Federal Government Solutions: At a Glance

ROBUST, COMPLIANT AND COST-EFFECTIVE SECURITY

SonicWall delivers government-certified security for operational reliability and mission success.

FEDERAL GOVERNMENT CHALLENGES

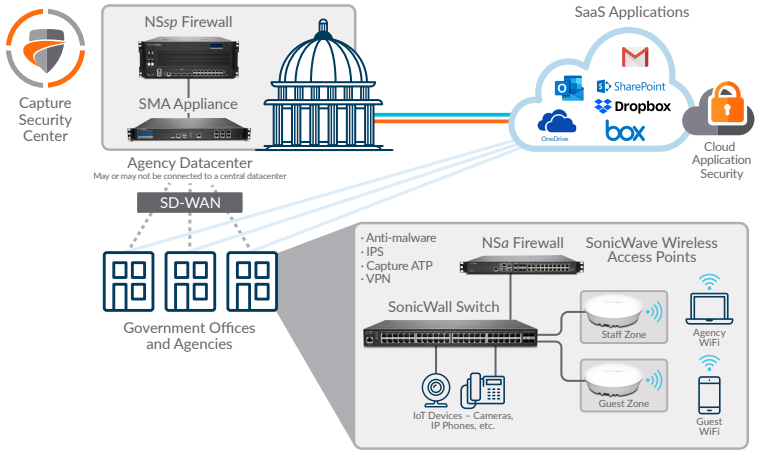
- Enable secure remote access to mission-critical resources
- Stay ahead of hidden, advanced and real-time global threats
- Centrally view and manage entire security ecosystem
- Lower administrative cost and complexity
- Comply with regulatory mandates

SONICWALL FEDERAL GOVERNMENT SOLUTIONS

- SonicWall meets governmental certification and interoperability requirements, e.g., NIST, FIPS 140-2, CSfC, Common Criteria, DoDIN APL, USGv6 and NSA CNSA Suite B
- SonicWall offers automated real-time breach detection and prevention, TLS inspection, Real-Time Deep Memory Inspection (RTDMI), Reassembly-Free Deep Packet Inspection (RFDPI), Capture ATP cloud-based multi-engine sandboxing, or Capture Security appliance (CS*a*) on-premise advanced threat detection, and Cloud App Security for 0365 and G Suite applications
- With SonicWall SMA, government organizations can provide a field-proven and secure remote access solution that boosts productivity, supports mobility, and enforces compliance through proper user and device authentications. SonicWall SMA also provides FIPS 140-2 via a simple software license.
- SonicWall solutions are easy to learn and deploy, centrally managed, dynamically updated, based on open standards, and backed by support, training and professional services

USE CASE SCENARIO

An agency might deploy an enterprise-class NS*sp* firewall at a datacenter, plus mid-range NS*a* and entry-level TZ firewalls at field offices, connected via site-to-site VPN, and manage them all centrally with Network Security Manager (NSM). Securely connect remote users via SMA. SD-WAN replaces expensive MPLS with cost-effective Ethernet, DSL or 3G/4G. Wireless access points, IP phones, cameras and other devices are enabled by Power-over-Ethernet (PoE). SonicWall Switch extends wired connectivity at the offices. CS*a* is used back at the datacenter for all devices on the network to reference for advanced malware detection. Capture Security Center provides single-pane-of-glass management.



SONICWALL BENEFITS FOR FEDERAL GOVERNMENT

- Unified network, wireless, switching, email, mobile, IoT, advanced malware detection and endpoint security platform
- Centralized deployment, management, reporting, analysis and rapid remediation from a unified console
- Secure, consistent access and availability from anywhere
- Lower overhead and TCO, and higher ROI

SONICWALL AND FEDERAL GOVERNMENT

SonicWall offers federal agencies a cost-effective, automated, real-time platform for defense, management, and connectivity. **Learn more** at www.sonicwall.com/federal

> "What we have learned from the numerous breaches in the public and private sectors is that the foundation of the internet is a digital supply chain that must be defended from end to end."
>
> – **BILL CONNER, PRESIDENT AND CEO SONICWALL**

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Misc-FederalAtAGlance-US-VG-2958