Globally Distributed Networks – Federal Agency Use Case

FEDERAL GOVERNMENT CHALLENGES

In addition to the military, the United States has numerous federal agency offices across the nation, as well as in many other countries and territories. Connecting facilities to one another in such a way that allows agents and personnel to safely connect to online resources from anywhere, while at the same time restricting access to unauthorized entities, presents a major challenge but is vital to success. This becomes increasingly difficult to do securely when those agencies have overseas locations and are transmitting sensitive information over the public internet.

THE SOLUTION

Just like in the private sector, distributed federal agencies like these use Next Generation Firewalls (NGFW) to both scout for malware as and manage VPN connectivity — but with some caveats. Since a single-vendor firewall solution (including HA pairs) can leave your network and resources vulnerable to inside, outside and partner-sourced attacks, it can also be a single point of failure. Security-sensitive agencies deploy a defense-in-layers strategy, using two or more vendor firewalls. This configuration helps to reduce cybersecurity risks, detect and stop malware, and protect onsite and remote personnel, integrators, and contractors. Employing an IPSec or VPN solution with the NGFW or a separate VPN appliance tied to it enables personnel to safely access relative information. Additionally, to securely connect outside personnel with online resources, agencies deploy a form of a unified secure access gateway to provide anytime, anywhere and any device access to any application based on policy.

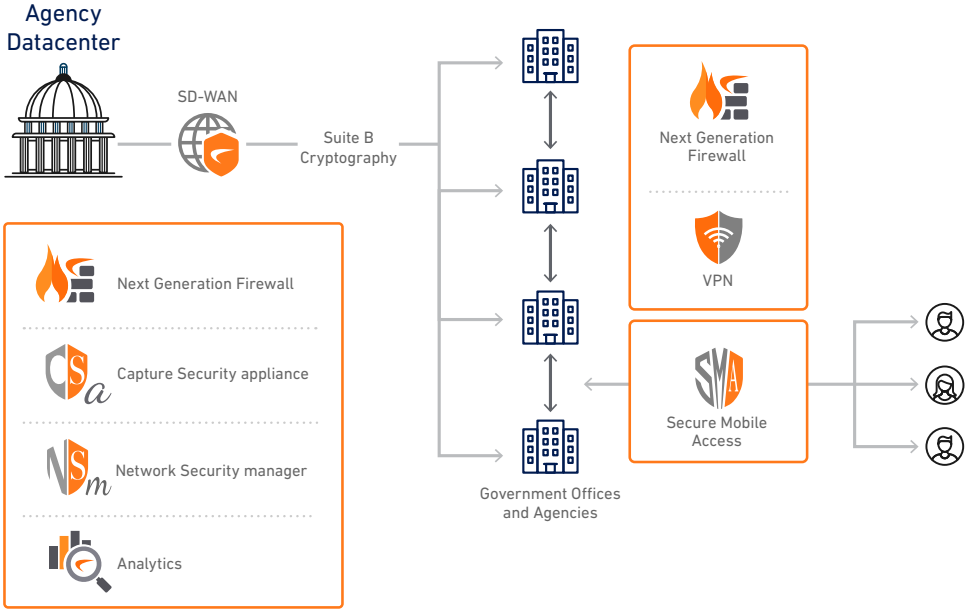
HOW SONICWALL HELPS

SonicWall provides these solutions to several distributed government agencies throughout the world. They use SonicWall NGFW devices alongside other third-party firewalls to create a defense-in-layers strategy. An agency might deploy an enterprise-class NSsp firewall at a datacenter, plus mid-range NSa and entry-level TZ firewalls at field offices or bases, all connected via site-to-site VPN, and all centrally managed with Network Security Manager (NSM). Additionally, they leverage the SD-WAN capabilities on the NGFW for site-to-site connectivity to protect data in transit without relying on MPLS connections which may not be even present in many locations. For advanced threat analysis without leveraging cloud-based detection, agencies use Capture Security appliance (CSa) back at the datacenter for all devices on the network to reference for advanced malware detection. SonicWall Secure Mobile Access (SMA) is used to define the policies and establish the security connection of personnel to agency resources, no matter where they are.

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



SonicWall, Inc.
13155 Noel Rd., Ste. 800 | Dallas, TX 75240
Refer to the SonicWall Federal team for additional information.
FederalTeam@sonicwall.com
(888) 977-1062

UseCase-GloballyDistNetworks-Federal-JK-3739

SONICWALL