SONICWALL

SOLUTION BRIEF: HOW TO STOP ADVANCED THREATS WITH NETWORK SECURITY SEGMENTS

Four key components of an effective segmentation strategy

Abstract

Network security segments are crucial to stopping advanced threats that leverage multiple areas of the network to succeed. However, defining logical segments is only part of the solution. Effective segmentation requires an integrated, dynamic network security approach to comprehensively enforce the integrity of each and every segment, and do so manageably and affordably. This paper explores best practices for what capabilities your segmentation firewall should have, and recommendations on how to apply segments for optimal security.

Introduction

As detailed in our executive brief, "Why you need network security segments to stop advanced threats," today's advanced persistent threats (APTs) take advantage of all areas of your network to attack via multiple vectors. Establishing and enforcing network security segments creates barriers to prevent these threats from propagating freely across the network, and limit the extent of capability and reach. Segment-based network security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or sophisticated attacks.

Inherently, a segment is a logical grouping of one or more interfaces designed to make management — such as the definition and application of access rules — a simpler and more intuitive process than following a strict physical interface scheme. A network security segment is simply a logical method of grouping one or more interfaces with friendly, user-configurable names,

and applying security rules as traffic passes from one segment to another segment. Security segments provide an additional, more flexible layer of security for the firewall. With the segment-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

Effective segmentation does not require a unique type of firewall. However, to succeed, it does require the segmentation firewall to have a robust set of segmentation and security capabilities. For optimal effectiveness against APTs, network security segmentation must apply an integrated set of dynamic, enforceable barriers to advanced threats. It must also meet operational requirements for performance, ease of management and affordability. The following brief describes four key components of a successful network security segmentation deployment.

A segmentation firewall checklist:

1. Flexible and scalable segmentation architecture
2. Comprehensive enforcement of segment policy
3. Wire-speed performance across segments
4. Ease of deployment and management

1. A flexible and scalable segmentation architecture

By applying security policies to the inside of the network, segmentation can be configured to organize network resources into different segments, and allow or restrict traffic between those segments. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Broadly, segments generally fall into the following categories:

- DMZ: Used for publicly accessible servers
- LAN: Can consist of multiple interfaces, each with different network subnets, but managed as a single entity
- WAN: Can also consist of multiple interfaces; when using the security appliance's WAN failover capability, a second internet interface could be added to the WAN segment
- Management: Used for appliance management
- Multi-cast: Supports IP multicasting
- VPN: Used for secure remote connectivity
- WLAN: Used for wireless access and guest services

An effective segmentation firewall should also be able to automatically enforce segmentation restrictions based upon dynamic criteria, such as user identity credentials, geo-IP location and the security stature of mobile endpoints. For extended security, the segmentation firewall should be capable of integrating multi-gigabit network switching into its security segment policy and enforcement.[1] Such firewalls should be able to apply segment policy to traffic at switching points throughout the network, and globally manage segment security enforcement from a single pane of glass.

2. Comprehensive enforcement of segment policy

Segments are only as effective as the security that can be enforced between them. For instance, the segmentation firewall should be able to apply an intrusion prevention service (IPS) to scan incoming and outgoing traffic on the WLAN segment to enhance security for internal network traffic.

For each segment, you should be able to enforce a full range of security services on multiple interfaces based on enforceable policy. Along with IPS, these security services should include, but not be limited to:

- Content filtering
- Anti-virus (and enforced client anti-virus)
- Anti-spyware
- Application intelligence and control
- TLS/SSL decryption and inspection

For optimal protection against APTs, the segmentation firewall should be able to apply cloud-based sandbox monitoring and remediation techniques. In addition, it should have the capability to enable wireless guest services for traffic transiting WLAN segments, or mandate login over HTTPS.

To enforce security policy by segment, each segment would correspond to a specific security type or category. For example:

- Trusted: A Trusted security type would provide the highest level of trust — meaning the least amount of scrutiny is applied to traffic coming from trusted segments. Trusted security may be thought of as being on the protected side of the security appliance. For example, the designated LAN segment might be considered Trusted.
- Untrusted: The Untrusted security type represents the lowest level of trust.

