SOLUTION BRIEF

Are Legacy Routers Putting Your Cloud Transformation at Risk?

Using a Fortinet Secure SD-WAN Assessment to Facilitate WAN Transformation

Executive Overview

Software-defined wide-area networking (SD-WAN) has quickly become the de facto solution for legacy WAN infrastructure replacement in distributed organizations. But not all SD-WAN approaches are the same. While some implementations simply add basic SD-WAN capabilities to existing legacy routers (featuring a stateful firewall for security), this adds infrastructure complexity while exposing branches to undue security risks. A Secure SD-WAN solution—such as FortiGate Secure SD-WAN—consolidates networking, routing, and security infrastructure in a single, organically developed solution. It provides network engineering and operations leaders with robust branch WAN networking capabilities that support the latest high-performance digital applications while ensuring seamless security across branch deployments.

IDC predicts that worldwide SD-WAN infrastructure and services revenue will see a compound annual growth rate (CAGR) of over 40% to reach $4.5 billion by 2022.[1]

Replacing Legacy Routers with SD-WAN

Network engineering and operations leaders have struggled to incorporate digital innovation initiatives at branch and remote locations due to the limits of traditional WAN infrastructures featuring legacy routers. Specific problem areas include:

- Business application performance issues due to traffic bottlenecks
- Increasing costs due to expensive multiprotocol label switching (MPLS) connectivity
- Limited infrastructure visibility and associated security issues

SD-WAN is increasingly seen as the solution for addressing these problems. And while a basic SD-WAN solution can be swapped out for traditional WAN networking, other legacy parts of the branch infrastructure are not necessarily SD-WAN ready. For example, many organizations currently rely on legacy routers featuring a simple stateful firewall for branch network security. These outdated devices typically lack key features such as:

- Application visibility into cloud traffic and business applications. This limitation increases vulnerability of branch network intrusions via the cloud. Critical applications in this area often include Microsoft Office 365 and Salesforce as well as unified communications tools for voice and/or videoconferencing.
- Bandwidth utilization capabilities that manage bandwidth/performance based on the application. It is important that bandwidth becomes smart in order to reduce WAN cost (via over-reliance on expensive MPLS connectivity). Effective bandwidth utilization capabilities require intelligent application awareness that selects and manages a range of connection options based on specific application and user priorities.
- Advanced security that applies real-time threat intelligence against the latest malware, botnets, and zero-day attacks. For example, inspection of encrypted network traffic is now essential, but at the same time, these security checks should not inhibit network or application performance.

Stitching SD-WAN functions onto a legacy router is an inefficient approach to upgrading WAN infrastructure. This method increases infrastructure complexity and overall costs while still lacking advanced features for visibility, security, and application awareness as well as unified management functionality. Networking teams typically struggle to maintain and protect branch networks that require a proliferation of point products to address new, advanced threat exposures as well as a growing set of compliance standards and requirements.

FortiGate Secure SD-WAN offers a consolidated networking, routing, and security solution for comprehensive and effective SD-WAN implementation. Fortinet's approach to SD-WAN supports:

- **Simplified operations** with built-in features such as zero-touch deployment and single-pane-of-glass management
- **Reduced cost** through application awareness that optimizes dynamic broadband connectivity while lowering WAN operating expenses (via MPLS connectivity)
- **Cloud-ready branches** by enabling secure network bandwidth and user quality of experience (QoE) for adoption of cloud on-ramping for things like Software-as-a-Service (SaaS) applications and Infrastructure-as-a Service (IaaS)

Fortinet has seen a 60% surge in global assessments in the first half of 2019; approximately 84% of these assessments have been for organizations with more than 1,000 users.

Fortinet Secure SD-WAN Assessment Program

A Fortinet Secure SD-WAN Assessment can help distributed organizations explore the value that FortiGate Secure SD-WAN can offer their current edge networking infrastructure. Network engineering and operations leaders can run a Secure SD-WAN Assessment behind their existing legacy router to assess the state of their current application, WAN, and security postures. Since Fortinet launched its assessment reporting program in 2015 with the NGFW testing, thousands of network engineering and operations leaders have used the service to evaluate security effectiveness within their environments.

