FORTINET FEDERAL

WHITE PAPER

Secure Wireless Connectivity for Mission-Critical Communications

Executive Summary

United States federal government agencies are required to perform a host of functions and conduct missions in remote locations, harsh environments, and on mobile platforms that require secure, highly available, and resilient networks. Traditionally, agencies have had to rely on wired or radio networks. Still, agencies now have options for connectivity through highly reliable and nearly ubiquitous LTE/5G and SATCOM networks, with technologies like SD-WAN that allow operators to select the best path for each environment. Regardless of the technology, they all need advanced cybersecurity protections. Without such secure communications, citizens may be left without essential services and support, and missions can be compromised or seriously delayed.

Fortinet Federal delivers innovative and secure networking technology that is ideally suited to address the above challenges and leverage wireless and wireline options. Based on our flagship FortiGate platform and FortiExtender gateways, the solution delivers reliable, high-performance networks fully integrated with the Fortinet Security Fabric. This allows agencies to quickly and easily deploy the right mix of wired and wireless technologies, including LTE/5G and SATCOM services, for mission needs, combining secure SD-WAN and next-generation firewall (NGFW) controls that can be managed on a single pane of glass.

Ever-Increasing Demand for Secure Agency Connectivity

Government agencies are facing growing demands to address the dual challenges of accessing reliable communications in almost any environment, with the need to protect communications and applications against increasing cybersecurity threats. This requirement for secure connectivity anywhere is driven by the following:

- The need to respond quickly to emergency or law enforcement demands while aiming for continual connectivity with mission operations and command
- A growing reliance on connected devices to accomplish basic missions and service delivery
- A parallel growth of applications that require robust connectivity to private and public clouds or directly to the internet
- The ability to leverage multiple types of connectivity options depending on the availability of technology
- The proliferation of Internet-of-Things (IoT) devices and the convergence of operational technology (OT) and information technology (IT) infrastructure management requirements
- A need to accomplish missions with minimal IT staff and other local resources

When Secure, Remote, and Resilient Connectivity Is Essential

Many agency missions have adopted mobile technology, applications, and networking. Their demand for trusted and uninterrupted access to information resources is clear, enabling the work of:

- Firefighters from the U.S. Forest Service and Bureau of Land Management
- Customs and border protection, frequently stationed in geographically remote locations
- Emergency responders to natural and human-made disasters
- Scientists and technical professionals managing advanced warnining systems
- Agency professionals operating from remote offices with limited connectivity
- Law enforcement officials conducting investigations in rural and rugged environments

Agencies Have Common Connectivity Challenges

Whatever the mission, agencies share similar connectivity challenges when dealing with remote, harsh, or mobile environments.

Limited network coverage availability: Wired broadband options, including MPLS, cable, DSL, and fiber, may not be available at many remote locations. Even when wired options have been present, they may be damaged and unavailable, and repairing or building new infrastructure is expensive and time-consuming, leaving branch or temporary support operations disconnected from necessary agency resources. In some areas, LTE/5G is similarly limited, and remote support may need to rely on SATCOM, especially Low Earth Orbit (LEO).

Network downtime: Many locations rely on a single internet service provider (ISP) or telecommunications provider, with limited or no built-in backup, and adding redundancy can be prohibitively expensive. When an edge device fails or connectivity is disrupted, there is often no alternative wired backup, leaving wireless as the only alternative for network redundancy.

Harsh conditions: Governments often conduct missions in remote, rugged environments where connectivity can be spotty (at best) and bandwidth limited (if available at all). Mission success will be constrained, and work-around ad hoc implementations may introduce cyber risks to the enterprise. In addition, extreme hot and cold climates and damp and dusty environments pose physical threats to traditional IT infrastructures. Standard industry appliances and devices are not equipped to operate in less-controlled conditions and likely will fail.

Wi-Fi obstacles: As Wi-Fi connectivity is primarily effective for short distances, it presents physical and environmental limitations for use in remote situations. Sites that require wireless access may experience challenges deploying Wi-Fi for proper coverage for public safety, emergency services, and other government activities that require very low latency connections.

Obsolete technology: Government agencies often are challenged with an extensive base of existing products and equipment that are becoming obsolete or were designed for network protocols no longer supported by the telecommunications carriers they rely on to meet their mission objectives.

