SOLUTION BRIEF

Solving WAN Edge Security and Performance Challenges for Distributed Organizations

The NTT Secure Edge Solution with Fortinet Offers Next-generation Security, Performance, and Agility

Introduction

Organizations rely on the wide-area network (WAN) for communication among their data centers, main offices, branch locations, remote workers, and the cloud. Maintaining information security, data availability, and application performance at the edge of the WAN can be a complicated and costly challenge for many organizations and is becoming increasingly difficult as the volume and nature of information, applications, and cloud usage continue to evolve. All aspects of an organization's operations are becoming digitized, putting tremendous demands on the security and performance of legacy WAN infrastructures.

The NTT Secure Edge Solution with Fortinet

The NTT Secure Edge solution with Fortinet provides organizations with enhanced security and data availability at the edge of the WAN, featuring robust failover and performance assurance capabilities, enforcement of centralized security policies across the entire WAN edge, internal segmentation at branch locations, and efficient and scalable virtual private network (VPN) connectivity. NTT offers the Secure Edge solution to clients in many different forms, from simple hardware and software deployments for a few sites, to highly complex and fully managed solutions for thousands of sites. Organizations that require a managed solution can rely on NTT's deep expertise and experience deploying Fortinet-based solutions for clients worldwide.

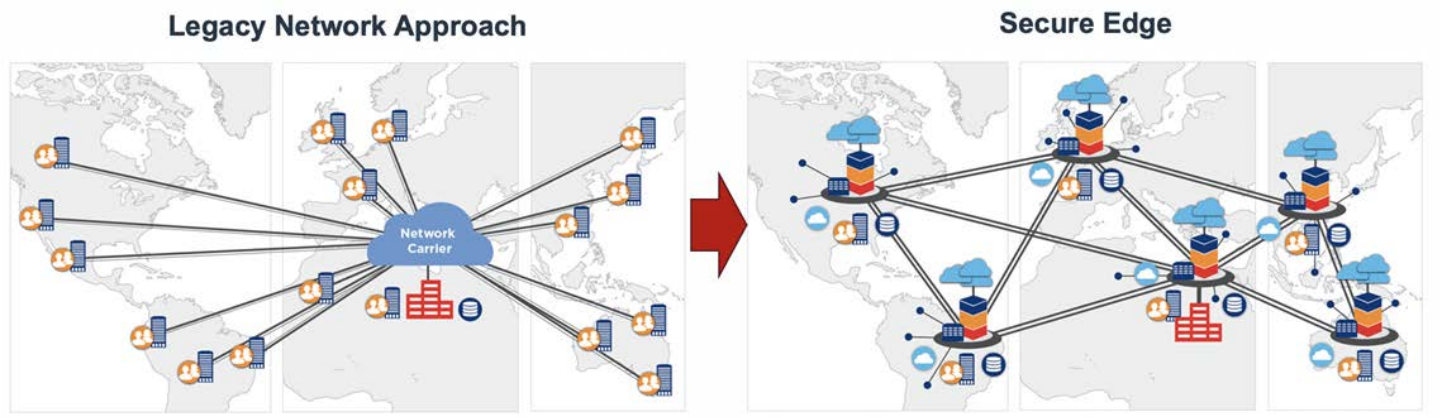
A Superior Solution To Address the Modern WAN Edge

The onset of digital transformation (DX) has introduced new technologies and solutions alongside lower-cost connectivity options for business, resulting in many organizations modernizing their legacy WANs. With more and more data becoming digitized, the emergence of the public cloud, including the adoption of Software-as-a-Service (SaaS) applications, necessitates a redesign of the WAN architecture, specifically the branch, edge network, and security architecture. Remote and branch locations at the edge of the WAN require secure and reliable high-speed connectivity for internet, voice, video, and data applications to ensure efficient operations.

Given dramatic increases in remote work and distributed workforce infrastructures, analysts predict that global business IP WAN bandwidth consumption will double in the near future.[1] Traditional WAN architectures use hub-and-spoke approaches that rely on inefficient legacy communication protocols and data backhauling to manage application traffic. These legacy WAN solutions typically employ the practice of backhauling branch and remote traffic through the data center to ensure edge security, which creates performance issues and can be ineffective due to direct internet connections at the edge, the limited visibility into SSL-encrypted traffic, and other factors.

The NTT Secure Edge solution with Fortinet features:

- Centralized security policy control
- Next-generation firewall (NGFW) feature set
- Intrusion prevention system (IPS), web filtering, anti-malware, and advanced threat detection (ATD)
- Secure sockets layer/ transport layer security (SSL/ TLS) inspection and internal segmentation
- Scalable auto Internet Protocol security (IPsec) VPN overlays
- Dynamic failover capabilities
- WAN path controller with application service-level agreement (SLA)
- Application awareness and acceleration



- Single exit point for security control
- Poor network performance based upon location
- Company data on-premises or in data center
- Network traffic backhauled to central location

- Global and consistent security controls
- Internet service distributed and commoditized
- Direct connects to cloud, Infrastructure-as-a-Service (IaaS), and SaaS distributed data
- Regional service provides optimized network performance

In many cases, backhauling can even increase security risks. Migrating data-center applications to multi-cloud environments such as AWS or Azure has increased these risks as users have more direct access to business-critical and sensitive information. Traditional WAN security and performance are being overwhelmed by these new demands. NTT Secure Edge with Fortinet addresses these new demands with comprehensive security, higher performance, and lower total cost of ownership (TCO).

