Secure SD-WAN: Integrated NGFW Security with WAN Transformation

Adoption of cloud services, SaaS applications, and mobile workforce are putting increasing strain on the corporate network. This is exacerbated as organizations look to better connect their remote and branch office employees and offer them higher quality network services. Enterprises are turning to SD-WAN—a more agile, responsive, and cost-effective solution as compared to traditional network solutions—to streamline connections between their enterprise sites.

Yet, SD-WAN does not come without its challenges. The most prevalent ones include:

- While moving to direct Internet access for cloud services improves productivity, it simultaneously raises more security concerns at distributed enterprise locations.
- 90% of SD-WAN vendors are not traditional security vendors, and thus there are serious gaps with many of their solutions.

Although SD-WAN may have started as a networking technology, the future of SD-WAN lies in balanced security and advanced WAN capabilities. Fortinet Secure SD-WAN integrates Next Generation Firewalls and SD-WAN features into a single solution that simplifies deployments, improves WAN efficiency, and delivers better next-generation security.

The following Research Note from Gartner explores these issues that are transforming SD-WAN. Gartner identifies four Secure SD-WAN architectures. The biggest challenge for SD-WAN vendors is that they predominantly focus on traditional Layer 3 (L3) network control security and do not support Layer 4 to Layer 7 controls that are required for strong security solutions.

Of the four Secure SD-WAN architectures, Fortinet Secure SD-WAN matches two of them:

- Firewall with Embedded SD-WAN
- SD-WAN with a Third-Party Firewall

Gartner includes recommendations on how best to architect both of these solutions. For security leaders seeking to see how Fortinet Secure SD-WAN can scale to meet the new demands of today's—and tomorrow's—branch and regional office network landscape, request a demo of Secure SD-WAN or visit the secure SD-WAN solution web page.

Source: Fortinet

Research from Gartner

Four Architectures to Secure SD-WAN

I&O leaders responsible for network and internet security planning can use embedded security in SD-WAN products to secure internet access, but must ensure that strong security requirements also incorporate traditional next-generation firewalls or secure web gateway services.

Key Challenges

- Software-defined WAN (SD-WAN) products now incorporate internet perimeter security, but more than 90% of SD-WAN vendors are not traditional security vendors, which causes clients to question whether they can rely on embedded security alone.
- As network leaders move to employ direct internet access to their branch offices, they are challenged to identify appropriate security solutions for all their branch offices.

Recommendations

I&O leaders with responsibility for planning SD-WAN security can:

- Choose an SD-WAN security solution by grouping all sites according to their security needs and match these to the four key options.
- Secure small remote sites by using cloud-based security as a-service, because it is easier to manage for remote office than on-site solutions.
- Choose SD-WAN vendors that can demonstrate strong device and controller authentication, authorization and access control.

Strategic Planning Assumption

By year-end 2018, at least 40% of branch office SD-WAN deployments will be using SD-WAN embedded security combined with secure web gateway (SWG) services, up from less than 10% today.

Introduction

As SD-WAN is being used to manage application traffic between the branch and the public internet, many network leaders ask how SD-WAN products can be secured for direct branch office access to the internet. The question is especially pertinent as the majority of available SD-WAN products are not offered by traditional security vendors. Network leaders and security leaders are therefore questioning how to ensure that current-generation SD-WAN solutions can deliver sufficiently mature branch office security.

While these questions are sound, it is important that network leaders approach their branch office security in the context of already established security policies, as well as strategies for the broader mix of security solutions, including on-site firewalls, intrusion detection and prevention, and cloud-based security-as-a-service solutions across branch offices, cloud services and internal data centers, including any security zones within the branch offices.

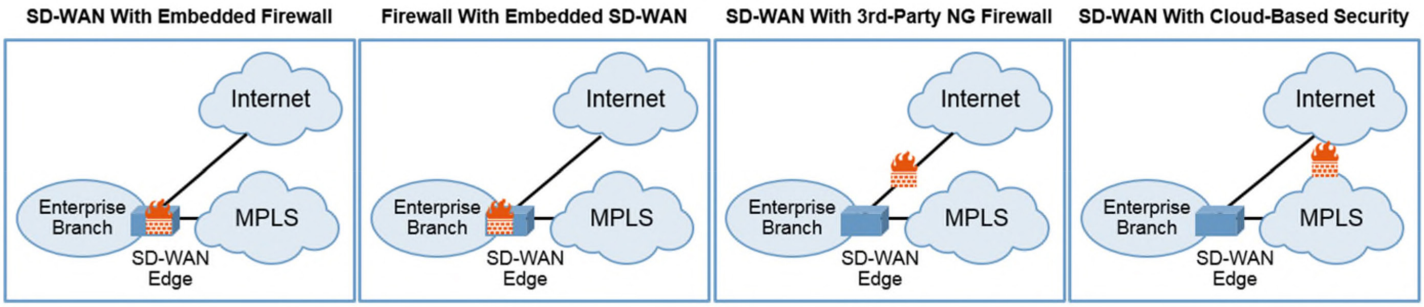
This research will outline specific evaluation criteria for four architectural options, which are outlined in Figure 1. Each of the four options can be amended with secure web gateway services. For smaller and remote offices, Gartner recommends using these services to reduce complexity. In a separate note, we discuss security services related to these choices.