Expanded attack surface: In addition to network challenges, malicious threat actors continue to develop sophisticated methods to detect and expand the attack surface introduced by remote connectivity. Transformative applications that rely on internet access can improve mission effectiveness and customer experiences and help to cut costs; however, they enable more internet egress points that may introduce new cyber risks. Network solutions backed by AI-powered security and threat intelligence are necessary to protect enterprise networks from known and zero-day threats.

Fortinet Federal Delivers Agency Networking and Security in a Single Solution

Fortinet Federal provides U.S. government customers with a powerful and unique solution that solves many of the challenges noted above. Fortinet wireless WAN solutions are flexible, simple to deploy, and secure. The solutions offer various cellular deployment options to fit agency-specific needs. In addition, Fortinet Federal offers seamless LTE/5G/Band 14 integration, secure SD-WAN, and protection from cyberthreats. Our solutions deliver optimal application experiences while protecting agency networks from advanced threats.

FortiExtender cellular gateways and FortiGate network firewalls can be deployed in nearly any branch, remote location, or mobile scenario, offering dual SIM and dual modem 5G/LTE options for optimal mission continuity. They can also be deployed as ruggedized options to withstand the harshest deployment conditions. The Fortinet Federal solution delivers:

- LTE/5G/Band 14 wireless WAN: Enables agencies to extend the edge network beyond wired limitations and deploy a cellular-first strategy with various 5G/LTE options with any major U.S. wireless provider, including FirstNet's use of Band 14. These range from cellular adapters that can extend for the best signal with minimal attenuation to integrated 5G/LTE firewalls for a streamlined, single-appliance solution ideal for remote locations or micro-site deployments. Where 5G/LTE is unavailable, agencies can access SATCOM links through the same FortiExtender device.
- High availability with built-in failover to Wireline, LTE/5G, Band 14, or SATCOM
- Bandwidth balancing, ensured by dynamic dual SIMS
- Ruggedized devices for environmentally harsh locations
- Rated IP64 to IP67, protecting against extreme high and low temperatures and providing dust, splash, and submersion protections
- Certified to protect against vibration
- Deployable kits for emergency responders
- Mobile-ready solutions with models and options tailored for deployment in vehicles, boats, and airborne platforms
- Private 5G/LTE for missions that require greater security protocols

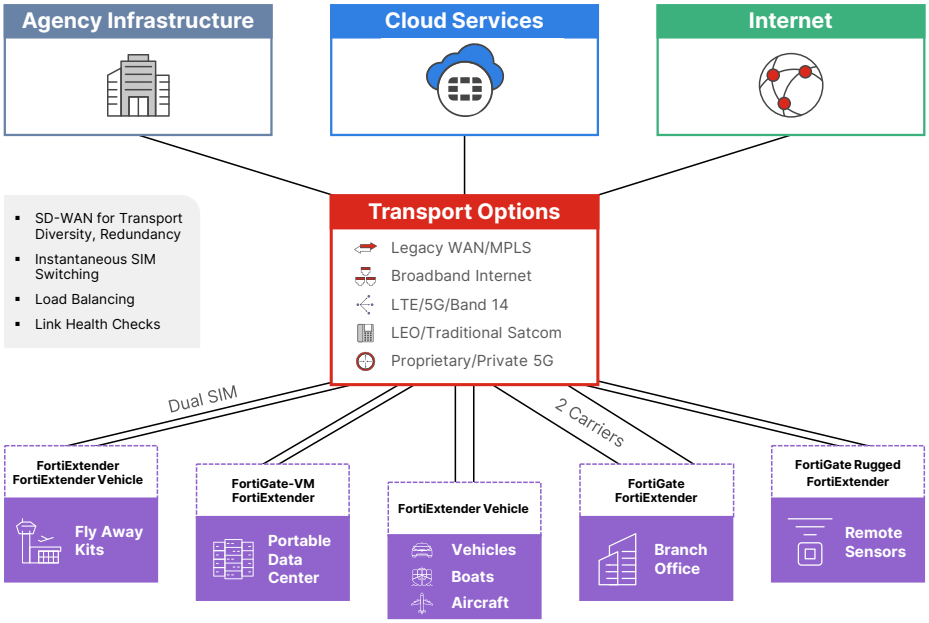

Figure 1: Leveraging Secure Wireless WAN for Mission-Critical Communications

FortiExtender cellular gateways and FortiGate NGFWs help agencies meet mission mandates with:

Improved network access and reliability: With cellular failover or active-active cellular WAN connections, remote offices, branches, and operational sites will experience significant improvements in continuity of operations and end-user experience.

