SOLUTION BRIEF

Secure Remote Access for Your Workforce at Scale

Executive Summary

Organizations face a number of different potential emergency situations, such as illness, flood, hurricanes, and power outages. Implementing a business continuity plan is essential to ensuring that the organization is capable of maintaining operations in the face of adversity and preparing for potential disasters.

An important consideration for organizations developing a business continuity plan is that the organization may not be capable of sustaining normal operations onsite. The ability to support employees working remotely is essential to ensuring both business continuity and security. Fortinet solutions offer an integrated solution to support telework. FortiGate next-generation firewalls (NGFWs) have built-in support for IPsec virtual private networks (VPNs), enabling remote workers to connect securely to the company network. With endpoint protection, provided by FortiClient, and multi-factor authentication (MFA) with FortiAuthenticator, organizations can securely support remote work and maintain business continuity.

The ability to securely support a remote workforce is an essential component of any organization's business continuity and disaster recovery plan. An organization may be incapable of sustaining normal operations onsite, due to a power outage or similar event, or illness or flooding may make it unsafe for employees to travel onsite.

In these scenarios, an organization must be capable of supporting secure, remote connectivity to the corporate network. For over 400,000 Fortinet customers, their existing technology deployment already contains this functionality. FortiGate NGFWs have integrated support for IPsec VPNs, enabling secure connectivity for employees working from alternate work sites.

Remote work decreases employee unproductive time by an average of 27%.[1]

Remote employees work an average of 16.8 more days per year than onsite employees.[2]

85% of employees claim that they reach maximum productivity when working remotely.[3]

Allowing remote work increased employee retention in 95% of organizations.[4]

Securing the Remote Workforce with FortiGate NGFWs

The IPsec and SSL VPNs integrated into every FortiGate NGFW offer an extremely flexible deployment model. Remote workers can either take advantage of a clientless experience or gain access to additional features through a thick client built into the FortiClient endpoint security solution. Power users and super users would benefit from deploying a FortiAP or a FortiGate NGFW for additional capabilities.

Fortinet solutions are designed to be easy to use from initial purchase through end of life. FortiGate NGFWs and FortiAP wireless access points include zero-touch deployment functionality. Appliances deployed at remote sites can be pre-configured before they ship, allowing for automatic set up onsite, which ensures business continuity and support for telework.

The Fortinet Security Fabric takes advantage of a common Fortinet operating system and an open application programming interface (API) environment to create a broad, integrated, and automated security architecture. With the Fortinet Security Fabric, all of an organization's devices, including those deployed remotely to support telework, can be monitored and managed from a single pane of glass. From a FortiGate NGFW or a FortiManager centralized management platform deployed at the headquarters environment, the security team can achieve full visibility into all connected devices, regardless of their deployment situation.

In the event of a natural disaster or other event that disrupts normal business operations, an organization must be capable of rapidly transitioning to a fully remote workforce. Table 1 shows the number of concurrent VPN users that each model of the FortiGate NGFW can support.

Beyond offering encryption of data in transit, via a VPN, Fortinet solutions offer a number of other features that can help an organization to secure its remote workforce. These features include:

- **Multifactor authentication.** FortiToken and FortiAuthenticator enable dual factor authentication of remote employees.
- **Data loss prevention (DLP).** FortiGate and FortiWiFi provide DLP functionality for remote workers, which is essential for teleworking executives with frequent access to sensitive company data.
- **Advanced threat protection.** FortiSandbox offers analysis of malware and other suspicious content within a sandboxed environment before it reaches its destination.
- **Wireless connectivity.** FortiAPs provide secure wireless access at remote work locations with full integration and configuration management in a single pane of glass.
- **Telephony.** FortiFone is a secure, voice over IP (VoIP) telephony solution, whose traffic is secured, managed, and monitored by a FortiGate NGFW. Available in soft client and several hardware options.

Model	Concurrent SSL VPN Users	Concurrent IPsec VPN Users	Managed FortiAPs (Tunnel Mode)
100E	500	10,000	32
100F	500	16,000	64
300E	5,000	50,000	256
500E	10,000	50,000	256
600E	10,000	50,000	512
1100E	10,000	100,000	2,048
2000E	30,000	100,000	2,048
All Larger Models*	30,000	100,000	2,048
*3300E supports 1,024 Tunnel Mode APs			

Table 1: Number of concurrent VPN connections supported by various models of FortiGate NGFWs.