Analysis

Choose an SD-WAN Security Solution by Grouping Security Needs and Matching Them to the Four Key Options

While the initial focus of SD-WAN solutions was to assist in designing and operating the enterprise WAN, we have seen most products in this market evolve with a range of security capabilities. SD-WAN vendors predominantly focus their security efforts on traditional Layer 3 (L3) network control — that is, firewall functions. However, most of these SD-WAN products do not support Layer 4 to Layer 7 controls, which are generally required for strong security solutions. This means that network planners should plan for Layer 3 security features, similar to those found in a traditional router, to be embedded within SD-WAN solutions:

FIGURE 1 Four Key Architectural Options for SD-WAN and Internet Security


SD-WAN With Embedded Firewall
Firewall With Embedded SD-WAN
SD-WAN With 3rd-Party NG Firewall
SD-WAN With Cloud-Based Security
Internet
Enterprise Branch
MPLS
SD-WAN Edge

Source: Gartner (October 2017)

- IPsec-based IP VPN
- Basic stateful firewall capabilities, such as policy-based filtering and blocking of applications, ports and IP addresses (access control list)
- Basic denial of service (DOS) prevention
- Network address translation

The majority of the pure-play SD-WAN products offer security that will suit less advanced security needs, with few exceptions. One exception is Versa Networks, which can demonstrate next-generation firewall (NGFW) certifications. For more advanced security, network planners must complement SD-WAN with a third-party NGFW, usually a branch office firewall. Conversely, besides pure-play SD-WAN products with embedded L3-based security, a few firewall vendors have also embedded SD-WAN functionality within their firewalls. These firewall-based SD-WAN solutions offer strong NGFW capabilities from L3 to L7.

Therefore, network planners have four different solutions available to secure their branch office SD-WAN:

- SD-WAN with an embedded firewall, equivalent to what is available in routers (if that is insufficient, then an NGFW is required)
- Firewall with embedded SD-WAN

Table 1 summarizes the key differences between these four scenarios.

Table 1. Comparison of Four Architectures

	SD-WAN With Embedded Firewall	Firewall With Embedded SD-WAN	SD-WAN With SWG	SD-WAN With Third-Party Firewall
SD-WAN	●	◑	●	●
Security Level	◑	●	◕	●
Branch Office Types	Smaller branch office with noncritical activities	Larger branch offices with more critical activities	Smaller remote branch office with noncritical activities	Larger branch offices with more critical activities
Relative Cost	◔	◕	◑	●
Sample Vendors	Citrix, CloudGenix, Silver Peak, VeloCloud	Barracuda Networks, Cisco Meraki, Fortinet	Symantec, Zscaler	Check Point, Cisco, Fortinet, Juniper Networks, Palo Alto Networks

Source: Gartner (October 2017)

- SD-WAN with security-as-a-service add-ons, such as SWG
- SD-WAN with a third-party firewall

If not already done, network and security leaders should group similar branch offices as separate, segmented zones to simplify the security requirements. This means that smaller offices with noncritical activities have basic firewall security only, and branch offices with more business-critical activities should have strong perimeter security. These zones should stretch from the branch offices via WAN-overlay VPN to the data centers where strong security controls should be located.

An advantage of SD-WAN is that these zones can be easily defined and managed and similar security policies can be orchestrated. In the event of a security incident, grouped branches make the response more effective, in that changes can be applied to multiple locations more easily and the work of the incident response team is made easier.

Using SD-WAN With Embedded Firewall Means an Additional Security Management Console

A key decision factor for adding SD-WAN with embedded security in branches is accepting the encumbrance of an additional console to manage for firewall functionality, as every enterprise already manages firewalls on their network. Gartner recommends that enterprises have, if possible, one brand of firewall, specifically to simplify management and reporting and prevent misconfigurations. However, if an enterprise already has routers deployed in branches where security is not managed by the firewall management console, it may already have accepted this common operational model, and SD-WAN is merely an “upgrade” to a more software-defined branch.

