SOLUTION BRIEF

Secure Remote Access for Your Government Workforce at Scale

Executive Summary

Governments face a number of different potential emergency situations, such as illness, flood, hurricanes, and power outages. Governments must function as the management and coordination point in the face of adversity by communicating with citizens through openness and transparency. Implementing a business continuity plan is essential to ensuring government is capable of maintaining operations in the face of adversity and preparing for potential disasters. We have entered a new era where government workers can be required to work remotely.

An important consideration in developing a business continuity plan is that it may not be possible to sustain 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 at scale. FortiGate next-generation firewalls (NGFWs) have built-in support for SSL and IPsec virtual private networks (VPNs), enabling remote workers to connect securely to the government network without any extra licensing. With endpoint protection, provided by FortiClient, and multi-factor authentication (MFA) with FortiAuthenticator, governments can securely support remote work and maintain business continuity.

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

In these scenarios, government must be capable of supporting secure, remote connectivity to the network. For over 400,000 Fortinet customers, their existing technology deployment already contains this functionality. FortiGate next-generation firewalls (NGFWs) have integrated support for SSL and IPsec VPNs, enabling secure connectivity for employees working from alternate work sites.

Securing the Remote Government Workforce with FortiGate NGFWs

Fortinet solutions are designed to be easy to use and maintain. FortiGate NGFWs include zero-touch deployment functionality to ensure business continuity and support for telework. This enables appliances to be rapidly deployed at remote sites with minimal preconfiguration, and to automatically retrieve their configuration settings over secure connections and complete setup once they are connected onsite.

The VPN integrated into every FortiGate NGFW offers 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. Government power users and executive users would benefit from deploying a FortiAP or a FortiGate NGFW for additional capabilities.

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 and users, 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:

- **Multi-factor authentication (MFA).** 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.
- **Endpoint security.** FortiEDR provides advanced threat protection for remote workers' computers including automated remediation.
- **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.
- **Device access management.** FortiNAC is able to enforce bring-your-own-device (BYOD) policies even over remote VPN connections, allowing the organization to control what types of devices can connect and what access they receive.
- **Telephony.** FortiFone is a secure, Voice-over-IP (VoIP) telephony solution, whose traffic is secured, managed, and monitored by a FortiGate NGFW. It is 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			

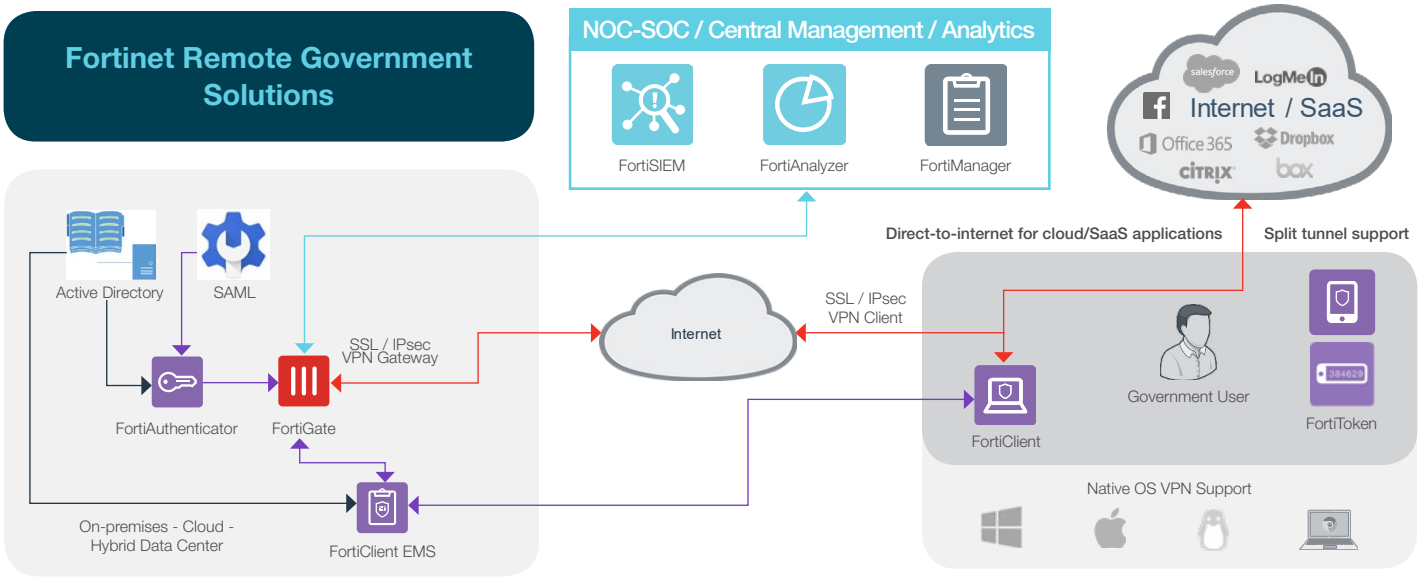
Table 1: Number of concurrent VPN connections supported by various models of FortiGate NGFWs.

