ENTERPRISE ARCHITECTURE RESEARCH GROUP

INTELLIGENCE BRIEF


# Security Controls in the US Enterprise

## Software-Defined Wide Area Network (SD-WAN)

JASON PAPPALEXIS

# Overview

Enterprise network traffic requirements continue to grow as applications, content, and hardware evolve. Reliable packet delivery between branch offices and data center headquarters is critical for business continuity, but a lack of options has left organizations saddled with expensive point-to-point links. The 5G network is on the horizon, but infrastructure requirements make it more of a three-to-five-year target for many.

The SD-WAN is a network technology that strategically complements perimeter security technology, but don't get rid of that firewall (yet).

By utilizing common VPN capabilities and by separating data and control planes within software-defined networks (SDN), software-defined wide-area-networks (SD-WANs) enable enterprises to leverage high-bandwidth, consumer-grade links (often links without guaranteed performance) for business-class services at a lower cost than traditional dedicated links. Enterprises are adopting SD-WANs for their branch office network needs—capitalizing on the visibility, scalability, performance, and control benefits the technology provides, and they are not looking back. The cost savings have a ripple effect: the SD-WAN can also reduce dedicated WAN optimization appliance footprints.

Replacing firewall technology with secure SD-WAN technology introduces additional considerations, of which security effectiveness is only one; NSS Labs has observed that secure SD-WAN products from non-firewall vendors have challenges providing the detailed information and control required of an edge security technology. Enterprises exploring SD-WAN technology should focus on network functionality and interoperability maturity to differentiate products, rather than labels (for example, the term "security" can fluctuate between vendors, referencing encryption, service chaining, and full security stack in varying degrees). For the next 12 to 18 months, NSS recommends a layered technology approach (i.e., next generation firewall + SD-WAN) for organizations intolerant to risk.

The prospect of having anti-threat capabilities bundled with WAN bandwidth management is compelling for enterprise consumers of WAN technology. NSS clients are exploring the security readiness of these products, motivated primarily by a desire to reduce their network security appliance footprint at branch offices.

## Findings

- Enterprises should not lower their expectations for security based on the cost savings of SD-WAN technology.
- Branch offload or public Internet access requires some form of packet inspection technology to reduce risk.
- Secure SD-WAN technology from non-firewall vendors is still evolving; risk-intolerant enterprises should retain their firewalls.
- The definition of security varies by SD-WAN vendor, referencing encrypted links, anti-threat capabilities, or full stack (NGFW).
- Full stack secure SD-WAN deployments retain all the challenges of NGFW deployments and more; for example, capacity planning must incorporate the performance impact once security features are activated.
- Secure SD-WAN proofs of concept (PoCs) should include testing of detection of layered evasions.
- Interoperability (API availability and maturity) is a top priority for enterprise consumers.
- 45.7% of participants in the 2018 NSS Labs Network Security Study consider security the primary benefit of SD-WAN technology.

## Table of Contents

**Overview** ..... **1**
Findings ..... 1
**Definition, Method, Deployment, and Alternatives** ..... **3**
**SD-WAN in the Enterprise** ..... **4**
Features in Use ..... 4
*Circuit Management* ..... *4*
*Full Security Stack* ..... *5*
Protection against Threats ..... 6
Management and Deployment ..... 7
Capacity Planning ..... 7
Cost ..... 8
**Secure SD-WAN as a Replacement for NGFW** ..... **9**
Secure SD-WAN – Strengths, Weaknesses, Opportunities, Threats ..... 9
Feature Parity and Impact to Risk Posture ..... 10
*Feature Parity* ..... *10*
*Impact to Risk Posture* ..... *11*
Product Capabilities and API Availability ..... 12
*API Requirements* ..... *12*
Request for Proposal and Proof of Concept Considerations ..... 13
*Planning and Development of a Request for Proposal (RFP)* ..... *13*
*Planning and Development of a Proof of Concept (PoC)* ..... *13*
**About the Enterprise Architecture Research Group** ..... **14**
**Reading List** ..... **14**
**Contact Information** ..... **15**

