and Silver Peak.

An important component of SD-WAN is the ability to secure unreliable Internet links and identify unusual traffic flows, as well as avoid Internet threats.

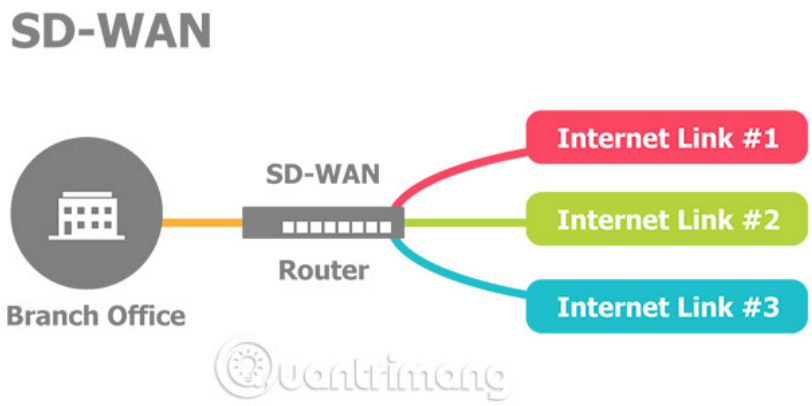
SD-WAN technology providers are continuing to increase the number of their own security features and create powerful ecosystems for network security partners.

IT managers should review their branch network security requirements and carefully assess the security of leading SD-WAN providers, including original security features and partnerships. with their network security providers.

Network security threats at branches

Network security is a constant concern for IT professionals and surveys show that the problem is getting worse. Branch security is a challenge, as the number of devices increases, including PCs, tablets, phones, POS devices and IoT endpoints, attached to the branch network. All of these terminals provide the opportunity for malware to infect the corporate network and give hackers access to important data. Security concerns are exacerbated by the lack of trained IT / security personnel at remote locations and the complexity of managing multiple security devices including IP VPN, IDS / IPS and firewall.

Another challenge for security at the branch is to coordinate security efforts across the network. Security systems in the branch need to contact the data center's end-to-end security products and network security systems directly. Traffic at the branch needs to be checked and any suspicious traffic is flagged, where it can be analyzed by cloud-based security system or centralized security system. Ideally, the branch security system will become fully automated and use cloud-based intelligence.



SD-WAN security capabilities

SD-WAN market is highly competitive with dozens of suppliers. A key factor for businesses that want to use SD-WAN is because of its ability to allow organizations to leverage low-cost Internet circuits, such as secure enterprise-level links. Network security is the main classification factor in SD-WAN technology and each provider has its own proprietary methods to ensure traffic traffic and identify "safe" sites.

Almost all SD-WAN providers will now provide basic firewall capabilities, as a standard product feature. They use packet identification to understand traffic traffic. For example, does traffic traffic come from a trusted location or cloud-based service? Additional features include content filtering, endpoint identification and management as well as policy enforcement capabilities.

1. Collection of the best free online data storage websites today
2. Firewall solutions for small and medium enterprises

SD-WAN providers are actively supporting leading network security providers such as Palo Alto, Z-Scaler, CheckPoint and Fortinet, to integrate their SD-WAN technology with next-generation firewalls. and UTM function. The integration between SD-WAN and the best network security providers needs to be streamlined to ensure high performance and low latency, because the transfer of traffic between applications can affect latency. The goal is to provide detailed traffic inspections and effective filtering of cloud-based sites to prioritize secure, important traffic and application flows.

Examples of SD-WAN security features

Aruba ClearPass's policy manager provides users, devices, applications and WAN context to enforce consistent policy, through its SD-WAN solution. Role-based implementation, device control and its access control, allow IT organizations to enforce LAN and WAN security policies at branch locations. This simplifies how policies are applied across different layers of the network and reduces the need for manual configuration.