[1] *For example, Dell Networking N-Series and X-Series switch support is available on SonicWALL TZ600, TZ500/W, TZ400/W and TZ300/W firewalls.*

It is used by both the WAN and the multi-cast segment. Traditionally, an Untrusted segment could be thought of as being on the WAN (unprotected) side of the security appliance. By default, traffic from Untrusted segments would not be permitted to enter any other segment type without explicit rules, but traffic from every other segment type is permitted to Untrusted segments.

- Public: A Public security type offers a higher level of trust than an Untrusted segment, but a lower level of trust than a Trusted segment. Public segments can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for instance, would be a Public segment because traffic flows from it to both the LAN and the WAN. Traffic from DMZ to LAN should be denied by default. But only LAN-initiated connections would have traffic between the DMZ and LAN. The DMZ would only have default access to the WAN, not the LAN.
- Management: The Management security type would be unique to the management segment and interface, and also provide the highest level of trust.
- Encrypted: An encrypted security type would be used for VPN and SSL-VPN segments. All traffic to and from an encrypted segment would be encrypted.
- Wireless: A wireless security type could be applied to the WLAN segment or any segment where the only interface to the network consists of trusted wireless access point devices. Wireless security type works specifically well in situations where the firewall is able to automatically discover and provision the trusted access point. Only traffic that passes through such a trusted wireless access point would be allowed through a wireless segment. All other traffic would be dropped.

3. Wire-speed performance across segments

The segmentation firewall must be able to have the capability to process internal and "east-west" traffic without hampering network performance.

Distributed enterprise networks and data center environments can be especially sensitive to security features bottlenecking traffic, which in turn hampers productivity and service levels. In such environments, it is crucial that the segmentation firewall is engineered