# Definition, Method, Deployment, and Alternatives

| Category | Description |
|---|---|
| **Definition** | The SD-WAN is the union of SDN and WAN technology. Part router, part WAN optimization, and in some cases, part firewall, the SD-WAN allows consumer-grade links (or links without assured performance) to be leveraged for business-class services.<br><br>Several SD-WAN offerings provide anti-threat functionality, which makes them a compelling alternative to the dedicated network security appliance approach that is often implemented at remote locations. NSS Labs labels an SD-WAN with anti-threat technology as a secure SD-WAN. Note that encrypted tunnels are not included in NSS' definition of anti-threat and thus are not included in the "secure SD-WAN."<br><br>NSS identifies three categories of SD-WAN vendors:<br><br>• SD-WAN only (security available through service chaining only)<br>• SD-WAN with built-in proprietary security technology<br>• Network security with proprietary SD-WAN technology |
| **Method** | An SD-WAN is a single logical WAN circuit used for establishing a secure connection (similar to a VPN) across one or multiple link types (e.g., fixed circuit, DSL, cable, mobile, MPLS), which allow traffic to be managed according to service or application priorities (e.g., VoIP vs. Facebook), and afford policy control capabilities (e.g., limit web-based traffic to 50% of a given link throughput capabilities). Individual links can be added or removed without impacting the uptime of the established circuit.<br><br>The SD-WAN permits considerable flexibility in traffic routing; remote branches can assign link types for parameters such as destination and application. For example, lower priority traffic can connect to the Internet using consumer-grade links, while high priority business traffic can connect to corporate data centers using MPLS. Consumer-grade circuits can also act as backups to the data center circuits.<br><br>Service chaining describes the capability of SD-WAN technology to support serialized network technologies (e.g., firewalls, intrusion prevention systems, load balancers). The routing is managed automatically within the system and is dynamically assessed and optimized to meet SLAs. |
| **Deployment** | Most SD-WAN deployments feature a dedicated appliance (physical or virtual). Some SD-WAN deployments leverage existing network edge technologies (routers, firewalls) to establish links between on-premises and cloud infrastructures.<br><br>The SD-WAN link is managed through a web-based central management system connected to a physical appliance, virtual appliance, or cloud architecture. |
| **Alternatives** | Traditional dedicated WAN circuit technologies such as MPLS, ATM, frame relay, and SONET |

**Figure 1 – Product Definition, Method, Deployment, and Alternatives**

# SD-WAN in the Enterprise

Many geographically distributed enterprises utilize dedicated WAN circuits to route network traffic between sites. While commonly deployed, these WAN circuits are accompanied by traditional challenges that include high bandwidth cost, significant operational costs associated with setup and runtime management, and inflexible configuration. Network congestion, packet delay variation, and packet loss are also realities facing enterprise users of this technology.

SD-WAN technology offers an alternative approach to traditional WAN circuits; however, an SD-WAN's quality of voice and video communication must be at the same level as those of the organization's service-assured circuits if it is to be considered as a replacement for business-grade communication.[1] Secure SD-WAN technology represents an opportunity for enterprises to consolidate technologies. An SD-WAN product's anti-threat capabilities as well as its capability to provide security information are key in distinguishing it from other SD-WAN products.

SD-WAN technology is rapidly evolving. NSS has witnessed tremendous change in just the last 12 months and expects even more evolution in the next 12 to 18 months. This section looks at features in use, protection against threats, management and deployment, capacity planning, purchase considerations, and cost for SD-WAN technology.

## Features in Use

NSS recognizes two categories of SD-WAN capabilities:

- Circuit management and encryption (e.g., circuit initiation, circuit teardown, load balancing, fault tolerance)
- Full security stack (e.g., NGFW feature parity; intrusion prevention, identity awareness, anti-threat, application control, etc.)

Circuit management and encryption reside at and below the transport layer, while full network stack security requires visibility through the application layer.

