Globally Distributed Networks – Military Use Case

FEDERAL GOVERNMENT CHALLENGES

The United States has a large, globally distributed military force that consists of several hundred installations in over 70 countries and territories. Allowing the right personnel to connect and check on the status of critical military equipment across this distribution, while at the same time restricting unauthorized access to sensitive information, is both a major challenge as well as vital to mission success. These connections range from the traditional hub-and-spoke model to specific site-to-site connections.

THE SOLUTION

In distributed organizations composed of people, equipment and installations, using a Next Generation Firewall (NGFW) that manages VPN connectivity is a standard practice, but it comes with some caveats for a military force. 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 forces employ a defense-in-layers strategy using two or more vendors' firewalls to reduce cybersecurity risks and detect and stop malware, all while protecting onsite and remote personnel, including troops, contractors and friendly forces. By employing an IPSec or VPN solution with a NGFW or a separate VPN appliance tied to it, personnel can safely and securely access and transmit information system data through blue and gray space networks around the world.

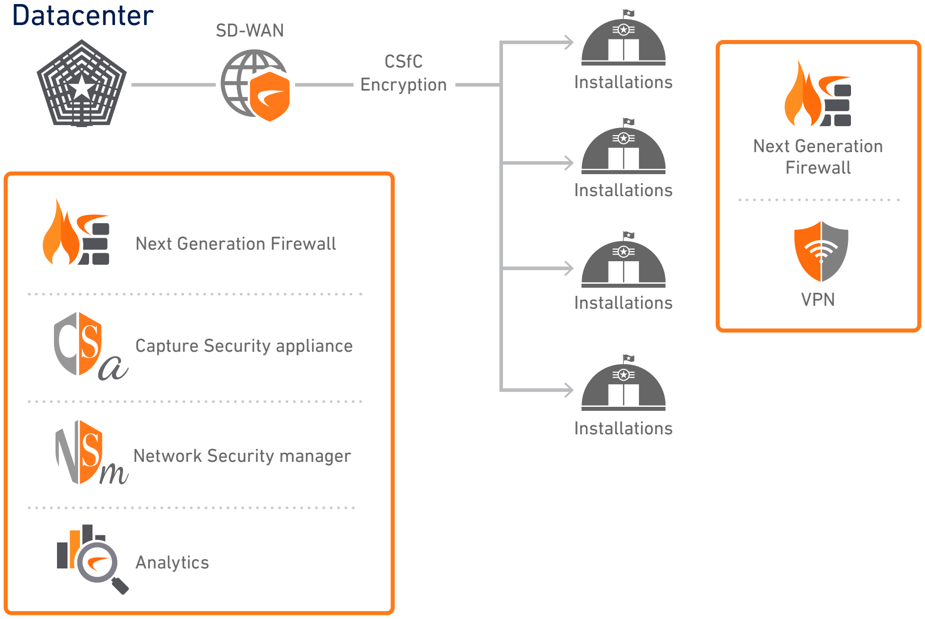
HOW SONICWALL HELPS

U.S. military commands integrate SonicWall's NSsp firewalls at HQ and SonicWall's mid-range NSa and entry-level TZ firewalls to lower echelons. These are connected via site-to-site VPN and Network Security Manager (NSM) or Global Management System (GMS) to Command, Control, Communications and Computer (C4) platform to enable the IS workforces with Boundless configuration, deployment, management, visibility, reporting and analytic capabilities. Additionally, SonicWall's next-generation firewall (NGFW) software-defined wide area network (SD-WAN) technology simultaneously enhances distributed network traffic performance while dramatically decreasing the command's internet service provider (ISP) cost. Those commands with SonicWall's Capture Security appliance (CSa) give their cyber forces the ability to thwart the latest zero-day attacks and never-before-seen malware variants and help uncover indicators of compromise (IoC).

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-Military-VG-3711