Use Cases for Fortinet Products Supporting Remote Work

Not every employee in an organization requires the same level of access to company resources when working remotely. Fortinet provides tailored telework solutions for every remote worker:

1. **Basic teleworker.** The basic teleworker only requires access to email, internet, teleconferencing, limited file sharing, and function-specific capabilities (finance, HR, etc.) from their remote work site. This includes access to Software-as-a-Service (SaaS) applications in the cloud, such as Microsoft Office 365, as well as a secure connection to the corporate network.

   Basic teleworkers can connect to the organization using FortiClient integrated VPN client software and verify their identity with FortiToken for multifactor authentication. Note that power users and super users would revert to the basic teleworker profile when they roam from their remote work location.

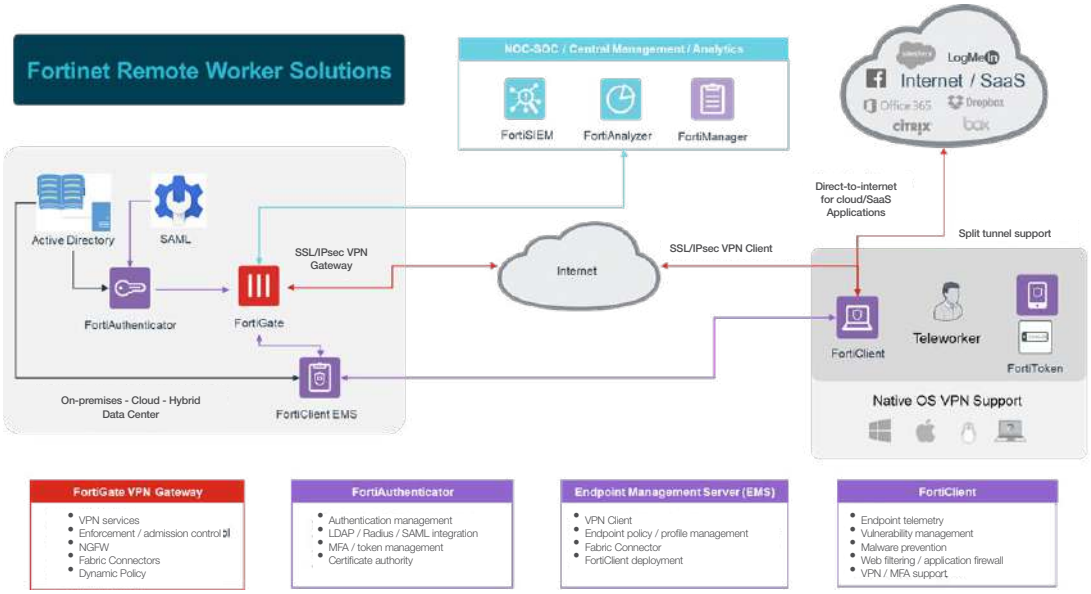

Figure 1: Notional Fortinet solution deployment for basic teleworker.

2. **Power user.** Power users are employees that require a higher level of access to corporate resources while working from a remote location. This may include the ability to operate in multiple, parallel IT environments and includes employees such as system administrators, IT support technicians, and emergency personnel.

   For these power users, deployment of a FortiAP access point at their alternate work site provides the level of access and security that they require. This enables secure wireless connectivity with a secure tunnel to the corporate network. FortiAPs can be deployed with zero-touch provisioning (ZTP) and will be managed by the FortiGate NGFWs in the office. Should a corporate phone need to be deployed, it can simply plug into the FortiAP for connectivity back to the main office.