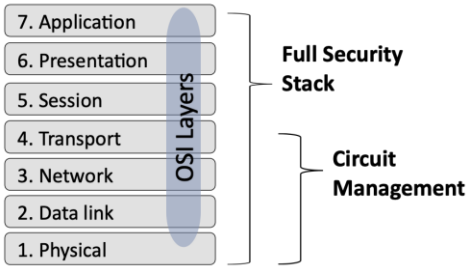



**Figure 2 – SD-WAN Features and OSI Layers**

### Circuit Management

Management of point-to-point WAN circuits is a fundamental requirement for all SD-WAN products. Enterprises evaluating SD-WAN technologies should assess the maturity of circuit management capabilities to understand if products can meet their most basic networking needs. These capabilities include:

- Streamlined workflow for the removal and addition of WAN links (circuit initiation, teardown)
- Application-aware routing, policy-based routing
- Visibility into network quality of experience (QoE)[2] for both network and applications

[1] NSS enterprise clients use information from the NSS Labs SD-WAN Group Test to assess the maturity of SD-WAN products.
[2] International Telecommunication Union: Quality of experience requirements for IPTV services

Before exploring an SD-WAN product's anti-threat and layer 7 security capabilities, it must be ascertained that it can meet the QoE requirements for its circuit. If it does not meet enterprise network requirements, there is no need to investigate it further. NSS' SD-WAN v1.0 testing[3] (2018) revealed a broad range of QoE scores among the SD-WAN products tested (both video quality and VoIP quality). Of the nine products tested, seven met or exceeded a QoE score of 4.05, which was identified as the minimum to achieve an enterprise-grade experience.

### Full Security Stack

The idea of using an SD-WAN to replace full stack inspection technology on-premises is appealing to many enterprises. A successful secure SD-WAN deployment must meet the same requirements of an enterprise's existing network security technology, typically an NGFW. At a minimum, layer 7 security features include:

- Layer 3 routing
- Policy-based firewall
- Application control
- Identity awareness, directory service integration
- Anti-threat capabilities

Anti-threat and user behavior control features, including:

- Protection from known threats (e.g., malware, exploits)
- Protection from unknown threats
- URL and content filtering

When investigating an SD-WAN as replacement for network security technology, NSS clients ask questions such as:

- How will my risk posture change if I adopt SD-WAN technology?
- How can my organization migrate our existing network firewall policies?
- Is there a best practice for rollout during the interim hybrid deployment?
- What limitations exist for interoperability with existing security products? (third-party integration)
- Is an appliance (physical or virtual) required at both ends of the WAN link?
- Do the access control capabilities of the SD-WAN technology meet our administrative needs?
- Can the SD-WAN technology meet our organization's anti-threat requirements?
- Are there limits to the types of threats that can be detected?
- Is there an operational cost to implementing anti-threat features and if so, what is it?

[3] NSS Labs 2018 SD-WAN Group Test results

## Protection against Threats

Detecting network-based threats and protecting against them is a top priority for organizations. In the 2018 NSS Labs Network Security Study nearly one-third (31.1%) of survey respondents indicated a minimum acceptable security efficacy between 95% – 99%.

Security technologies installed at the network edge are often the first and last line of defense for on-premises systems. Organizations using SD-WAN as a security technology will have the same expectations for protection against threats as for their NGFW technology, including detection of viruses, phishing attacks, ransomware, advanced persistent threats, and bots. See Figure 3.