SD-WAN Systems Do Not Offer Advanced Security Features

While SD-WAN embedded security is similar to capabilities supported by current routers, several more advanced features are not supported by SD-WAN products, such as intrusion prevention systems (IPS), content specific controls, limited URL filtering and anti-malware protection, nor are they tailored to offer incident detection and response capabilities.

Enterprises with high-security needs where an NGFW is required should use traditional firewall vendors. Many SD-WAN vendors have partnered with traditional firewall vendors, and can host NGFWs on a virtualized appliance together with other WAN edge functionality, such as WAN optimization, as well as connect to secure gateway services such as Zscaler.

Both Barracuda and Fortinet have enhanced their firewalls with advanced SD-WAN functionality. Cisco Meraki also offers SD-WAN embedded in its firewall. Enterprises with “big security and little SD-WAN” requirements should use this option.

Recommendations:

- Group all sites according to their security needs, and choose one security solution per office group.
- Use the native SD-WAN security for basic firewall perimeter security as a basic prevention layer.
- Seek traditional next-generation firewall vendors for higher security needs, or combine on-site SD-WAN with SWG services. Do not use the native SD-WAN security to address high-security requirements.
- Use the software-defined segmentation advantages of SD-WAN to implement better zoning than traditional routers.

Secure Small Remote Sites by Using Cloud-Based Security as a Service

As enterprises move direct internet access to their remote offices, deploying and managing on-premises security controls and policies in remote locations have proven difficult to achieve due to a lack of staffing resources and security expertise. To reduce or remove these complexities, network and security leaders should use cloud-based or security as a service (SecaaS) controls to protect branch offices.

Enterprises started adoption cloud-based security to protect their remote branch offices. According to a global survey conducted by Gartner at the beginning of 2016, public cloud will be the primary delivery model for more than 60% of security applications by the end of 2017. Moreover, adoption of cloud-based security offers will remain strong, at about a 19% CAGR through 2020. This has in particular been the case for secure email gateway (SEG) and SWG tools. Based on client inquiries, Gartner estimates that over 80% of cloud-based SWG implementations are driven primarily by the remote office use case, and the remaining 20% are cloud services that are optimized for protecting mobile users. While most security controls can be sourced as a cloud service, one size does not fit all. Gartner still recommends that high-performance solutions, such as high-volume firewall or intrusion detection and prevention (IDP), are deployed via on-site appliances.

Currently, most SD-WAN vendors partner with secure web gateway services, such as Zscaler. Some SD-WAN providers, such as Aryaka, Bigleaf Networks, Cato Networks and NetFoundry, offer a broad set of security services from their WAN-based hub locations, including URL filtering, antivirus, sandboxing and firewall services.

Recommendations:

- Use SecaaS, such as secure web gateway services, to complement SD-WAN embedded security for remote offices when a third-party firewall product is not deployed.

- Reduce costs and support scaling by offloading the SWG and secure email gateway functions onto a SecaaS, even if a third-party firewall is deployed.

- Choose a third-party firewall by looking first to using the same brand as already used in your enterprise.

Secure the SD-WAN Solution With Strong Device and Controller Authentication, Authorization and Access Control

SD-WAN systems generally consist of two key components: the edge device deployed in the branch office, and the controller and management system, which are centrally deployed. Because these components potentially need to connect to each other via the internet, it is critical that the deployment and configuration can be performed securely. At a minimum, check the following:

- The control server must support role-based access control (RBAC) and firewall-like logging that is supported by your security information and event management (SIEM).

- SD-WAN edge devices must support secure tunnels to the controller and other edge devices, based on key exchanges, and provide a unique device identification and activation code.

- The solution must include a certificate server, which makes tunnel setup and key rotation fully automated for each tunnel individually.

Source: Gartner, "Four Architectures to Secure SD-WAN," Bjarne Munch, Greg Young, 6 October 2017

About Fortinet

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management, next generation firewall and high performance datacenter firewall. Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

A key differentiator, Fortinet's custom-built FortiASIC content and network processors enable our flagship FortiGate systems to detect and eliminate even complex, blended threats in real time without degrading network performance, while an extensive set of complementary management, analysis, database and endpoint protection solutions increases deployment flexibility, assists in compliance with industry and government regulations, and reduces the operational costs of security management.

US Headquarters
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737

Secure SD-WAN: Integrated NGFW Security with WAN Transformation is published by Fortinet. Editorial content supplied by Fortinet is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2018 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Fortinet's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website.