NTT and Fortinet—A Global Partnership

NTT partners with Fortinet to provide best-in-class network security and WAN-edge performance to its clients. Rather than providing "point solutions," the Fortinet solution offers a holistic approach that integrates network edge security capabilities and centralized security policies that can be enforced via global rulesets. Fortinet is the only vendor with a custom-designed application-specific integrated circuit (ASIC) that provides the fastest application identification and steering in the industry, while ensuring faster connectivity and advanced security when compared to other solutions.

Gartner listed Fortinet as a leader in the 2020 WAN Edge Infrastructure Magic Quadrant and a leader in the 2020 Enterprise Network Firewall Magic Quadrant—the only vendor with a single device and a single management platform to be named a Leader in both, and what we view as a testament to Fortinet's vision of converged networking and security.[2,3] In addition, NSS Labs validated Fortinet as having an order of magnitude lower TCO when compared to other solutions.

The NTT Secure Edge solution integrates Fortinet capabilities natively into a single device that provides seamless, automated, and preemptive failover for your network and defined applications. Continuous health checks can be performed on FortiGate appliances, and if connectivity becomes an issue, failover can be initiated to another node before network performance is impacted. Policies can also be assigned to critical applications to prioritize connectivity.

Modernizing the WAN Edge Infrastructure

If your organization has one or more of the following characteristics, the NTT Secure Edge solution can help you mitigate security risks, improve performance, and lower costs associated with supporting a WAN-connected distributed workforce:

- Distributed workforce expansion (due to remote work, mergers, acquisitions, globalization, etc.)
- Distributed industrial/manufacturing sites
- Limited security staff and/or lack of resources to efficiently manage the integration of security and networking
- Escalating network edge cybersecurity threats and attacks
- Digital transformation, cloud migration, new services, and branch office expansion
- Requirements to simplify remote location setup and management
- Initiatives to reduce the cost and effort of supporting remote and branch locations
- Migrating away from costly traditional WAN infrastructures
- Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act of 2002 (SOX), State Civil Code, Revised Payment Service Directive (PSD2), and/or other compliance adherence

Conclusion

Global workforces have become more distributed and remote, which increases demands on network architectures and edge security requirements. Connecting more branch and other locations has escalated risks for security incidents, higher workloads, and budget overruns related to a lack of centralized management. User frustration can increase due to slower network performance, and valuable corporate assets may be compromised when employees access networks from less secure locations.

The NTT Secure Edge solution with Fortinet addresses these concerns while reducing or eliminating the need for expensive legacy architectures and protocols, enabling direct internet access to improve cloud-application performance, simplifying integration with NGFW, and offering network application awareness that dynamically selects optimal WAN routing.

The NTT Secure Edge solution helps ensure superior threat prevention, higher performance, lower complexity, and lower TCO for WAN environments. Secure Edge also delivers an application-aware automated WAN path controller with transparent visibility, superior network security, and simplified management that extends to the edge of the network and beyond.

NTT is a leading provider of security and networking services and solutions for global enterprises and organizations. NTT provides deep expertise and services to deliver the most secure and integrated solutions available for digital transformation and distributed workforces. Given NTT's proven experience, combined with extensive Fortinet Technical Professional Certifications, NTT can help your team create optimal infrastructures using Fortinet solutions. The NTT and Fortinet partnership offers a consistent level of service and support worldwide. NTT's proactive teams monitor and maintain security devices and networks through its five Global Service Centers using Information Technology Infrastructure Library (ITIL)-aligned Global Services Operating Architecture Service capabilities, which include 24x7 technical support, product education, and professional integration services.

For more information, contact NTT at:

Global headquarters:

4F Verde Building, 10 Bressenden Place, Victoria, London SW1E 5DH
Telephone:
+44 203 936 0400

NTT Ltd. North America
Security Operations Center
9420 Underwood Ave.
Omaha, Nebraska, 68114
United States

Website:

https://hello.global.ntt/en-us/solutions/intelligent-cybersecurity

Contact Information

References

[1] Michael Cooney, "Cisco predicts nearly 5 zettabytes of IP traffic per year by 2022," Network World, November 28, 2018.

[2] "Fortinet Named a Leader in the 2020 Gartner Magic Quadrant for WAN Edge Infrastructure," Fortinet, September 23, 2020.

[3] "ANALYST REPORT: 2020 Gartner Critical Capabilities for WAN Edge Infrastructure," Fortinet, September 30, 2020.

November 26, 2020 6:27 AM

845275-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\NTT-FTNT Secure Edge\sb-FA-solving-wan-edge-security-and-performance-challenges-11262020\sb-FA-solving-wan-edge-security-and-performance-challenges-11262020