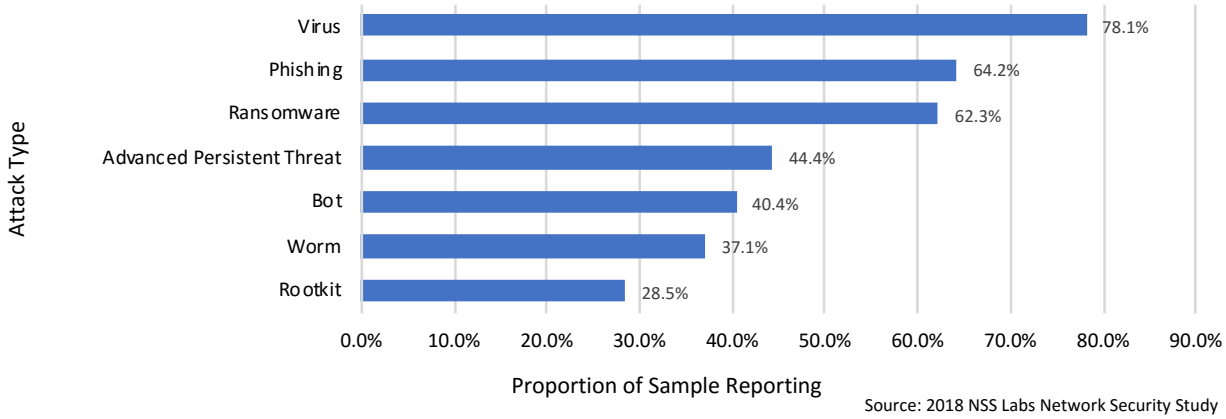



**Figure 3 – Respondent-Reported Attack Types Detected by NGFWs**

Comprehensive protection against network-based attacks is not trivial. NSS' NGFW testing reveals inconsistent historical average exploit block rates for a number of NGFW vendors, including some that are mature in the market: 89.5% in 2012 (NGFW methodology v4.0); 97.2% in 2016 (v6.0); 92.7% in 2017 (v7.0) and 96.8% in 2018 (v8.0)[4]. In addition, a 2018 investigation[5] by NSS revealed that 10 leading NGFW products were negatively impacted—some significantly so—when exploits delivered by JavaScript were transformed by one or more common code obfuscation techniques and web transport encoding mechanisms.

SD-WAN vendors entering the network security space must recognize enterprise expectations for threat detection as well as the challenges associated with meeting them. Enterprises should not reduce their expectations for protection based on the cost savings of SD-WAN technology.

[4] Evolution of Product Testing – Firewall. NSS Labs

[5] 2018 NSS Labs Investigative Report: The Impact of Code Obfuscation and Web Delivery Encoding on NGFW Scanning Accuracy

## Management and Deployment

The number of WAN links within large enterprise deployments can reach well into the hundreds. For this reason, circuit management efficiency is often described as a fundamental element of SD-WAN technology. The technology is available as a managed service as well as an enterprise-managed product. Management is typically through a secure web-based console (i.e., a web-browser utilizing HTTPS); however, NSS has observed that several vendors retain access through command line while they mature their GUI.

Enterprise operational management expenses can be reduced through automation via API. While APIs are listed as available in most SD-WAN products, NSS has observed that the maturity of security APIs is varied—often significantly so—dependent on whether the SD-WAN is part of a firewall vendor offering. SD-WAN APIs are constantly evolving; more API discussion can be found in the Product Capabilities section of this paper.

Deployment of SD-WAN technology requires a termination point (commonly called a "controller") at each end of a circuit. The SD-WAN controller can take multiple forms (illustrated in Figure 4):

- Dedicated physical appliance provided by the SD-WAN vendor
- Dedicated virtual appliance provided by the SD-WAN vendor and installed within a client-side hypervisor or a bare-metal install on dedicated common off-the-shelf (COTS) hardware
- Cloud-delivered through common public cloud providers (e.g., Microsoft, Amazon, Google)
- Feature of network edge technology (e.g., router, firewall) as physical or virtual appliance

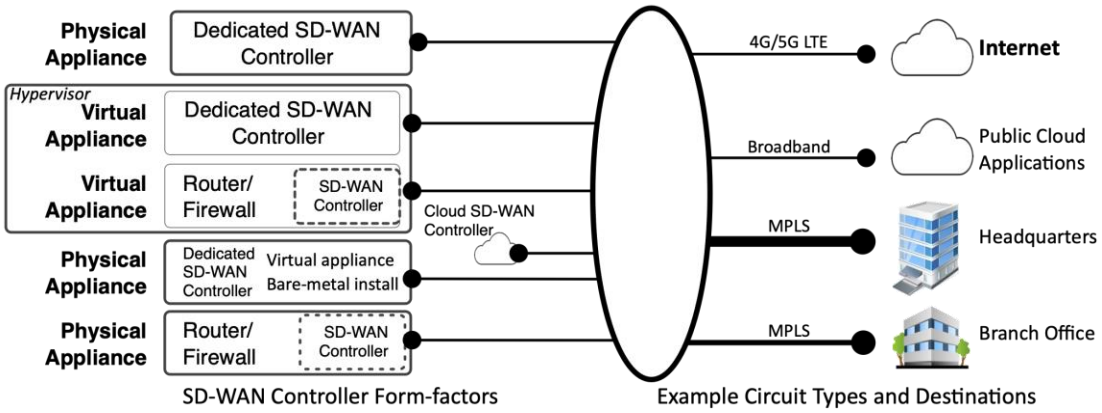



**Figure 4 – SD-WAN Controller Form Factors, Example Circuit types, and Example Destinations**

Enterprises are cautious about deploying security products inline because of the potential impact to business continuity, and secure SD-WAN is no exception. NSS expects enterprises will deploy SD-WAN technologies in a phased approach (e.g., small circuit management trial, larger circuit deployment, then security capabilities). Only once confidence is reached for each phase will enterprises consider the next level.