Use Cases for Fortinet Products Supporting Remote Government Work

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

1. **Standard government worker.** The majority of these workers require access to email, internet, teleconferencing, limited file sharing, and function-specific capabilities (HR, etc.) from their remote work site. This includes access to Software-as-a-Service (SaaS) services in the cloud, such as Microsoft Office 365, as well as a secure connection to the government network.

   They connect using FortiClient integrated VPN client software and verify their identity with FortiToken for MFA.



FortiGate VPN Gateway	FortiAuthenticator	Endpoint Management Server (EMS)	FortiClient
• VPN services • Enforcement / admission control • NGFW • Fabric connectors • Zero-trust policy enforcement	• Authentication management • LDAP / RADIUS / SAML integration • MFA / token management • Certificate authority • Zero-trust user / device authentication	• VPN client configuration • Endpoint policy / profile management • Fabric connector • FortiClient deployment • Zero-trust agent configurator	• Vulnerability management • Malware prevention • Web filtering / application firewall • VPN / MFA support • Zero-trust agent

Figure 1: Fortinet solution deployment for standard government worker.

2. **Government power user.** Power users are government employees who require a higher level of access to government 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 persistent, secure tunnel to the government network. FortiAPs can be deployed with zero-touch provisioning (ZTP) and will be managed by the FortiGate NGFWs in the office. Should a government phone need to be deployed, it can simply plug into the FortiAP for connectivity back to the agency office.

