SOLUTION BRIEF

Strengthen and 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, creating an enticing opportunity for attackers.

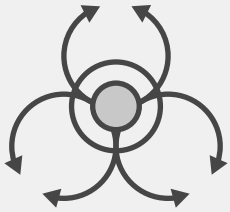
Securing the LAN edge is critical to the success of every network. To cut down complexity while effectively delivering secure network access, a solution is needed that:

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

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

62%

62% of organizations' attack surfaces increased over the past two years.[1]



Top Protection and Simplified Management

Fortinet Secure Networking with FortiLink technology is centered on the FortiGate Next-Generation Firewall (NGFW). This convergence of network access and security enables our LAN edge solutions to integrate directly with our wireless access points (APs) and wired switches. With a common security operating system, FortiOS, and a single source of threat intelligence, FortiGuard Labs, 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, FortiGuard AI-Powered Security Services can be fine-tuned to any organization's security posture.

Integration of network and security functions is achieved through FortiLink, which offers a superior solution for the internal segmentation of Ethernet and wireless. Users and devices can be segmented based on roles and device types. FortiLink is included, unlicensed, and free of 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. FortiLink technology allows network access control (NAC) features to be built into the solution at no extra cost to the user.

In addition, Fortinet provides a family of management and analytics tools to vigilantly monitor user and network activity as well as generate reports to satisfy 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, as a virtual machine, or in the cloud. A FortiGate deployed in the cloud or data center can protect remote workers 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 size and composition, as products from multiple vendors are often installed. Without a common framework, the disparate security solutions are "bolted on" rather than integrated, creating deployment and management challenges.

Through secure 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 security and the network access layer, tying the access layer into the automated Fortinet Security Fabric and enabling secure connectivity.

FortiLink integration of access-layer management into the FortiGate enables single-pane-of-glass management of 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 network access 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 alert management and health of 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 applications, and securely network bring-your-own-device 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 industry's most secure and manageable remote branch. To address the explosion of IoT devices, Fortinet Secure SD-Branch uses FortiGate as a network sensor with additional onboard 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 wired and wireless networking within FortiGate extends the capabilities of a secure SD-WAN solution to the branch access layer, combining NGFW security, switches, 5G/LTE WAN gateways, 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).

Securing the remote office

While working remotely is not new, the global shift from a generally minimal remote workforce to a fully remote workforce and then to a hybrid workforce is. 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 remote workers from even the latest cyberthreats. 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 home office via the FortiAP wireless access point and 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 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 Secure Networking enables organizations to comprehensively secure the Fortinet 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 to maintain the balance between security and openness.

Our LAN edge solution is visible and controllable from a single pane of glass and integrated with the Fortinet Security Fabric. 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 improving threat, intrusion, and breach response time.

[1] Jon Oltsik, Why companies need attack surface management in 2024, Tech Target, February 20, 2024.

July 22, 2024 1:05 PM / 766366-C-0-EN