UPGRADE YOUR WAN INFRASTRUCTURE USING FORTIGATE SD-WAN

Enterprises are adopting digital transformation to embrace an increase in productivity and allow businesses to grow at a rapid rate. A key component of digital transformation is to move the infrastructure or services to the cloud, which allows enterprises to get started immediately. "Enterprises must alter their WAN architectures in support of new digital business initiatives and adoption of public cloud services, which are forecast to grow 86% between 2014 and 2018."[1] With cloud migration, traffic from branches to the cloud is backhauled, which decreases application performance. Backhauling cloud traffic can not only increase the latency but also create security concerns. According to Gartner, "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."[2] Gartner recommends to "choose SD-WAN vendors that can demonstrate strong device and controller authentication, authorization and access control."[3]

As administrators weigh the pros and cons of traditional WAN solutions, it becomes obvious that there is an immediate need for a replacement infrastructure with significant simplification, improved cost advantage, and better support for cloud adoption. SD-WAN technology fills that need by effectively routing network traffic from branches to the cloud, headquarters, or other branches. It allows branches to directly access cloud applications by dynamically utilizing broadband connections, thereby increasing network performance and reducing costs. SD-WAN also takes an application-centric approach, allowing enterprises to maximize the available bandwidth for business-critical applications, and increasing the ROI.

FORTIGATE SD-WAN

Secure SD-WAN can be enabled on the FortiGate Next Generation Firewall. Fortinet was recognized as a Leader in the Gartner Magic Quadrant for Enterprise Network Firewalls.[4] FortiGate also has the lead in total number of annual security unit shipments worldwide, according to IDC.[5] FortiGate combines NGFW and SD-WAN features into a single solution that improves WAN efficiency and security. FortiGate SD-WAN includes these key components:

- **Application Aware**
  With traditional WAN, enterprises have a hard time maintaining the quality of user experience per application. Traditional WAN infrastructure relies on packet routing, and isn't application aware. FortiGate SD-WAN helps customers gain visibility into the applications being used across the enterprise so that customers can make well-informed decisions while creating SD-WAN policies. Fortinet has a rich database to identify over 3,000 individual applications. Even with cloud applications, where the traffic is encrypted, FortiGate SD-WAN can identify the application, starting from the time the first packet is transferred.
- **WAN Path Controller**
  Being application aware opens the doors to intelligently prioritize the routing of applications across network bandwidth based on the specific application and user. Offering a per- application-level SLA, path-awareness intelligence dynamically selects the best WAN link/connection for the situation. FortiGate SD-WAN has the capability to provide granular WAN path-aware information, such as latency, jitter, and packet loss. Based on this awareness, multipath technology can automatically failover to the best available link when the primary WAN path degrades. All this automation is in-built and the end-user does not need to make any changes, which reduces complexity and improves the application performance. Gartner advises customers to "pilot SD-WAN solutions for branch offices to redress device complexity and/or high WAN transport or equipment costs."[6]
- **NGFW Security & Compliance**
  Fortinet's unique value is providing a secure SD-WAN solution by delivering high-class enterprise security with a single-box solution. Fortinet is the only SD-WAN vendor with an NSS Labs NGFW Recommendation. FortiGate SD-WAN offers the following features:
  - SSL inspection and threat protection to provide visibility and prevention against malware
  - Web filtering service to enforce internet security and reduce complexity, eliminating the need for a separate SWG device
  - Highly scalable and high-throughput IPsec VPN tunnels can be established to ensure that traffic is always encrypted and stays confidential.
  - Tracks real-time threat activity to facilitate risk assessment, detect potential issues, and mitigate problems. Firewall rules and policies are monitored to automate compliance audits.
- **Single-Pane-of-Glass and Zero-Touch Deployment**
  As enterprises adopt an SD-WAN solution, it's important to be able to seamlessly deploy the new technology and have the right tools to manage it. FortiGate SD-WAN can be administered