## Capacity Planning

SD-WAN capacity is elastic by design – as business requirements grow, throughput can expand, either by increasing the number of individual links or by increasing the capacity of existing links. QoE is important during SD-WAN capacity planning and enterprises relying on this technology for business communication should evaluate QoE metrics carefully; see the NSS Labs SD-WAN v1.0 test results for metrics from evaluated SD-WAN products.

Capacity planning for inline network security products is challenging. To accommodate environment unknowns as well as to support future organizational growth, enterprises often oversize their firewall deployments. For example, almost one-third of respondents in the 2018 NSS Labs Network Security Study indicated that their organizations target 50% above peak throughput requirements during capacity planning (see Figure 5). Expect a similar approach during capacity planning for SD-WAN controllers.

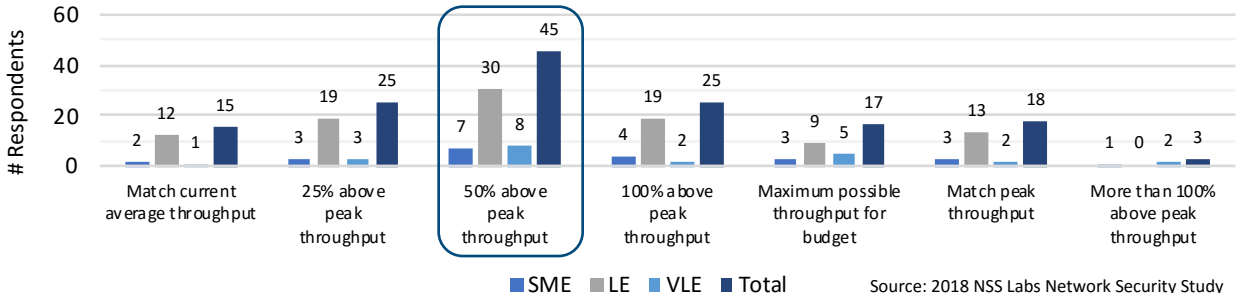



**Figure 5 – Capacity Planning Guidelines for NGFW Technology**

Sizing considerations for SD-WAN controllers for secure SD-WAN deployments will likely align with those for commonly deployed NGFW technology. The largest proportion of respondents in the 2018 NSS Labs Network Security Study (38.4%) reported choosing NGFW appliances with throughput between 2 – 10 Gbps, followed by 24.5% reporting 10 – 20 Gbps and 23.8% reporting 1 – 2 Gbps. See Figure 6.

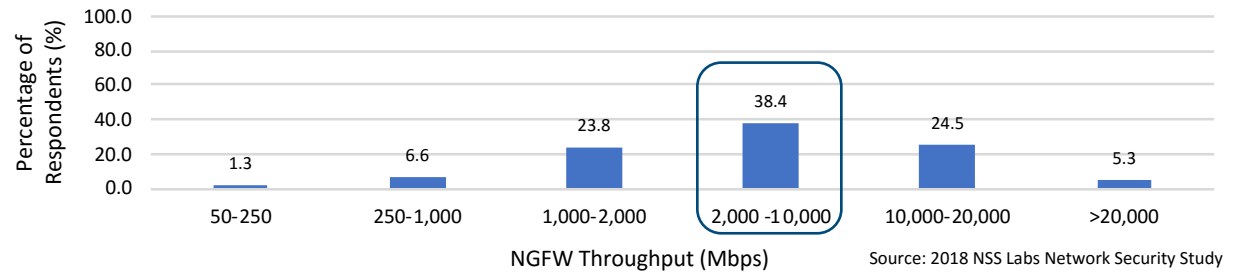



**Figure 6 – Reported Maximum Inspection Throughput of Respondents' Most Commonly Deployed NGFWs**

SD-WAN controller hardware provides a limit on throughput, regardless of the number of managed links. Activated security features will impact throughput if they are implemented on the controller rather than in a cloud-delivered workload. Enterprises evaluating secure SD-WAN technology should evaluate factors such as latency, jitter, error rate and throughput carefully.

