Federal Government Solutions: At a Glance

ROBUST, COMPLIANT AND COST-EFFECTIVE SECURITY
Federal agencies need high security and compliance, kept within budget. SonicWall offers advanced security at a low cost of ownership.

FEDERAL GOVERNMENT CHALLENGES
- Stay ahead of advanced, real-time global threats
- Centrally manage entire security ecosystem
- Lower administrative cost and complexity
- Comply with regulatory mandates

SONICWALL FEDERAL GOVERNMENT SOLUTIONS
- SonicWall offers automated real-time breach detection and prevention, DPI-SSL encrypted threat detection, Real-Time Deep Memory Inspection (RTDMI), Reassembly-Free Deep Packet Inspection (RFDPI), Capture ATP cloud-based multi-engine sandboxing, and Cloud App Security for O365 and G Suite
- SonicWall meets governmental certification and interoperability requirements, e.g., NIST, FISP 140-2, UC APL, CSfC, Common Criteria, USGv6 and NSA Suite B
- 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
A typical federal agency network might deploy an enterprise-class NSap firewall at a datacenter, plus mid-range NSa and entry-level TZ firewalls at field offices, connected via site-to-site VPN. 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). Capture Security Center provides single-pane-of-glass management.

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