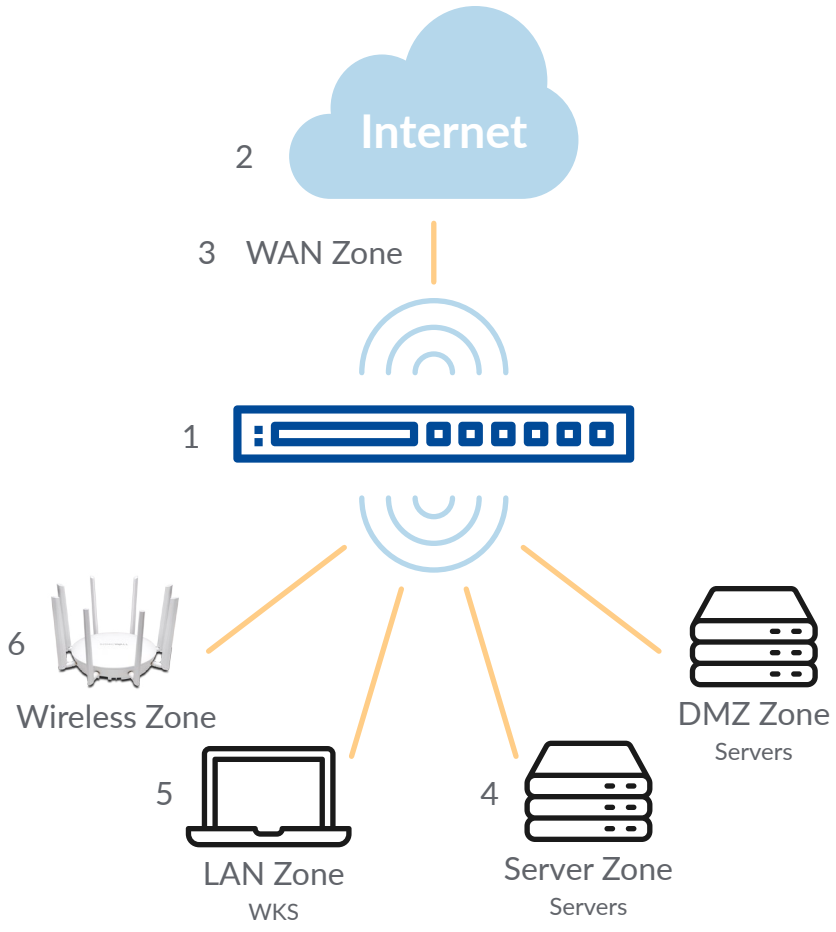

Figure 1: A segmentation-based network security model

1. By leveraging expansive network interface density and a segmented topology, the firewall should be able to segment multiple network areas into a single security appliance delivery.
2. With a significant portion of today's most popular internet sites and services now being encrypted (HTTPS), the segmentation firewall should enable deep packet inspection of SSL traffic (DPI-SSL).
3. Each segment should be able to be physically and/or logically isolated and secured from other segments on the firewall to protect against both LAN-based attacks and wireless-based attacks from mobile devices.
4. Each segment should be able to apply unique security configuration rules, including gateway anti-virus, intrusion detection and prevention, anti-spyware, anti-botnet, content filtering and application rules.
5. The firewall should be able to scan every packet, and block any malware originating on devices using unsecure networks from entering protected segments.
6. Wireless security can be further enhanced by deploying wireless access points that integrate network segmentation and security policy.

to conduct deep packet inspection (DPI) of inter-segment traffic at multi-gigabit speeds.

Third-party evaluation of firewall performance is available from independent analysts, such as NSS Labs.

4. **Ease of deployment and management**

Business and operational demands require any segmentation solution minimizes complexity and administrative overhead costs in order to promote growth and reduce total cost of ownership (TCO). To accomplish this, an effective segmentation firewall should be able to provide in-depth visibility and control over all traffic, across all segments, from a single-pane-of-glass management console. The segmentation firewall should be able to provide dynamic policy enforcement, simplify configuration of wireless and mobile endpoints, and enforce security updates.

To ease deployment, minimize disruption and enhance scalability, the segmentation firewall should be capable of being deployed in an existing network with absolute transparency, using a Layer 2 (L2) bridged mode or transparent mode. Segments should also be configured to allow full exposure of the Network Address Translation (NAT) table for control over the traffic across the interfaces, by controlling the source and destination addresses as traffic crosses from one segment to another. This means that NAT would be applied internally, or across VPN tunnels. Effective segmentation firewalls would also be able to drive VPN traffic through the NAT policy and segment policy, since VPNs would logically be grouped into their own VPN segment.

While no firewall is uniquely a "segmentation firewall," a robust and comprehensive firewall platform is required to enable effective network security segments.

A network security segmentation scenario

Depending upon the solution's flexibility and scalability, a network segment deployment could potentially use a single high-performance firewall to enforce security across its defined segments, or leverage multiple firewalls as needed.

Figure 1 on the following page illustrates an intra-VLAN deployment model. Using this approach, the firewall inspects data going between all network segments, including internal-to-internal traffic. All network traffic could be forced into the appropriate segment using VLAN tagging on switches and Layer 3 gateways on the firewall. In this scenario, APT malware might be introduced within any single segment, but will be inspected, blocked and trigger alerts as it attempts to propagate to other segments.

Conclusion

While no firewall is uniquely a "segmentation firewall," a robust and comprehensive firewall platform is required to enable effective network security segments.

To combat advanced persistent threats, a segmentation firewall must be able to attribute and enforce a broad range of security controls based upon defined segment security profiles and other dynamic criteria. It must do so in a way that also meets business and operational demands. Not all firewall solutions or vendors can deliver all the components required to stop today's advanced threats with network security segments.

SonicWall can help you meet all requirements for a secure segment network, with comprehensive, flexible network security solutions to fit any segmentation configuration. Learn more about SonicWall network security solutions at www.sonicwall.com/solutions/security-solutions.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com