It is a well-known fact that encrypted web traffic considerable impacts network scanning technologies when protocol decryption is activated. Enterprises must weigh the value of this feature prior to deploying SD-WAN technology in their environment.

## Cost

Enterprise investment (opex and capex) in network security products is considerable. The overall budget for an enterprise's firewall refresh project can easily exceed six figures ($US). SD-WAN technology claims to provide significant cost reductions over dedicated point-to-point WAN links. Layered security, both Tier 2 and Tier 3, would provide additional cost reductions assuming the technology meets enterprise security requirements. Cost will vary, depending on deployment form factor.

# Secure SD-WAN as a Replacement for NGFW

NSS enterprise clients have expressed interest in replacing NGFW technology with secure SD-WAN technology from non-firewall vendors in order to reduce security hardware footprints (consolidation) and operational costs. Enterprises base NGFW purchasing decisions on diverse factors, including risk tolerance, security effectiveness, throughput, and overarching IT security architecture. If firewall deployments are to be replaced with secure SD-WAN technology, then the technology must be evaluated against the same requirements. Is a secure SD-WAN from a non-firewall vendor a viable option for your organization? In our opinion, secure SD-WAN products from non-firewall vendors currently do not meet all firewall use cases and should be evaluated carefully.

## Secure SD-WAN – Strengths, Weaknesses, Opportunities, Threats

### Strengths

- Answers multiple high-profile needs; enables full-service WAN perimeter (SD-WAN, security, WAN optimization, load balancing, etc.)
- Potential for reduced capital costs
- Bandwidth and link control based on policy, application, URL, and destination is appealing for branch office deployments and growing use of cloud workloads and storage
- Growing number of SD-WAN vendors layering security over network; competition breeds differentiation

### Weaknesses

- Many new SD-WAN companies with young company challenges expanding into security (e.g., security technology effectiveness, customer support, global presence, root cause analysis data, SLAs, etc.)
- There are three types of vendor, and each may approach the technology differently: WAN circuit-only vendors relying on third-party security; WAN circuit vendors with proprietary security technology; network security vendors with SD-WAN technology
- Capacity planning for an all-in-one security and network appliance is challenging
- Translating existing firewall policies into a non-firewall-based SD-WAN product may be complex
- Enterprise risk metrics may require retooling based on data availability on a non-firewall-based SD-WAN

### Opportunities

- Manual firewall policy review would facilitate culling of policies (increases operational costs)
- Secure SD-WAN technology is young; as it matures, it will likely impact multiple network consumption models

### Threats

- Enterprises evaluating secure SD-WAN technology must consider the security impact to their business:
    - Maturity of QA/validation of signatures prior to production rollout
    - Potential impact of false positives and false negatives on business
    - Potential misalignment between separate teams when collapsing network and security
    - Challenges with feature parity between NGFW and secure SD-WAN
    - Collapsed WAN and security broadens impact of firmware bugs/faults
- SD-WAN on COTS may reduce ability to scale and introduce other uncertainties (e.g., performance)

## Feature Parity and Impact to Risk Posture

NSS enterprise clients considering replacing existing NGFW technology with secure SD-WAN technology have expressed concerns over feature parity ("What is my organization gaining/losing?") and risk ("How has my organization risk posture changed?"). These concerns should be addressed to facilitate a successful secure SD-WAN deployment.

### Feature Parity

Our experience with firewall and SD-WAN technologies allows us to highlight critical areas enterprises should investigate during PoC activities. Enterprises should evaluate these areas according to their specific requirements for the technology. Figure 7 compares the maturity of security features for traditional NGFW technology and for non-firewall-based secure SD-WAN technology.