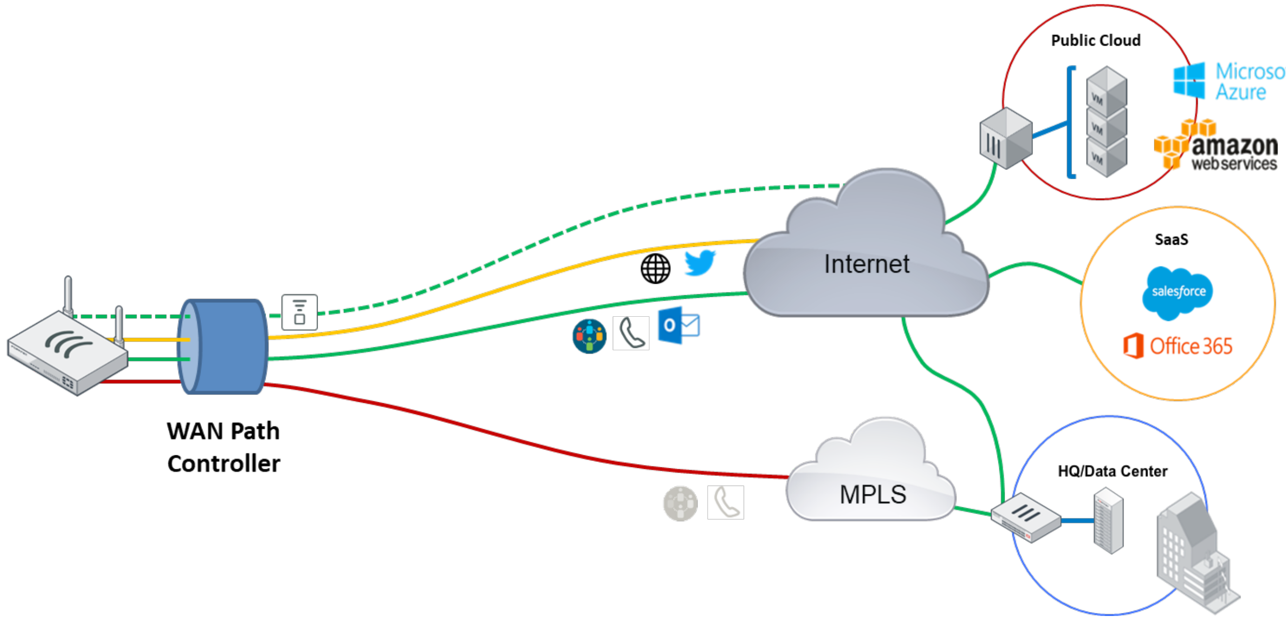
through a single intuitive and unified management console called the FortiManager. It includes options for a cloud-based or hosted solution for remote control and orchestration. This powerful management solution allows you to manage thousands of distributed locations in this way. FortiGate devices are true plug and play. Centralized policies and device information can be configured from the FortiManager, and the FortiGate devices will automatically be updated to the latest policy configuration.

- **Total Cost of Ownership**
  The move to public broadband means that expensive MPLS connections can be replaced with more cost-effective options. With Fortinet's transport-agnostic solution, enterprises can utilize the entire available bandwidth by using the connections in active-active mode. FortiGate SD-WAN includes best-of-breed security and SD-WAN functionality in a single appliance.

SUMMARY

The traditional WAN is no longer an effective solution for today's distributed enterprise. Organizations are overcoming significant security and network issues by moving to SD-WAN. There are many different SD-WANs on the market today, and VPs of IT should carefully review their options. Gartner recommends customers "avoid making strategic WAN decisions in a siloed, incremental fashion, solely within the networking group."[7]

FortiGate SD-WAN integrates enhanced SD-WAN features with proven security capabilities, delivering next-generation protection and networking capabilities that improve network efficiency without compromising security.



References:

[1,6,7] Gartner, "Market Guide for WAN Edge Infrastructure," Andrew Lerner and Neil Rickard, March 2017.

[2,3] Gartner, "Four Architectures to Secure SD-WAN," October 2017.

[4] Gartner, Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, and Rajpreet Kaur, July 2017.

Gartner Disclaimer
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[5] IDC Worldwide Security Appliances Tracker, April 2017 (based on annual unit shipments).

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

March 13, 2018 1:57 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:SB-SD-WAN:sb-fortinet-sd-wan