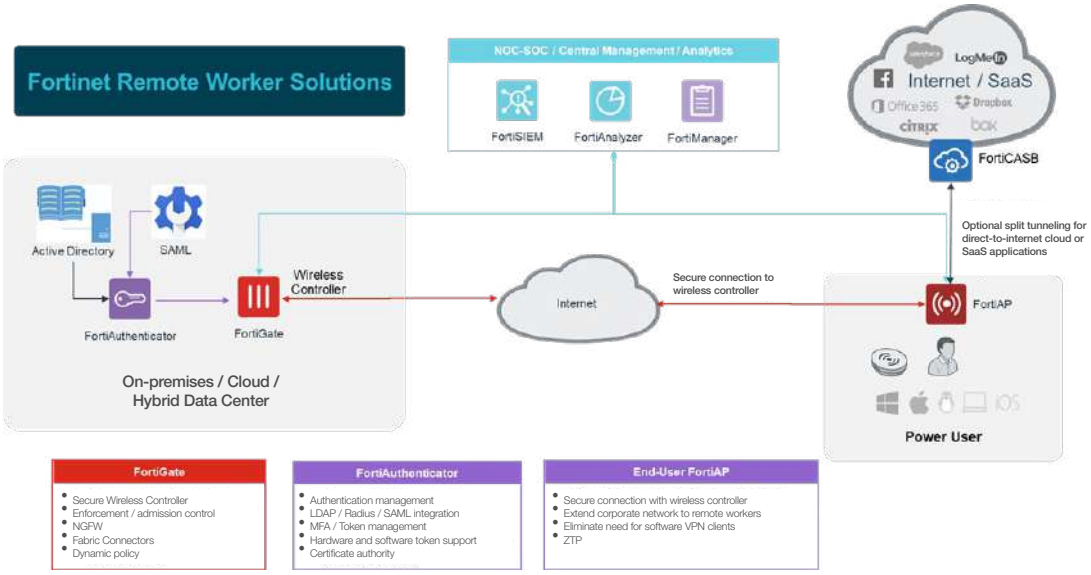

Figure 2: Notional Fortinet solution deployment for power user.

3. **Super user.** A super user is an employee that requires advanced access to confidential corporate resources, even when working from an alternate office location. They frequently processe extremely sensitive and confidential information. This employee profile includes administrators with privileged system access, support technicians, key partners aligned to the continuity plan, emergency personnel, and executive management.

   For these super users, their alternate work site should be configured as an alternate office location. While they require the same solutions as basic telecommuters and power users, they also require additional functionality. FortiAP can be integrated with a FortiGate NGFW or FortiWiFi appliance for secure wireless connectivity with built-in DLP. FortiFone provides soft client or hardware versions of telephony VoIP that is managed and secured via onsite FortiGate NGFWs or a FortiManager centralized management platform deployed at the headquarters location.

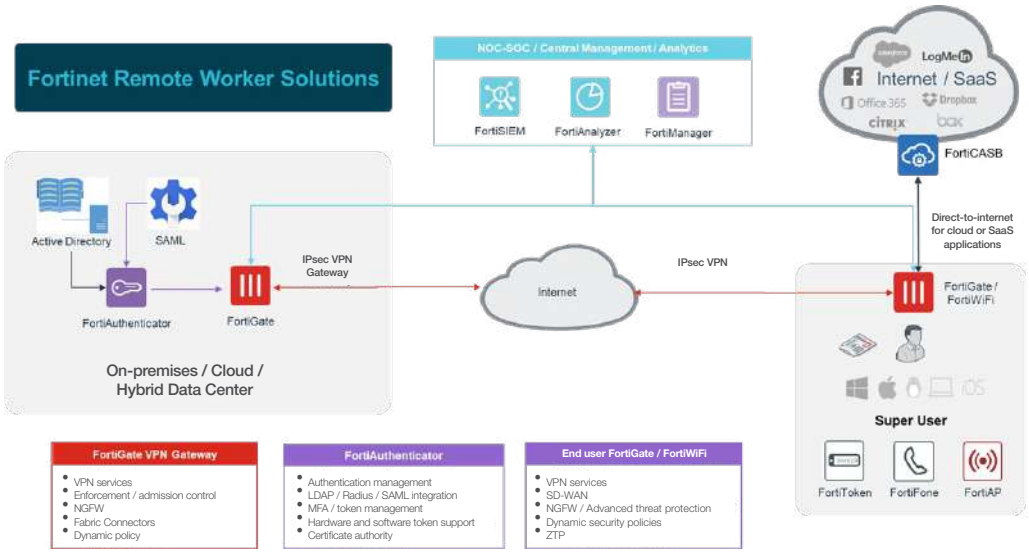

Figure 3: Notional Fortinet solution deployment for super user.

Supporting a Remote Workforce

Fortinet solutions are easily deployed to remote work locations. However, an organization also requires resources onsite or in the cloud to securely support teleworkers.