The Fortinet Secure SD-WAN Assessment monitors activity within a network over several days, which is collected into logs. It then generates a report to help network engineering and operations leaders evaluate the potential business outcomes of FortiGate Secure SD-WAN within their actual, real-world environment. The Fortinet Secure SD-WAN Assessment report provides detailed measurements and analysis of critical SD-WAN networking and security areas while allowing decision-makers to experience Fortinet's immediate value—without disruption to their network.

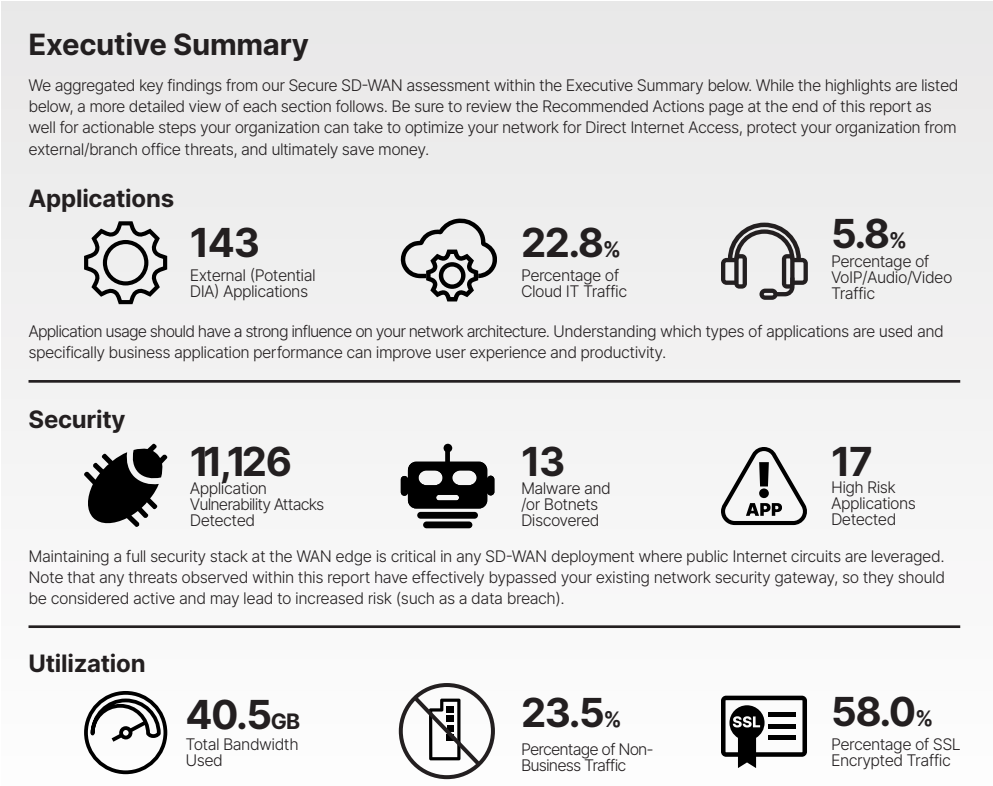

Figure 1: Fortinet Secure SD-WAN Assessment Report executive summary (example).

Application visibility and user experience

This detailed Fortinet Secure SD-WAN Assessment report section helps network engineering and operations leaders understand not only which applications are being used but also how they are used within the network. This is done in terms of connections to internal and external resources. The top applications and their bandwidth usage are sorted into different categories—such as Voice over IP (VoIP), video, collaboration, social media, and so forth (Figure 2). In addition to bandwidth usage, this data helps networking and operations teams to understand the performance and usage of specific applications operating in accordance with corporate service-level agreement (SLA) and usage policies.

