SOLUTION BRIEF

FortiAP Access Points Provide Secure, Painless Connectivity for Remote Workers

Executive Summary

The ability to support remote workers is essential for an organization's business continuity plan. Additionally, the ability to work remotely has a significant impact on employee productivity and retention.

A crucial component of supporting a remote workforce is the ability to guarantee secure connectivity between remote work sites and the corporate network. FortiAP remote access points (APs) provide this secure connection in an intuitive solution that requires minimal configuration by remote users or on-site IT staff.

80% of employees want to work from home at least part-time.[2]

37% of employees would change jobs for the opportunity to telework at least part-time.[3]

Introduction

Over three-quarters of employees want the option to work from home at least part-time.[1] The ability to support a remote work program can help an organization retain employees and is a crucial component of a business continuity plan.

While not every remote worker needs a full corporate environment to do their jobs, some do. For these power users, native access to the corporate network directly in their home workspace saves time and energy and increases productivity. Fortinet remote FortiAP access points provide a simple and effective extension of the corporate environment, and the Fortinet Security Fabric, to a remote worker's home.

Components of a Remote AP Solution

Many organizations have certain, basic requirements for remote APs. These include the ability to manage the AP from the corporate headquarters, rather than the employee's residence, and to securely transmit traffic to and from the corporate network. However, additional factors exist that can impact the effectiveness of a remote AP solution.

Simplified setup

While some home workers may be IT professionals, the majority are not. A remote AP must be simple and straightforward to set up, ideally "plug and play" for the user. It should also include the flexibility to be powered either by Power over Ethernet (PoE) or by a standard DC power supply.

The same need for simplicity also applies to the IT side of the equation. IT should be able to "set it and forget it" for these APs. This includes the knowledge that the APs' controller is prepared to push configurations and perform remote device management at time of use rather than requiring additional coordination and setup during installation.

Access point options

A variety of APs should be available, enabling a choice of desktop, wall-mounted, or ceiling-mounted APs depending on the size of the remote site and preferences of the worker. When applicable, additional wired ports that provide access to the same secure tunnel to the corporate network are a plus.

The same network

From the teleworker's point of view, the corporate network at their home and the corporate network in the office should look and behave the same. Separate service set identifiers (SSIDs) or one-off security settings only confuse users and create additional work for IT staff handling support calls from teleworkers.

Traffic bridging

Not everything that the worker needs to do will be destined for the corporate network. Routing this non-corporate traffic to the wireless controller before sending it to its destination only creates additional latency.

With the rise of Software as a Service (SaaS)-based applications, as well as local resources such as printers and other machines in the home office, a significant percentage of traffic does not need to be routed through to the corporate environment. The ability to control what traffic is routed where will

increase the overall quality of experience (QoE) for the user, while keeping the corporate network connection free of spurious traffic.

Fortinet Solution

Fortinet provides a complete solution for supporting a remote workforce. The Fortinet remote AP solution set offers a robust solution based upon FortiAP hardware managed by a FortiGate installed on the corporate network. Extending the Fortinet Security Fabric into a remote worker's home ensures network security by protecting teleworkers from the latest cyber threats.

Fortinet APs

Fortinet offers a wide selection of FortiAP wireless access points designed to meet every use case. The wallplate series of APs offers a mount stand to convert them into simple desk mount models. Extra switched wired ports on these APs provide teleworkers with the option to directly connect multiple devices to the AP. Alternatively, standard APs are available for ceiling and wall mount.

Fortinet also offers access points that can provide security services on the AP before traffic reaches the wired network. These APs leverage threat intelligence provided by FortiGuard Labs services to support onboard unified threat management (UTM) services.

FortiGate as a wireless controller

FortiGate next-generation firewalls (NGFWs) can manage both local and remote APs. Wireless 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 out to the teleworker's home office via the FortiAP wireless access point, as well as any switched ports on that AP.

Secure SSIDs

Corporate SSIDs appear the same to a teleworker as they do in the office. With all incoming and outgoing traffic traversing the FortiGate NGFW, the company can feel assured that the internal network is properly protected from traffic originating off-site.

Fortinet Features for Remote APs:

- Same user experience for on-site and remote workers
- High-availability (HA) failover configurations for the FortiGate NGFWs ensure the network is always available
- Split-tunnel options allow local or internet traffic to be routed at the AP rather than passing through the corporate network
- Simple "zero-touch" deployment for the user, simplified large-scale setup for the IT manager
- FortiGuard services at the edge, with APs capable of UTM services
- Simple to configure and deploy with no licenses required on the FortiGate
- Full visibility and auditability with security reporting on the FortiGate
- WAN connectivity options with FortiExtender

For the user, they can connect to and use the network in the same way they would when they are in the office. Multiple options are available for establishing the secure connection between the AP and the controlling FortiGate, including Internet Protocol security (IPsec).

Zero touch with FortiDeploy

Fortinet's 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 any and all FortiAPs. The user never needs 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.

Local bridging

Fortinet split-tunnel architecture allows traffic that does not need to be sent back to the controlling FortiGate to be bridged and routed directly at the AP. FortiGate traffic inspection is only performed on traffic that requires it based upon business needs, and not every packet.

Network Resiliency

FortiGate NGFWs can be configured in a HA configuration to ensure that a single point of failure does not remove access to corporate resources. Additionally, should all connectivity back to the FortiGates be lost, the FortiAP will continue to operate and route any locally bridged traffic until connection to the FortiGate is restored.

Conclusion

Working from home is likely to continue to grow in popularity, but it does not need to create challenges for IT staff. Workers who require repeated access to resources on the corporate network can benefit from having direct, immediate access in their residences via a company wireless AP.

Fortinet enables easy teleworker support via the FortiAP wireless access point. When managed remotely by the FortiGate, the FortiAP can offer secure corporate network access without any required knowledge or configuration by the remote worker, enabling IT to support remote workers without a large support overhead.

[1] "2019 State of Remote Work Report," Owl Labs, September 2019.

[2] "2019 State of Remote Work Report," Owl Labs, September 2019.

[3] "State of the American Workplace Report," Gallup, April 2017.

April 16, 2020 4:19 AM

636674-0-0-EN

D:\Fortinet\Solution Briefs\red solution briefs\Remote AP - Teleworker Asset\sb-FA-fortiap-access-provides-secure-painless-connectivity-for-remote-workers-4162020