The Role of SD-WAN in Securing the Expanding Network Perimeter

Software-defined wide area networking (SD-WAN) is one of the most rapidly adopted technologies of the past decade. According to a study published by Dell'Oro Group, the worldwide sales of SD-WAN technologies are forecasted to grow at double-digit rates over each of the next five years to surpass $3.2 billion in 2024. This growth is certainly a testament to some of the more well-known benefits of SD-WAN technology, such as centralized network policy management, network flexibility and application-aware routing. More recently, SD-WAN has emerged as a key component for building more flexible, integrated security frameworks.

With SD-WAN, branch offices become part of an enterprise's larger network topology, with their own Internet egress. Corporate devices can access the Internet via multiple endpoints, adding a layer of complexity to network security. However, if properly configured and equipped, SD-WAN can simplify management, help improve security, and decrease threat vectors.

Key considerations

Traditional security models were designed to support a walled castle approach where all of a company's data, applications, and users operate behind a firewall at a centralized headquarters or data center. As more enterprises continue to support hybrid workforces and cloud migration, critical data and applications are also moving out of the traditional data center to the edge. As security perimeters evolve, every access point and network element becomes a potential risk for security breach. The basic firewall functionality may not be enough to help protect enterprise networks. Organizations are better served by using an SD-WAN solution that integrates security into the network functionality. The following are some key considerations for optimization:

Network policies and segmentation for security:

SD-WAN delivers the flexibility to segment networks and implement application-aware routing, thus limiting the attack surface of highly sensitive data and systems. For example, segmenting mission critical systems and data from those less critical systems like basic productivity, office and research tools creates risk domains. Network segmentation can minimize the impact of a successful attack to said domain. When set up properly, enterprise security policies with segmentations can help prevent or reduce the impact of a security incursion, and hopefully prevent propagation beyond the borders of the impacted segment.

Without SD-WAN, application-specific security for cloud-based applications can be complicated and expensive. By setting up protected regional zones to securely direct cloud-based application traffic to where it needs to go based on corporate security policies—SD-WAN can help you architect and incorporate security controls to platforms and apps into your connectivity fabric.

Encryption:

In order to help protect the site-to-site traffic of corporate locations, software-defined networking (SDN) management can connect all locations with a secure tunnel using AES256 encryption. SD-WAN can also help you prioritize and route that traffic by application, and then allow IT leaders to apply security policies using the SD-WAN appliances as enforcement.

Unified threat management (UTM):

UTM delivers multiple security functions through a single service designed to help protect business infrastructure. This combined security approach can present a unified security posture over geographically dispersed, distributed networks. SD-WAN appliances with UTM and/or next-generation firewall capabilities built in, to help protect each branch location – getting back to the expanding perimeter point. Using SD-WAN technology that includes integrated security solutions can reduce the complexity of deploying and networking a separate suite of security tools. This includes point solutions like NGFW, IDS/IPS, URL or a fully stand-alone UTM.

Single Pane of Glass Monitoring:

Once proper orchestration and security policies are in place, IT teams can monitor all traffic and ports. With SD-WAN's real-time, simultaneous management of the network and UTM threat detection on a single pane of glass, flagging risks and thwarting potential threats can help reduce corporate risk profile.

Compliance:

For retail or other credit card accepting digital commerce organizations, finding an SD-WAN solution that is PCI compliant should be a top consideration for transmitting sensitive credit card data using industry standard encryption. Flexible provisioning and segmentation capabilities of SD-WAN are especially relevant for retailers in order to easily isolate their POS systems, as well as other critical networks and data. Segregating the POS system from the rest of the network is highly recommended and considered a best practice.

Managed security and managed SD-WAN:

Managing both an SD-WAN and advanced security is simplified when combined, but can still be a lot to handle, especially in an environment where companies may be working with a reduced staff. Working with a service provider that has a broad purview of the threat landscape can reduce a threat before it even reaches the organization's perimeter. Threat visibility and management are a critical component in managed security services and can offer peace of mind in an environment where security threats are constantly changing.

Be ready for tomorrow's security threats with the next generation of global secure networking solutions, with Ethernet, SD-WAN, and advanced security, from Comcast Business. Learn more here: **https://business.comcast.com/enterprise/products-services/secure-network-solutions**

COMCAST BUSINESS

www.ComcastBusiness.com/Enterprise