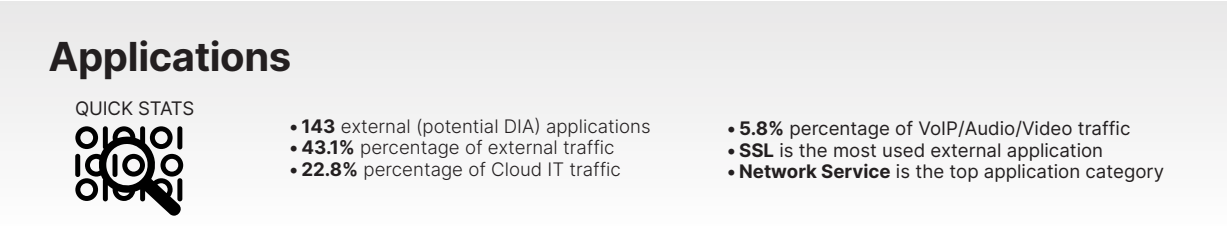

Figure 2: Applications statistics: summary (example).

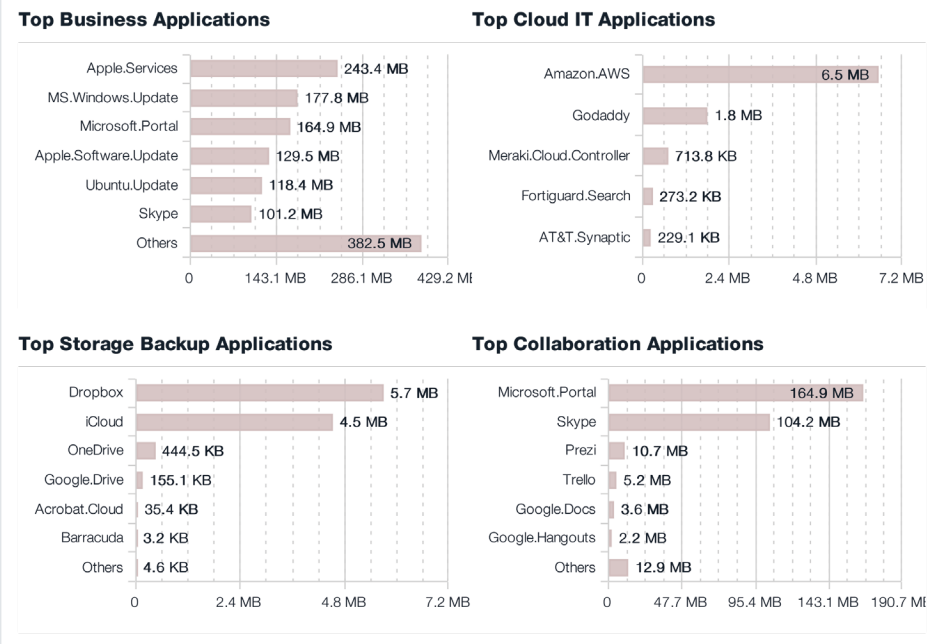

Figure 3: Applications statistics: breakout detail (example).

Bandwidth utilization and performance

The Fortinet Secure SD-WAN Assessment report's utilization analysis helps network engineering and operations leaders to determine bandwidth utilization across distributed branch locations by enabling them to see which locations consume the most bandwidth (Figure 4). It also gives them insights on top bandwidth-consuming host and destination resources. This section can help network engineering and operations leaders to ensure that WAN links are utilized and optimized for cost-effective operations without compromising user experience. It can also help them to start to extrapolate costs associated with inefficient WAN solutions (such as MPLS-based connectivity costs).

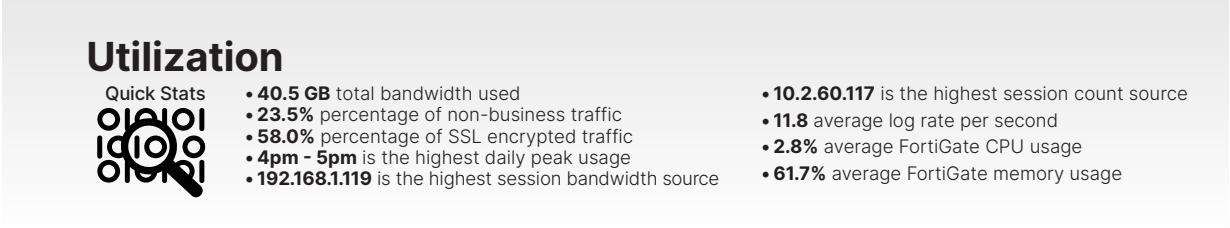

Figure 4: Utilization statistics: summary (example).