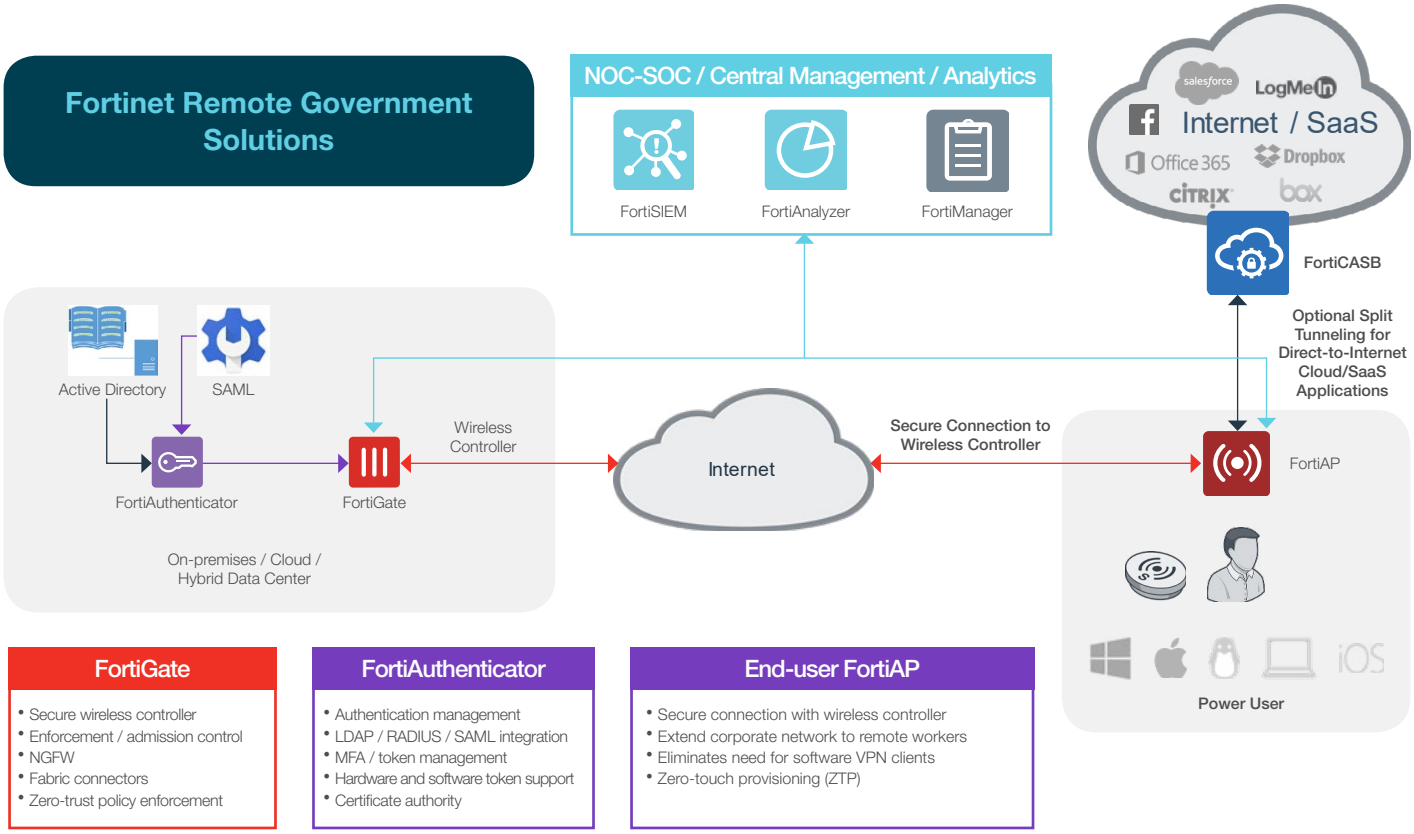


Figure 2: Fortinet solution deployment for government power user.

3. **Government super user.** A super user is an employee who requires advanced access to sensitive government resources, even when working from an alternate office location. They frequently process extremely sensitive and confidential information. This employee profile includes administrators with privileged system access, support technicians, key government partners and organizations aligned to the continuity plan, emergency personnel, government executives such as agency heads, governors, and mayors and their staffs.

   For these super users, their alternate work site should be configured as an alternate office location. While they require the same solutions as standard government workers 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 via VoIP that is managed and secured via onsite FortiGate NGFWs or a FortiManager centralized management platform deployed at the office location.