Many organizations already have these resources in place as they are part of their existing security architecture. A FortiGate NGFW provides a NGFW capable of inspecting encrypted and plaintext traffic at enterprise scale with minimal performance impacts. However, it also includes an integrated VPN gateway that acts as an endpoint for encrypted connections to teleworkers.

The FortiGate NGFW also includes integration with common IT infrastructure, including corporate director services, such as Microsoft Active Directory (AD), and MFA and single sign-on (SSO) solutions. FortiAuthenticator provides a single, centralized integration point for authentication solutions and supports third-party solutions as well as FortiToken, which offers hard, soft, email, and mobile token options.

When managing a remote and distributed workforce, centralized security visibility and management are essential. All Fortinet solutions can be integrated via the Fortinet Security Fabric. This enables the organization's security team to achieve single-pane-of-glass visibility and control using FortiManager, perform log aggregation and security analytics with FortiAnalyzer, and rapidly detect and respond to potential threats using FortiSIEM.

Achieve Full Security Integration with Fortinet Solutions

The Fortinet Security Fabric enables seamless integration of an organization's remote workforce. All Fortinet solutions are connected via the Fortinet Security Fabric, enabling single-pane-of-glass visibility, configuration, and monitoring. A number of Fabric Connectors, an open API environment, DevOps community support, and a large extended Security Fabric ecosystem enable integration with over 250 third-party solutions as well.

This is essential when an organization is preparing a business continuity plan, since the company may be forced to transition over to a fully remote workforce with little or no notice. Single-pane-of-glass visibility and management of an organization's security architecture ensures that support for telecommuting does not jeopardize an organization's cybersecurity.

The following solutions are part of the Fortinet Security Fabric and support secure telework:

- **FortiClient.** FortiClient strengthens endpoint security through integrated visibility, control, and proactive defense and enables organizations to discover, monitor, and assess endpoint risks in real time.
- **FortiGate.** FortiGate NGFWs utilize purpose-built cybersecurity processors to deliver top-rated protection, end-to-end visibility and centralized control, as well as high-performance inspection of clear-texted and encrypted traffic.
- **FortiWiFi.** FortiWiFi wireless gateways combine the security benefits of FortiGate NGFWs with a wireless access point, providing an integrated network and security solution for teleworkers.
- **FortiFone.** FortiFone provides unified voice communications with VoIP connectivity that is secured and managed via FortiGate NGFWs. The FortiFone soft client interface allows users to make or receive calls, access voicemail, check call history, and search the organization's directory right from a mobile device. Multiple hardware options are available.
- **FortiToken.** FortiToken confirms the identity of users by adding a second factor to the authentication process through physical or mobile application based tokens.
- **FortiAuthenticator.** FortiAuthenticator provides centralized authentication services including SSO services, certificate management, and guest management.
- **FortiAP.** FortiAP delivers secure, wireless access to distributed enterprises and remote workers and can be easily managed from a FortiGate NGFW or via the cloud.
- **FortiManager.** FortiManager provides single-pane-of-glass management and policy controls across the extended enterprise for insight into networkwide, traffic-based threats. This includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices.

- **FortiAnalyzer.** FortiAnalyzer provides analytics-powered cybersecurity and log management to enable improved threat detection and breach prevention.
- **FortiSandbox.** Fortinet sandboxing solutions offer a powerful combination of advanced detection, automated mitigation, actionable insight, and flexible deployment to stop targeted attacks and subsequent data loss. Available as a cloud service that is included in most FortiGuard subscriptions.

A Secure Foundation Ensures Business Continuity

Preparing for business continuity and disaster recovery is vital for any organization. An important component of this is the ability to support a mostly or fully remote workforce with little or no notice.

When developing business continuity plans, it is essential to ensure that the organization has the resources in place to secure this remote workforce. Fortinet solutions are easily deployable and configurable and enable an organization to maintain full security, visibility, and control regardless of their deployment environment.

1 "The Benefits of Working From Home," Airtasker, September 9, 2019.

2 Ibid.

3 Abdullahi Muhammed, "Here's Why Remote Workers Are More Productive Than In-House Teams," Forbes, May 21, 2019.

4 Ibid.

March 12, 2020 10:11 AM

618770-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\FortiWork@Home\sb-secure-remote-access-for-your-workforce-at-scale-V1-3122020-1008AM