| Feature | | Traditional NGFW Technology | Secure SD-WAN Technology from Non-Firewall Vendors |
|---|---|---|---|
| Packet filtering | | High | (2016) Very low, (2018) Medium |
| Stateful multi-layer inspection | | High | Low/Medium |
| NAT, high availability, layer 3 functionality | | No observed challenges | No observed challenges |
| VPN | | No observed challenges | No observed challenges but third-party hardware may be required |
| Application awareness/control | | Medium/High | Medium |
| User/group control | | High | Medium/Low |
| Integrated Intrusion prevention system (IPS) | | High | Medium |
| Anti-threat | | Medium/High | Low/Medium |
| Forensic threat information | | Medium/High | Low/Medium |
| Application Programming Interface (API) | *Security* | High | Low/None |
| | *Network* | High | Medium/High |
| Logs | *Security* | High | Low |
| | *Network* | High | Medium |
| Real-time diagnostics | *Security* | High | Medium/Low |
| | *Network* | High | High |
| Alert handling | | High | Low/Medium |
| Central Management System (CMS) | | Network and security both typically mature | Network more mature than security |

**Figure 7 – Comparison of Security Features**

## Impact to Risk Posture

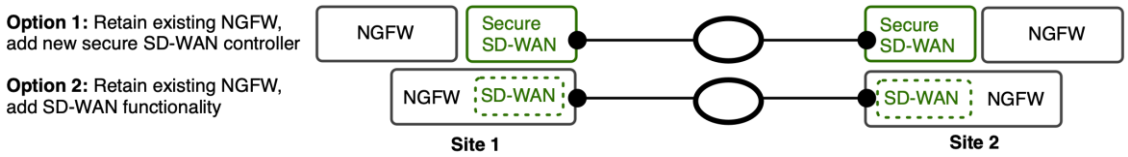
Non-firewall vendors in the secure SD-WAN industry are encouraging enterprises to explore replacing NGFW appliances with their technology. However, enterprise IT security teams evaluating this technology recognize that any impact on organizational risk must be included in evaluations.

Figure 8 illustrates SD-WAN deployment options to consider based on an enterprise's risk tolerance.

**Enterprise is Intolerant to Risk**

*Option 1: Retain existing firewall in production and add secure SD-WAN technology as separate controller*

*Option 2: Add SD-WAN to existing firewall if available*




- Retaining a firewall allows for predictable security capabilities and risk measurement; there is also less need for training, less likelihood of policy misconfiguration, and existing security integrations can be maintained
- A secure SD-WAN controller from a vendor other than the NGFW vendor leverages WAN link cost savings and provides time to assess support quality, reliability, security capabilities, etc.
- Adopting SD-WAN capabilities into the existing NGFW provides the low potential of change in risk.

**Enterprise is Somewhat Tolerant to Risk**

*Deploy new firewall with SD-WAN capabilities if existing firewall does not offer SD-WAN*


- New technologies of any kind introduce some risk as products are deployed, tuned, and understood.
- Multiple firewall vendors with consistently high security effectiveness scores offer SD-WAN technology.[6]
- This option is not recommended for enterprises seeking to replace a firewall with a secure SD-WAN from a non-firewall vendor because of high deployment costs and lack of visibility into capabilities.

**Enterprise is Tolerant to Risk:** *Replace firewall with secure SD-WAN technology*


- Enterprises tolerant to risk could consider replacing NGFW technology with secure SD-WAN technology, but this is not recommended until the security features, interoperability and security effectiveness of secure SD-WAN technology mature.

**Figure 8 – SD-WAN Deployment Considerations Based on Risk Tolerance**

[6] NSS Labs 2018 SD-WAN Group Test

## Product Capabilities and API Availability

Products from SD-WAN technology vendors differ according to whether a vendor has a networking background (i.e., WAN) or a security background (i.e., firewall). Figure 9 displays vendor approach, claimed features, API focus and API availability.

While network APIs are commonly available, security APIs are most provided by firewall vendors or SD-WAN vendors with proprietary security technology. Enterprises that are intolerant to risk and that are looking to consolidate (or simplify) their network security architectures should first consider SD-WAN products from firewall vendors in order to maintain a consistent level of data.

