CHECKLIST

SIX REASONS WHY FORTINET SECURE SD-WAN IS THE RIGHT CHOICE

By the end of 2019, 50% of enterprises will use SD-WAN technology across their remote sites—up from less than 1% today.[1] However, the performance and convenience gains of SD-WAN over traditional WAN come largely at the expense of centralized security provided by backhauling network traffic through the data center, where everything can be checked and filtered in one place. And while the use of public links for direct internet access in an SD-WAN architecture provides improved options for enterprise-wide delivery of cloud applications, this also introduces new vulnerabilities and an expanded attack surface.

FORTINET SECURE SD-WAN FOR DISTRIBUTED NETWORK ARCHITECTURES

With this in mind, it is extremely important to ensure you select the right SD-WAN solution. Fortinet Secure SD-WAN delivers all the essential capabilities needed for maintaining secure operations across multiple branches and remote locations. Following are six reasons why Fortinet Secure SD-WAN is the right fit for enterprises:

1. NEXT GENERATION FIREWALL (NGFW) SECURITY. The FortiGate Next Generation Firewall (NGFW) provides best-of-breed, integrated SD-WAN networking and security capabilities in a single device. It offers a multifunctional solution with SD-WAN-ready features for efficient adoption of public cloud applications. Following are some of its key features:

- Offers combined **NGFW protection** and **SD-WAN networking** capabilities in one device.
- Purpose-built **security processors** enable better performance for **SSL inspection** to unlock encrypted sessions, see into encrypted packets, find threats, and block them.
- First line of defense **web filtering** against web-based attacks by blocking access to malicious, hacked, or inappropriate websites (only web filtering service in the industry that is **VBWeb certified**[2]).
- Security processor-powered high **IPsec VPN** and **threat protection performance** for secure communications.
- Track **real-time activity** to facilitate risk assessment, detect potential issues, and mitigate problems, while automating **compliance audits** with firewall rules and policies.

2. SD-WAN NETWORKING. Cloud application adoption is driving much of the need for superior networking capabilities. The router or firewall responsible for SD-WAN connectivity needs to intelligently balance internet and intranet traffic across the available WAN services. Following are key reasons why Fortinet Secure SD-WAN is the right choice:

- Dynamic **cloud applications database** that routes applications on the same ports and bandwidth to accommodate SaaS apps where IP addresses change frequently.
- FortiOS **path awareness intelligence** supports dynamic routing based on link quality measurements to maintain high availability of business-critical applications and complete visibility into applications.
- **Agnostic channel delivery** supports a wide range of cost-effective connectivity options to **mix and match multiple broadband connections** (internet, MPLS, LTE, etc.) for the direct use of public internet connections.

3. CENTRALIZED CONSOLE MANAGEMENT. Although able to extend the full range of security features with each new network connection (wired or wireless), SD-WAN should be fully managed from a central location. Here's how Fortinet Secure SD-WAN makes that possible:

- Through **a single-pane-of-glass console**, Fortinet Secure SD-WAN provides **transparent visibility** across the network and **unified policy management** and **centralized VPN control** across all branch/remote locations.

☐ **4. ZERO-TOUCH DEPLOYMENT.** Automatic device provisioning and branch deployments (without the need for skilled network engineers to be sent to each location) save vast amounts of time in comparison to the involved processes of adding branches in traditional WAN environments. Here's how Fortinet Secure SD-WAN streamlines this entire process:

- FortiOS dynamically builds the entire physical and logical network topology once a FortiGate is launched (see diagram).

☐ **5. LOW TCO.** Less expensive connectivity, simplified deployment, and centralized management via a single-box solution for both networking and security operations deliver as much as 50% better TCO versus architectures with separate security and networking devices.

☐ **6. DETECTION AND REMEDIATION.** Cybersecurity involves more than just **prevention**, as it is impossible to stop all attacks. It also involves **detection** and **remediation**. Having a security solution such as Fortinet Secure SD-WAN that delivers high performance and efficacy with optimal cost-effectiveness is key. (FortiGate received recommendations for **superior performance** and **security** in the NSS Labs 2017 **Next-Generation Firewall Test Results**.[3])

GET STARTED TODAY

The time to move to SD-WAN is now. Organizations that fail to make the move put themselves at a competitive disadvantage, with 50% of enterprises predicted to migrate to SD-WAN by 2019.[4] The benefits are tangible and quite achievable given the selection of the right technology. And Fortinet Secure SD-WAN offers the best of networking and security capabilities in one solution.

1. Andrew Lerner and Neil Rickard, "Market Guide for WAN Edge Infrastructure," Gartner, March 2017.
2. Martijn Grooten and Adrian Luca, "VBWeb comparative review February 2016," Virus Bulletin, February 2016.
3. "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," NSS Labs, November 2017.
4. Andrew Lerner and Neil Rickard, "Market Guide for WAN Edge Infrastructure," Gartner, March 2017.

Jan 9, 2018 3:39 PM
Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Checklist-SD-WAN:Checklist-SD-WAN.indd