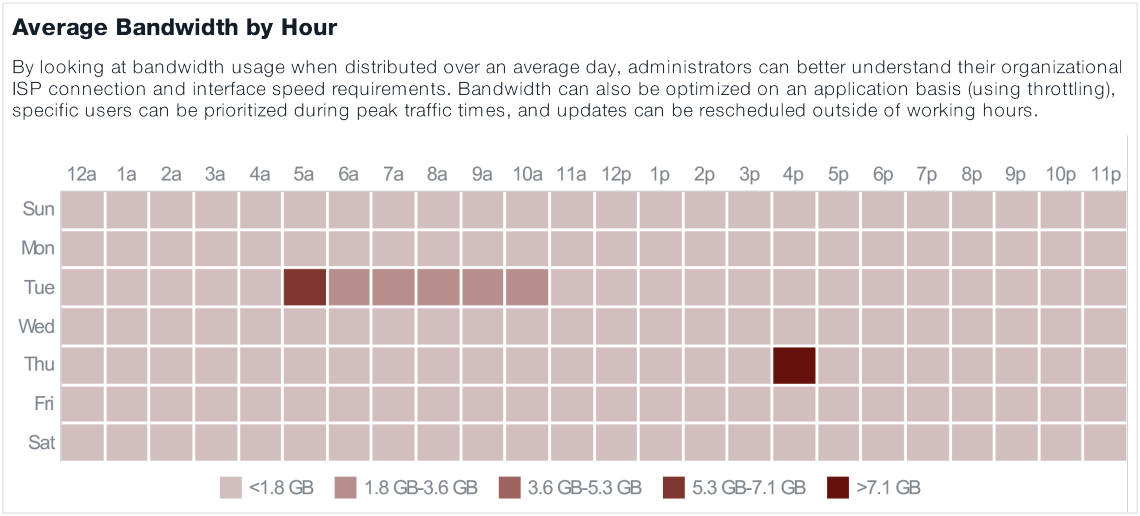

Figure 5: Utilization statistics: bandwidth-by-hour analysis (example).

Security and threat prevention

The Fortinet Secure SD-WAN Assessment report's security analysis section evaluates the state of how the organization currently secures the traffic breaking out locally from the branch. It highlights high-risk applications used on the network, pinpoints top threats based on application vulnerability exploits detected, and even identifies devices/hosts that are currently at risk on the network (Figure 6). This information helps network engineering and operations leaders ensure that critical protections are not compromised.

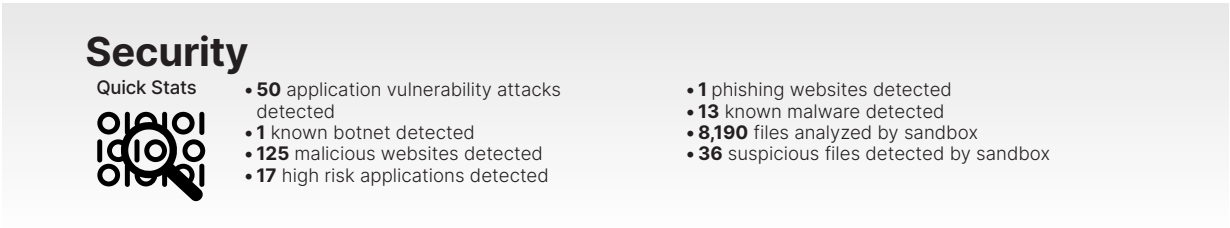

Figure 6: Security statistics: summary (example).

High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
4	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
5	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
6	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
7	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
8	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
9	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38
10	4	FlashGet	P2P	Peer-to-Peer	3	309.78 KB	37

Figure 7: Security statistics: high-risk application ranking (example).

Organizations need scalable secure sockets layer (SSL)/transport layer security (TLS) inspection to verify the ever-increasing volume of network traffic that is encrypted. Indeed, as much as 60% of encrypted traffic contains hidden malware.[2] But in many SD-WAN deployments, encryption inspection causes wide-ranging performance degradation due to the limitations of legacy network firewalls.