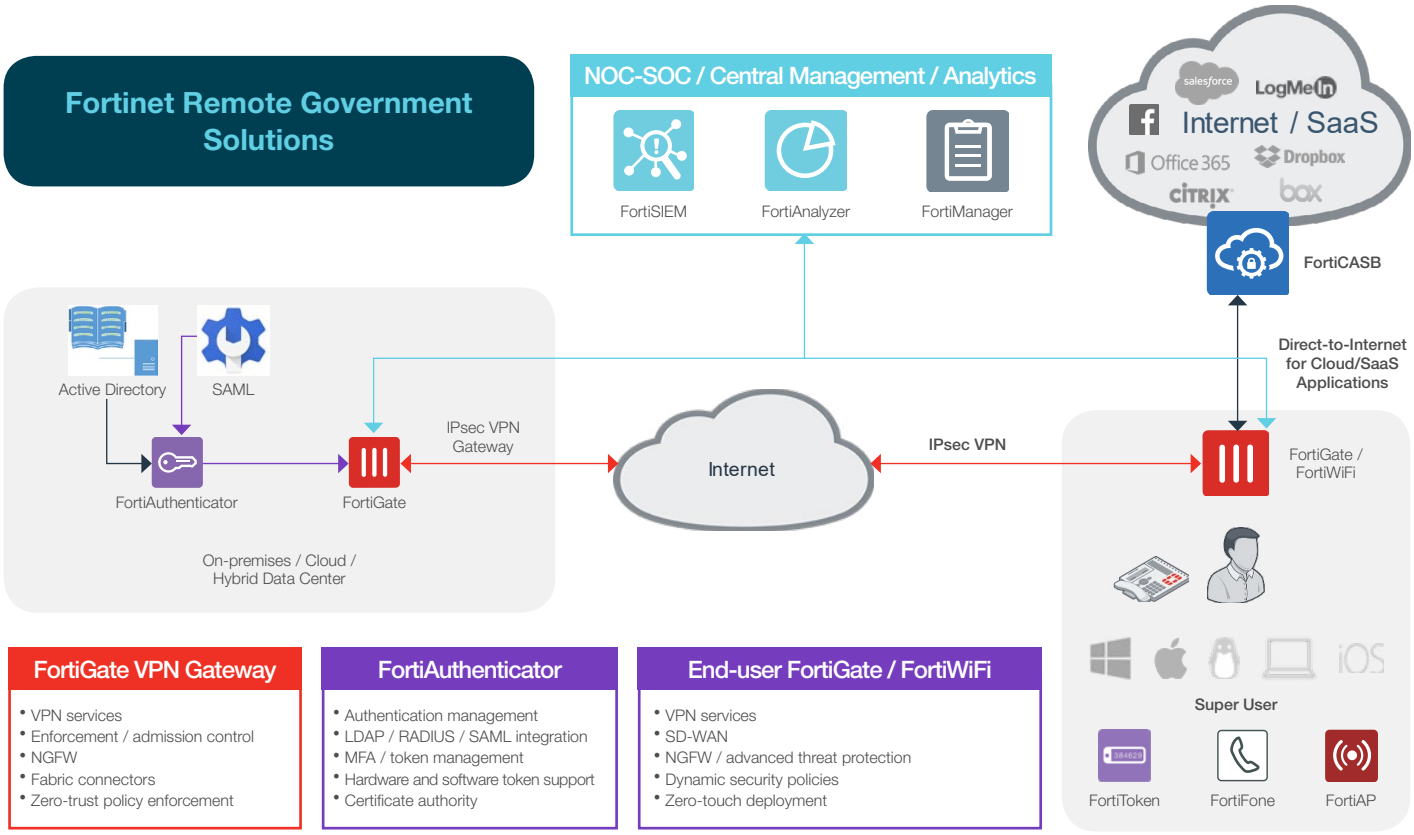


Figure 3: Fortinet solution deployment for government super user.

Achieve Full Security Integration with Fortinet Solutions

The Fortinet Security Fabric enables seamless integration of the government 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 governments are preparing a business continuity plan, since they may be forced to transition over to a fully remote workforce with little or no notice. Single-pane-of-glass visibility and management of security architecture ensures that support for telecommuting does not jeopardize 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 (BYOL, PAYG):** 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-text 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 single sign-on 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.
- **FortiWeb Cloud (BYOL, PAYG):** Fortinet WAFs protect hosted web applications from both known vulnerabilities and zero-day threats using multilayered and correlated detection methods.
- **FortiManager (BYOL):** 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 (BYOL):** FortiAnalyzer provides analytics-powered cybersecurity and log management to enable improved threat detection and breach prevention.
- **FortiSandbox (BYOL, PAYG):** 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.

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.

April 8, 2020 2:54 AM

D:\Fortinet\Solution Briefs\grey solution briefs\Government telework\sb-secure-remote-access-for-your-government-workforce-V2.1-472020-223AM

635636-0-0-EN