Reduction in security incidents: Fortinet products are fully integrated with the Fortinet Security Fabric and FortiGuard AI-Powered Security Services. Fortinet is recognized for its industry-leading security expertise, and its wireless WAN and private 5G/LTE networks are built on a strong foundation of network firewalling, zero-trust network access, IDS/IPS, and URL, DNS, and content filtering.

Increased IT team productivity: Fortinet Federal delivers simple-to-use management options, such as FortiManager, streamlined automation capabilities, and extensive training and certification programs. The solutions can be managed through on-premises or private cloud infrastructures through a single pane of glass.

Securing Federal Government Networks

Fortinet Federal secure wireless WAN and private 5G/LTE solutions are engineered to help extend, ensure, and secure U. S. federal government networks to meet primary mission requirements, deliver excellent user experiences, and modernize secure operations and IT environments. Only Fortinet Federal offers wireless WAN and 5G/LTE solutions fully integrated into a comprehensive security fabric that includes industry-leading SD-WAN and Layer 7 security protections.

Vetting Fortinet Solutions for Your Agency

For agencies considering options to modernize secure, remote connectivity solutions, Fortinet Federal provides various resources to help technical and contracting officials make data-driven decisions to support market research, product evaluation, and contract compliance. Agency staff can avail themselves of the following:

- Technical deep dives with Fortinet Federal subject matter experts (SMEs)
- Product demonstrations and performance comparisons at a customer site, at the Fortinet Federal lab (in Reston, Virginia), or by virtual meeting
- Architectural and design analysis and recommendations
- Rough Order of Magnitude Bill of Materials and sample pricing
- Product evaluation units

Procuring Fortinet Technology: Government Contracts and Partnerships

- Fortinet technology is available to U.S. government customers through multiple contracts, including SEWP V, EIS, GSA-70, CIO-SP, and other GWAC and agency-specific contracts.
- Fortinet Federal partners with resellers, including small and disadvantaged businesses, telecom carriers, and Federal Systems Integrators that serve as prime contractors for specific agency requirements.

The Fortinet Federal team is dedicated to trusted cybersecurity for government. For additional information and support designing and implementing the most cost-effective and future-proof solution for your organization, contact Fortinet Federal at info@fortinetfederal.com or at 1-833-386-8333.

Secure Solutions Tailored to U.S. Federal Government

With a sole focus on supporting the U.S. government, Fortinet Federal offers the following technical and contracting advantages to its agency customers:

- **Exceptional supply chain security:** Fortinet products are secure by design. Fortinet Federal has one of the most robust and independently validated Security of Supply programs, including software and hardware testing that goes well beyond FAR and other U.S. government requirements, developed in partnership with the Department of Defense.
- **Risk mitigated transitions:** Fortinet Federal engineers and implementation staff have the expertise and experience to plan, coordinate, and implement a transition program that minimizes risk, ensures no disruptions to critical operations, and quickly ramps up agency staff to handle ongoing operations. Cleared staff are available as required.
- **Simplified licensing, predictable costs:** Fortinet Federal uses simplified SKUs and part numbers that make contract administration easy to understand and manage.

Components of a Fortinet Federal Secure Wireless Network

FortiGate Secure Networking Platform Options

- FortiWiFi with 5G
- FortiGate Rugged 5G Dual
- FortiGate controller

FortiExtender or FortiExtender Vehicle

- Connectivity for AT&T, Verizon, and T-Mobile LTE and 5G networks
- Band 14, FirstNet capable for use by first responders
- Connectivity to SATCOM/LEO (Starlink, Hughes) ground stations

FortiManager

FortiAnalyzer

FortiGuard AI-Powered Security Services

FORTINET FEDERAL

www.fortinetfederal.com

Fortinet Federal, Inc.
12005 Sunrise Valley Drive, Suite 201
Reston, VA 20191
Phone: 1-833-386-8333
Email: info@fortinetfederal.com

April 3, 2025 9:39 AM / MKTG-1176-0-0-EN