Top Malware, Botnets and Spyware/Adware Detected

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, Fortinet identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

#	Malware Name	Type	Application	Victims	Sources	Count
1	EICAR_TEST_FILE	Virus	FTP	1	1	824
2	EICAR_TEST_FILE	Virus	HTTP	1	1	792
3	Asprox.Botnet	Botnet C&C	Asprox.Botnet	55	1	600
4	Adware/TEST_FILE	Adware	HTTP	1	1	411
5	ETDB_TEST_FILE	Virus	FTP	1	1	406
6	W32/NGVCK	Virus	HTTP	1	1	405
7	W32/ForeignRansom.583D!tr	Virus	HTTP	1	1	400
8	W32/ForeignRansom.583D!tr	Virus	FTP	1	1	395
9	W32/NGVCK	Virus	FTP	1	1	384
10	Adware/TEST_FILE	Adware	FTP	1	1	379

Figure 8: Security statistics: malware, botnet, and spyware/adware detail (example).

Recommendations

This section of the Fortinet Secure SD-WAN Assessment report offers customized recommendations for network leaders to take next steps in improving their branch network security posture (see Figure 9).

Recommendations

1. Leverage Direct Internet Access for External Traffic

Approximately 43.1% of all organizational traffic was classified as external. If you haven't done so already, weigh routing external traffic remotely versus backhauling through a centralized gateway. This will optimize traffic flows and reduce overall operational costs.

2. Create Service Level Agreements (SLAs) for Key Applications

A significant number of applications were detected which are communicating with external (e.g. cloud-based) servers. When architecting an SD-WAN rollout, ensure that these applications are selecting WAN links that meet performance (latency, jitter, and packet loss) criteria.

3. Route High Bandwidth Applications Through Broadband Circuits

We detected a large amount of high bandwidth applications (typically Audio/Video streaming, P2P, etc.) which are consuming your available bandwidth. If that traffic is originating from your branch offices, we suggest that you consider Direct Internet Access for those applications when setting up your SD-WAN.

4. Augment Your Security to Protect Against Known Malware

Known malware is currently bypassing your existing gateway controls. We recommend that you verify the malware signatures on your existing firewall are up to date. If those signatures are already current, consider either augmenting your security with a secondary gateway or replacing your existing firewall.

5. Add Sandboxing Technology to Detect Unknown Malware

Files exhibiting suspicious behaviors (potentially unknown malware) were detected. Consider implementing sandboxing technology to supplement your gateway security solution.

6. Inspect Encrypted Traffic

A significant amount of your organizational network traffic is encrypted. Contemplate implementing SSL inspection to ensure full application visibility and traffic inspection.

Figure 9: Customized recommendations: summary (example).

The Path Toward Comprehensive WAN Consolidation

Fortinet is the only vendor with a purpose-built SD-WAN ASIC. As a result, FortiGate Secure SD-WAN is able to deliver the fastest application identification and best application accuracy on the market. Deep SSL/TLS inspection can be performed on all traffic, ensuring that important application traffic is identified without negatively impacting the end-user's experience. Optimal network performance is maintained for business-critical applications while ensuring comprehensive security effectiveness.

Using a Fortinet Secure SD-WAN Assessment report, network engineering and operations leaders can validate their application performance, cloud connectivity optimization, security posture, and operational costs of the WAN edge. They can also use it to plot a path toward:

1. WAN edge simplification
   FortiGate Secure SD-WAN consolidates point products to simplify branch infrastructure. This enables bandwidth-constrained network teams to facilitate the transition to SD-WAN.
2. WAN TCO reduction
   FortiGate Secure SD-WAN reduces WAN costs while providing better security at the edge (e.g., use of direct internet connections, application awareness for bandwidth management, automation, etc.). Indeed, FortiGate Secure SD-WAN delivered the lowest total cost of ownership (TCO) per Mbps based on real-life scenarios in the latest NSS Labs testing.[3]
3. Business agility
   A Fortinet Secure SD-WAN Assessment report can help network engineering and operations leaders to target specific problem areas with existing branch infrastructure to facilitate the transition to SD-WAN implementation.

[1] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022," IDC, August 8, 2018.

[2] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[3] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019.

April 9, 2021 12:52 PM
sb-FA-are-legacy-routers-putting-your-cloud-transformation-at-risk
498185-B-0-EN