SOLUTION BRIEF

Simplify Wired and Wireless Network Security with the Fortinet LAN Edge Solution

Executive Summary

The local-area network edge (LAN edge) is one of the most challenging vectors to secure. There are a multitude of different users and devices that connect, plus copious amounts of data, that all need to be protected. Add to that the growing number of inherently unsecure devices accessing the network as Internet-of-Things (IoT) deployments rise, and an enticing opportunity for attackers is created.

Securing the LAN edge is critical to the success of every network. To cut down complexity, while effectively delivering secure network access, a solution is needed that:

- Minimizes administration time
- Scales easily to handle increasing, expanding use, and different topologies
- Maximizes security capabilities

92% of U.S. survey respondents said attack volumes have increased in the past 12 months.[1]

Part of the Fortinet Security Fabric, the Fortinet LAN Edge solution offers built-in security, end-to-end network visibility, integrated detection, and automated threat response.

Top Protection and Simplified Management

Fortinet Security-Driven Networking enables our LAN Edge solution—centered on our FortiGate next-generation firewall (NGFW)—to integrate directly with our wireless access points (APs) and wired switches. This consolidation of security and network access offers a number of game-changing benefits. With a common security operating system, FortiOS, and a single source of threat intelligence, FortiGuard, the LAN Edge solution eliminates both the complexity and the protection shortcomings that occur when mixing different security and networking vendors. Enabling the entire ecosystem to behave as a single entity from a policy and logging perspective reduces the risk from advanced threats. Furthermore, security services can be fine-tuned in accordance with any organization's security posture.

Integration of network and security functions is achieved through FortiLink and offers a superior solution for the internal segmentation of Ethernet and wireless. Users and devices can be segmented based on roles and devices types. FortiLink is included, unlicensed and without charge in the majority of FortiGate models. This differs from the majority of network access vendors that require additional software and management consoles to achieve such integration, increasing complexity and cost, often through recurring fees.

In addition, Fortinet provides a family of management and analytics tools to vigilantly monitor user and network activity as well as generate reports to meet internal and regulatory compliance requirements. Authentication solutions support single login, social login, and captive portal authentication options. Analytics provides network security logging, analysis, and reporting to interpret and visualize network threats, inefficiencies, and bandwidth usage. Centralized policy management, analytics, and reporting reduce management costs and deployment time, plus simplify configuration.

Flexibility and Scalability To Fit Every Location

FortiGate NGFWs are available in a large range of configurations and multiple form factors, offering the right level of protection and performance for any site in the network. FortiGate enterprise firewalls fit at remote locations, campus edges, and data centers. They can be deployed as a hardware appliance, virtual machine, or in the cloud. A FortiGate deployed in the cloud or data center can protect teleworkers in their home offices.

Securing the campus

IT teams commonly experience difficulty deploying, managing, and securing the dynamic, complex, multilayered LANs in today's campus settings. These challenges are due to both size and composition as products from multiple vendors are often installed. Without a common framework, networks often feature disparate security solutions "bolted on" rather than integrated, creating both deployment and management challenges.

Through Security-Driven Networking, our LAN Edge solution reduces campus LAN complexity by centralizing LAN management and security functions within the FortiGate. Through FortiLink, the FortiGate is the centralized controller of both security and the network access layer, tying the access layer into the automated Fortinet Security Fabric and enabling Security-Driven Networking. FortiLink integration of

access-layer management into the FortiGate enables single-pane-of-glass management of both network and security functions. Integration of wired and wireless configuration and management with the FortiGate means there is only one operating system to support and manage, and only one configuration for both network access functions and security functions. This simplifies moves, adds, and changes, troubleshooting, policy changes, and day-to-day operations. It reduces the chance for error and enables simplified management of alerts and health of both network and security functions.

Securing branch offices

Branch office networks have evolved as digital transformation has driven new business requirements and architectures that leverage the latest technologies and innovations. IT organizations need to enable multi-cloud architectures, speed access to Software-as-a-Service (SaaS) applications, and securely network bring-your-own-device (BYOD) and IoT devices. Adapting the network to these innovations also creates new network edges that need to be secured.

