WHAT TO EXPECT FROM TODAY’S UTM
WHAT TO EXPECT FROM TODAY’S UTM

TRADITIONAL STAND-ALONE NETWORK AND SECURITY SOLUTIONS

Network and security technologies continue to evolve along with the fast pace of today’s business and evolving threat landscape. Required by most small and medium-sized businesses (SMBs), the necessary introduction of these technologies over time has made their environments increasingly complex and difficult to manage. Specifically, the rise of mobile and remote workers, as well as an explosion of connected devices, spurred needs for virtual private networking, wireless access points, wired routing/switching, and more. At the same time, the use of cloud-based services and simple growth of the business to expand with multiple locations has driven the need for WAN connectivity/optimization along with 4G connectivity for business continuity. All while cyber criminals and their attacks have become more sophisticated.

Procurement, deployment, configuration, and management of so many individual components takes significant effort and expertise, driving additional overhead and cost of dedicated administrators or service providers to manage their network.

A typical SMB infrastructure has five main categories of components:
- Core Network
- Security
- Wide Area Network (WAN)
- Local Area Network (LAN/WLAN)
- Management

CORE SMB NETWORK COMPONENTS THAT CONNECT USERS, DEVICES, AND OFFICES VIA THE INTERNET IN A TYPICAL SMB DEPLOYMENT

ROUTER

Routers are Layer 3 network devices that connect disparate networks. In an SMB deployment, it connects the central office to remote offices and acts as a gateway between the LAN and the WAN networks as well as broadband networks such as the public Internet. Some routers support additional modules for secure connectivity to other branches through VPN, intrusion prevention, and content filtering, etc. Routers have WAN ports and LAN ports to support WAN and LAN connections, respectively, and some of them have built-in wireless capabilities.

FIREWALL

Firewalls are a crucial component that provide gateway-level network security, inside of the router, to protect the various endpoints used in the organization. Firewalls control the traffic allowed or denied at these key ingress/egress points, especially for networks that are connected to the Internet. They enable organizations to dictate what the computers on your network are able to send and receive from the outside world, helping you to cut threats off at their source.

VPN

VPN is a virtual version of a secure, physical network that connects remote offices and devices to the central office and resources. VPNs ensure secure communications over

SECURITY SOLUTIONS APPLIED TO SMB TRAFFIC

WEB FILTERING

Web filtering technology allows or denies access to and from specific web pages, sites, or domains, usually based on their reputations. It gives IT admins the ability to explicitly allow good or appropriate websites and traffic, or to block malicious or inappropriate websites and traffic. IT can easily add websites or URLs to the local

WHITE PAPER: WHAT TO EXPECT FROM TODAY’S UTM
URL filtering list to either block or allow them on an employee device off the network as well as on it.

**APPLICATION CONTROL**
Similar to web filtering, application control enhances content-based security by empowering organizations to monitor the Internet-based applications communicating on their network, typically based on reputation, and take steps to control them. Organizations can create user or group policies to identify, block, or limit use of Internet-based applications.

**IPS**
Intrusion prevention system (IPS) technology monitors network traffic flows, looking for patterns associated with known or suspect threats, in order to block attacks that might otherwise take advantage of network vulnerabilities and unprotected systems.

**ATP**
Advanced threat protection (ATP) is designed to detect file-based malware both known and previously unknown traversing the network. It is a crucial solution in an SMB environment to prevent, detect, and mitigate potential incidents in corporate as well as remote offices.

**WIDE AREA NETWORKING COMPONENTS THAT ENSURE AND OPTIMIZE CONNECTIVITY**

**WAN OPTIMIZATION**
WAN optimization helps improve the performance and capacity of SMB networks through the use of compression, deduplication, caching, and more to speed delivery of information. It allows SMBs, which can vary from a small office needing Internet connectivity for email and web access to a bigger company that moves large amounts of data between its various locations, to optimize the use of its bandwidth to support network application and other traffic requirements.

**LOAD BALANCING**
Load balancing helps distribute (L4 through L7) application traffic loads across multiple network devices at both central and remote locations. Specifically, it routes traffic to redundant servers based on the load on each one, to ensure high availability, optimized user experience, and increased performance and scalability.

**3G/4G/LTE**
In addition to wired Internet connections, SMBs can utilize wireless 3G/4G/LTE connections for data delivery. This ensures business continuity by having a robust, fast, and failproof network for small to medium enterprises. It also allows SMBs to open new locations and set up Internet connectivity quickly, whereas, a wired network can take weeks to set up and get fully functional.

**HYBRID WAN**
Hybrid WAN allows multiple wired and wireless, public and private network connections to integrate into one large interoperable wide area network for an SMB that can span multiple locations and ensure almost 100% network availability. Hybrid WAN helps affordably alleviate congestion on business networks without degrading application performance and securely offloading data directly through the Internet to remote locations, making it an appealing alternative to traditional WAN.

**LAN AND WLAN CONNECTIONS AT EACH SITE ON THE WAN**

**LAN/SWITCH**
Switches are layer 2 network devices used to link together individual devices inside a specific location defined by the router and firewall at the edge, forwarding data from one device to another. In a typical SMB environment, switches provide direct connectivity to various network devices like PCs, printers, laptops, wireless access points, etc.

**WIRELESS ACCESS POINT**
Access points provide wireless (Wi-Fi) rather than wired (switch) access to PCs, laptops, mobile phones, and other connected devices in the branch office. It gives SMBs the ability to connect both employees to their business network with greater security and allow visitors to log on to a guest Wi-Fi network with the appropriate level of access.

**WLAN CONTROLLER**
A WLAN controller is used to manage access points in a wireless network deployment. Basically, a wireless controller
provides centralized authentication, network policies, radio frequency management, wireless intrusion scanning, and other functionalities required for wireless users across the network.

INTEGRATED WI-FI/WIRELESS CONTROLLER
Both wireless access points and controllers are often found integrated within network security devices, in addition to the traditional delivery as individual pieces of networking equipment.

MANAGEMENT REQUIREMENTS FOR A TYPICAL SMB NETWORK

CENTRALIZED MANAGEMENT
With all of the network and security components previously mentioned, one can see the importance of centralized management that allows SMBs to easily manage multiple network devices from a single dashboard. IT administrators can better control their network by applying centralized configuration, policy-based provisioning, firmware upgrades, and end-to-end network monitoring. The benefits of centralized management include greater operational efficiency and reduction in overall administrative burden and cost.

MSSP MANAGEMENT
In many cases, management of SMB networks is done by third-party service providers who handle day-to-day administration while still offering visibility for the customer into their environment as well as the ability to comply with regulations. These MSSPs offer full management of the entire network infrastructure, which can scale from a small number of devices to an enterprise scale deployment.

CLOUD MANAGEMENT
Cloud management allows SMB organizations and MSSPs to manage all elements of their networks through a single console located in the cloud rather than on premises. It allows SMB organizations to turn traditional hardware into a cloud platform by automating and streamlining the deployment and providing complete visibility and control over the entire network over the web from one central dashboard. This is especially valuable for organizations with multiple sites, as well as MSSPs managing sites for multiple customers.

CLOUD SECURITY
Cloud security provides agility, visibility, and control of applications and data among varying private cloud, public cloud, and hybrid cloud deployments. A cloud platform integration through auto-scaling security automation and high availability (HA) helps avoid errors in manual configuration and provides elasticity through a single-pane-of-glass management for all security components.