| | Vendor Approach | Proprietary Security? | Claimed Features | | API | |
|---|---|---|---|---|---|---|
| | | | Circuit Management | Full Security Stack | Network | Security |
| Vendor A | WAN | No | Yes | No | Yes | No |
| Vendor B | Firewall | Yes | Yes | Yes | Yes | Yes |
| Vendor C | WAN | Yes | Yes | Yes | No | No |
| Vendor D | WAN | No | Yes | No | Yes | No |
| Vendor E | Firewall | Yes | Yes | Yes | Yes | Yes |
| Vendor F | WAN | No | Yes | No | Yes | No |
| Vendor G | WAN | No | Yes | No | Yes | No |
| Vendor H | Firewall | Yes | Yes | Yes | Yes | Yes |
| Vendor I | Firewall | Yes | Yes | Yes | Yes | Yes |
| Vendor J | WAN | No | Yes | No | Yes | No |
| Vendor K | WAN | No | Yes | No | Yes | No |
| Vendor L | WAN | Yes | Yes | Yes | Yes | Yes |
| Vendor M | Firewall | Yes | Yes | Yes | No | No |
| Vendor N | WAN | No | Yes | No | Yes | No |
| ***Number of Yes:*** | | 7 (50%) | 14 (100%) | 7 (50%) | 12 (86%) | 5 (36%) |

*Data obtained through secondary research, not NSS Labs testing

**Figure 9 – Approach, Proprietary Security, Features and API Availability from 14 SD-WAN Products**

### API Requirements

Automation capabilities (i.e., interoperability, often through API) are often discussed during NGFW product selection inquiry with NSS clients. This aligns with results from the 2018 NSS Labs Network Security Study where almost half of the respondents (46.4%) indicated “Very” and 40.4% indicated “Extremely” when asked how important API features are during NGFW product selection. A five-point scale was used, with study respondents having the option to select “Extremely,” “Very,” “Moderately,” “Slightly,” or “Not at all.”

NSS Labs expect API requirements for NGFW to align with requirements for secure SD-WAN technologies.

## Request for Proposal and Proof of Concept Considerations

Enterprises considering secure SD-WAN products from non-firewall vendors as replacements for NGFW technology can use the following information as guidance.

### Planning and Development of a Request for Proposal (RFP)

- Determine your use case(s) and gather requirements from all teams that require operational access to the management console, event data, log data, etc.
- For environments requiring business-grade communication, use QoE metrics to pare your list of SD-WAN candidates prior to PoC.
- If you are replacing your NGFW, request data on API maturity (i.e., the presence of comprehensive documentation, support for industry standards, etc.) and evaluate your organization's need for forensic threat details.
- Focus the RFP on product capabilities and measurable results rather than marketing claims.
- RFP requirements should be highly focused, ideally prompting only "yes" or "no" answers from vendors; this will dramatically simplify review of RFP responses.
- Prioritize and weight requirements in order to simplify final decisions; separate your "wants" from your "needs."

### Planning and Development of a Proof of Concept (PoC)

- Clearly list the capabilities the PoC must provide guidance on, focusing on what is measurable. Determine which test cases can be run internally and which require third-party resources.
- Evaluate the SD-WAN product's QoE and management capabilities.
- Understand how anti-threat security features will impact business applications.
- If possible, evaluate the secure SD-WAN using production traffic to understand if it meets current NGFW product requirements for remote/branch offices.
- Evaluation of the management console workflow should include exploring what threat and system data is available through the management console, API, and logs.
- Rigorously test false positives within your production environment. Excessive false positives can dramatically impact operational workflows, and NSS has found considerable differentiation between products in this area.
- Threat detection testing should include layered evasion capabilities; this is a lagging area for many firewall technologies.

# About the Enterprise Architecture Research Group

The mission of the Enterprise Architecture Research Group is to work with enterprises to solve security architecture and product challenges. We provide research and advisory services that are objective, accurate, reliable, and actionable. Our data comes from NSS test results, first-hand experience in the lab, novel primary research, and interaction with our enterprise clients.

# Reading List

Evolution of Product Testing: Firewall. NSS Labs. June 7, 2018
https://research.nsslabs.com/library/network-security/evolution-of-product-testing-firewall-2012---2018/

2018 NSS Labs Investigative Report: The Impact of Code Obfuscation and Web Delivery Encoding on NGFW Scanning Accuracy. NSS Labs. August 14, 2018
https://research.nsslabs.com/library/research/investigative-report/investigative-report-the-impact-of-code-obfuscation-and-web-delivery-encoding-on-next-generation-firewall-scanning-accuracy/

Software-Defined Wide Area Network Group Test v1.0. NSS Labs. August 8, 2018
https://research.nsslabs.com/library/network-security/software-defined-wide-area-network/

# Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com