As distributed organizations re-examine branch operations, they expect better integration of LAN and wide-area network (WAN) platforms. The Fortinet SD-Branch solution, based on LAN-edge equipment, extends the features of SD-WAN to the enterprise branch network. Fortinet Secure SD-WAN technology is integrated with network access to deliver the most secure and manageable remote branch in the industry. To address the explosion of IoT devices, Fortinet Secure SD-Branch further utilizes FortiGate as a network sensor with additional onboard network access control (NAC) features, enabling administrators to discover and secure IoT devices.

SD-Branch is powered by FortiLink, which includes a common management platform and integrated security, enabling wired Ethernet switch and wireless WLAN interfaces to be controlled with the same level of enforcement as firewall interfaces. FortiLink switch and wireless integration requires no license. It is included as part of the FortiOS running on every FortiGate.

Convergence of both wired and wireless networking within FortiGate extends the capabilities of a secure SD-WAN solution to the branch access layer—combining NGFW security, switches, extenders, and APs in one interoperable solution. This integration reduces infrastructure complexity by simplifying branch management of security, network access, and SD-WAN. It eliminates multiple vendors, interfaces, and operating systems, which can burden limited staff, while erasing defensive gaps along the seams between different solutions. SD-Branch increases agility through a single-pane-of-glass interface, which improves branch visibility and control. It also supports zero-touch deployment for improved total cost of ownership (TCO).

[1] "VMware Releases Cybersecurity Threat Survey Report Detailing Increased Attack Volume and Breach Levels in the United States," VMware, July 14, 2020.

Securing the teleworker remote office

While working remotely is not new, the global shift from a generally minimal remote workforce to a fully remote workforce is. Numerous surveys have found that firms will continue to employ more teleworkers than previously, even after the 2020 pandemic is over. This means investment in telework security is key for now and the future.

Fortinet provides a complete solution for securely supporting a remote workforce. The Fortinet remote AP solution set is robust. It is based upon FortiAP hardware that is managed by a FortiGate on the corporate network. Extending the Fortinet Security Fabric into a remote worker's home ensures network security by protecting teleworkers from even the latest cyber threats. FortiGate NGFWs can manage both local and remote APs. Wireless service set identifier (SSID) traffic receives the same level of inspection and security as a firewall port and becomes an integrated piece of an organization's overall security profile. The Fortinet Security Fabric is extended to the teleworker's home office via the FortiAP wireless access point, as well as any switched ports on that AP.

Our FortiDeploy option (part of the FortiCloud suite of products) makes installation of a remote AP simple. Once the FortiAP acquires an IP address and has internet connectivity, it will check in with the FortiDeploy system to learn which FortiGate it should connect to for management. All that IT needs to do within the FortiDeploy interface is set the IP address of the intended FortiGate being used for wireless management for each FortiAP. The user does not need to know this information or perform any manual configuration steps. The FortiGate can be configured to auto-adopt and push configuration to discovered FortiAPs. Once a FortiAP contacts it, it will install the correct corporate image onto the AP, and the AP will start beaconing the corporate SSID.

Summary

Fortinet Security-Driven Networking enables organizations to comprehensively secure the LAN edge as part of a larger ecosystem while maintaining the same level of services and protection throughout. With the flexibility to choose deployment style, the solution can be adapted to a company's security posture so that the balance between security and openness is maintained.

Our LAN Edge solution integrates into the Fortinet Security Fabric, which is visible and controllable from a single pane of glass. Every element of the Fortinet Security Fabric communicates with each of the other pieces, automating workflows and threat-intelligence sharing. This minimizes the amount of time overstretched security teams spend on manual processes while shaving threat, intrusion, and breach responses.

FORTINET

www.fortinet.com

September 4, 2020 11:12 PM

766366-0-0-EN

D:\Fortinet\Solution Brief\Red Solution Brief\FortiLink Launch\sb-FA-simplify-wired-and-wireless-network-security-922020