RiverConnect SteelConnect supports natural perimeter firewalls, network address translation and network partitioning, based on policies that help minimize network intrusion and limit the spread of threats. It automatically creates secure IPsec VPN paths with AES-256 encryption between sites and provides a thorough check for encrypted applications such as SSL / HTTPS. SteelConnect Manager provides centralized management and visibility capabilities, allowing IT professionals to assign application-based security and traffic paths.

Failsafe SD-WAN of Talari Networks reduces Internet traffic at the branch, using integrated firewall and reliable URL traffic, can be automatically redirected to the Internet. Talari supports RADIUS authentication to access its managed devices and encrypted packages by default.

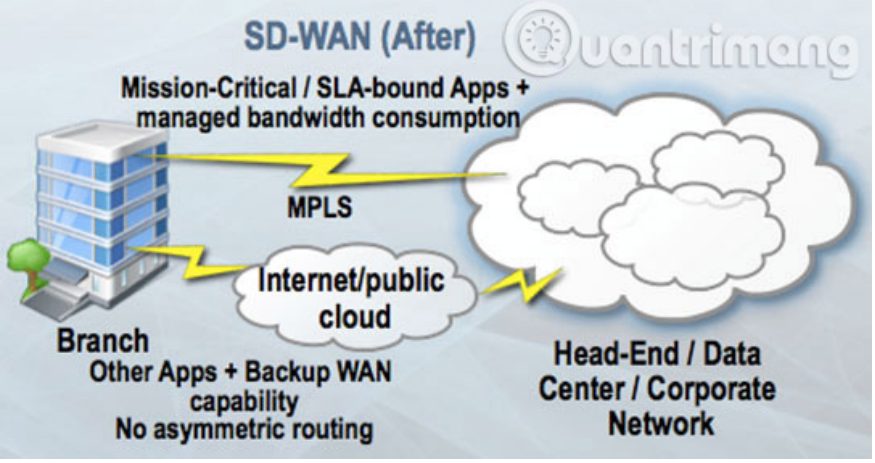
Examples of SD-WAN security ecosystems

An important aspect of SD-WAN security is whether SD-WAN platforms are integrated and compatible with leading network security products, including advanced firewall, UTM, secure and secure web portals. cloud based network or not. Here are some examples of security ecosystems created by selected SD-WAN providers.

1. Cisco SD-WAN (Viptela): Security solutions of Cisco (diverse), Bluecoat, Palo Alto, Z-Scaler.
2. Cloud Genix: Palo Alto, Symantec, Z-Scaler.
3. Cradlepoint: Cisco, Trend Micro, Webroot, Z-Scaler.
4. Silver Peak: Check point, Fortinet, Palo Alto, Z-Scaler.
5. VMware (VeloCloud): Check Point, Palo Alto, Symantec, Z-Scaler.

(**Disclosure:** Aruba, Cisco, Cloud Genix, Cradlepoint, Riverbed, Silver Peak, Talari and VMware are Doyle Research customers.)

SD-Branch is defined as having SD-WAN functionality, routing, network security and LAN / Wi-Fi functionality, all in one platform with centralized and integrated management. The advantage of SD-Branch is that it consolidates multiple software / device modules from multiple vendors into one platform, making it easier to deploy and use. Many SD-WAN providers will or will soon introduce SD-Branch solutions.



Recommended for IT managers

SD-WAN is a powerful technology for connecting distributed organizations and security as the key point in provider differentiation. Each provider has proprietary code for their own security capabilities. Customers should evaluate SD-WAN technologies based on both security capabilities in the branch and the cloud as well as the ability to develop a wide network security ecosystem.

Suppliers also need to expand further and enhance integration with a wide range of popular network security products, through their partner ecosystem.

IT managers should assess SD-WAN security on the ability to easily enhance and integrate with their specific security environment and incumbent providers.

See more:

1. 7 basic tips to ensure network security
2. 11 elements of network security strategy
3. Network security and data security in Vietnam: When the bell rings .