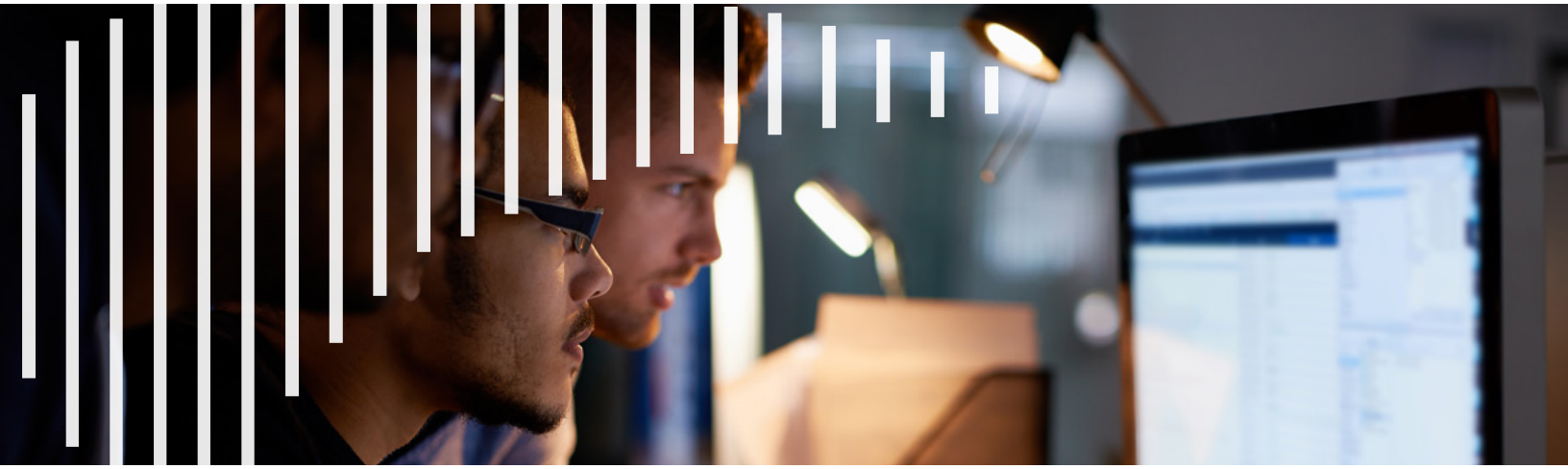

The Role of Switches in Today's Distributed Networks

Why switches are a cornerstone of unified security for SD-Branch.

ABSTRACT

Today's anywhere/anytime business model demands secure distributed networking. Switches are a crucial element to a unified security posture across distributed enterprises and SD-Branch networks. The SonicWall Switch Series delivers the core functionality required in an effective and secure switch solution.

Introduction

A modern business paradigm demands flexibility for a remote distributed workforce. Distributed organizations must deploy, configure, manage, monitor and troubleshoot a growing number of disparate devices in branch sites. Additionally, the rising demands of high-bandwidth applications have created a surge in network infrastructure that supports gigabit and multi-gigabit throughput.

High-performance switch components integrated into an end-to-end security stack can provide a strong, unified posture, amplify visibility and control, and enable single-pane-of-glass (SPOG) management. A unified security posture enables granular security controls to help identify and prevent today's stealthiest and never-before-seen attacks from compromising your network.

SD-Branch Networks

Switches can play an integrated role in SD-Branch networks, whether across distributed enterprises, large campuses, government agency sites or even at designated home-based office sites. SD-WAN applies software-defined networking and virtualization to build highly available and higher-performance WANs. By using low-cost internet access (broadband, 3G/4G/LTE, fiber, etc.), organizations can cost-effectively replace expensive WAN connection technologies such as MPLS. In turn, SD-Branch integrates SD-WAN with switches, firewalls, wireless, zero-touch deployment and central management on a single unified platform. This provides a rapidly scalable solution for securing distributed branch sites.

Segmenting and Extending Networks

Network segmentation allows security administrators to create multiple network segments, compartmentalize internal networks and provide granular secure access. Functioning on layer 2 (Data Link Layer) of the OSI model, an effective switch would allow administrators to segregate traffic based on MAC addresses or VLANs and break up the large collision domain into smaller ones. Each port on a switch would support a separate collision domain. Being able to easily segment devices in the network helps organizations maintain compliance with regulatory mandates. Segregating can be accomplished by creating policies or VLANs. For example, features such as 802.1X authentication help transactional businesses to maintain PCI-DSS compliance. By integrating switches with other networking elements, administrators can also make any wireless network an extension of the wired network.

Streamlining Secure Network Management

SPOG management of switches and other integrated components enables unified control, reporting and analytics, delivering complete network visibility. By accessing analytics in real time, administrators can make more informed decisions.

Zero-Touch Deployment (ZTD) capability can allow organizations to configure the switch quickly and securely at new locations without requiring advanced and costly on-site personnel. Switches should be able to operate independently or be daisy-chained together to form a single switch with the port capacity of the combined switches. This allows administrators to work on one large switch rather than multiple smaller ones. Some switches offer Power over Ethernet (PoE), which is ideal for powering on APs, VOIP phones and IP cameras.

Ensuring Quality of Service

To ensure quality of service (QoS), switches should enable traffic to be prioritized and avoid excessive broadcast and multicast traffic. Traffic such as voice and video streaming could be assigned a higher priority, while non-critical traffic can be assigned a lower priority. Today's switch solutions must also support gigabit and multi-gigabit throughput.

Conclusion

Switches are an integral part of protecting today's distributed enterprise in effectively and securely managing the flow of network traffic. The SonicWall Switch Series delivers intelligent switching while providing unparalleled performance, security and manageability. Its unified security posture makes it ideal for SD-Branch and enterprise deployments. This enables businesses – big or small – to undergo digital transformation and keep pace with the changing network and security landscape.

As a key component of the unified SonicWall SD-Branch solution, the SonicWall Switch Series tightly integrates with SonicWall next-generation firewalls (NGFWs), Secure SD-WAN, Zero Touch Deployment, SonicWave wireless access points, Capture Client endpoint security and Cloud App Security, all under Capture Security Center's single-pane-of-glass management. When network requirements change, any of the network functions can be upgraded or downgraded. With the flexibility that SonicWall Switches and SD-Branch offer, organizations can be more agile, open and cloud-centric.

Learn More

Contact your SonicWall representative today or visit www.sonicwall.com/switch.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®