Tip-of-the-Spear Use Case

A commander's ability to dominate defensively and offensively in cyberspace is key to their success in multi-domain operations (MDO). Mission critical assets, such as personnel, infrastructure, equipment and data must be protected at all times during defensive cyberspace operations (DCO). Additionally, commanders must also be able to deliver desired effects to adversaries when the mission dictates the need during offensive cyberspace operations (OCO). To accomplish their mission, commanders require:

- Secure command-and-control (C2) communications
- Technology that is easy to deploy, manage and use, especially for mobile users
- Threat intelligence for situational awareness
- Detect, prevent and response capabilities

HOW THEY ACCOMPLISH THE MISSION

To achieve these four aims, commanders use next-generation firewalls (NGFWs). A NGFW is a multi-use tool to secure connections and communications to networks. For most, VPN capabilities top the list to help ensure a private connection from point to point. Access Control Lists (ACLs), access rules and account privileges are essential to make sure the right people, domains and devices can access specific network resources.

What sets NGFWs apart from stateful firewalls is the use of threat prevention services to stop known and unknown malware attacks on the device. Having the ability to inspect encrypted traffic for threats is viewed as necessary in today's threat landscape, according to military commanders over cyber defense. Reporting and analytics features work together to offer intelligence on firewall activity, along with the ability to diagnose anomalous activity — capabilities commands of the past did not have access to.

Additionally, having intelligence on firewall activity and the ability to diagnose anomalous activity is achieved by using a mixture of reporting and analytics on activity. In order for these firewalls to be used and deployed efficiently, they need to be standardized on the department's configurations as they are sent from the manufacture known as "Zero Touch deployment". With multiple firewalls in use, on-premise and/or cloud management is needed to monitor and make changes to firewalls without immediate physical access.

HOW SONICWALL HELPS

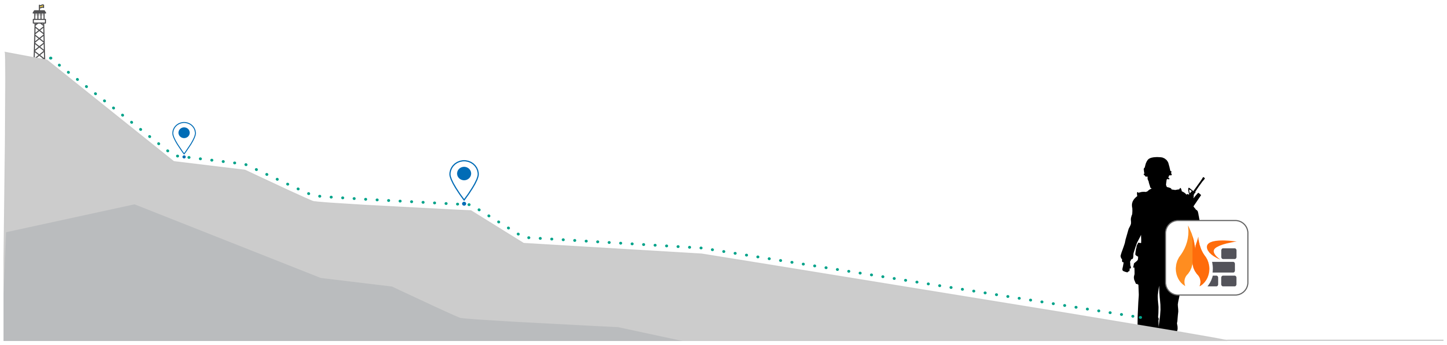
Whether your mission is to support DCO efforts to protect critical assets or to deliver kinetic effects-conducting OCO, the SonicWall Federal Next Generation Firewall provides your command with the right tools. Secure communication through VPN connectivity. Access real-time intelligence with SonicWall's Reporting and Analytics. Plus, take advantage of the rapid detection, prevention and response capabilities needed to thwart cyberspace attacks with threat prevention services. These protect against known malware attacks (Gateway Antivirus), IPS attacks, and unknown malware (either Capture ATP or Capture Security appliance) that are present in the current and future MDO environment. For protection against encrypted threats, military commanders also use SonicWall DPI-SSL to inspect encrypted traffic.

Ground troops can be equipped with a SonicWall TZ or virtual series next-generation firewall in their Tip-of-the-Spear kit. Designed to work in both dry and humid environments, these zero-touch enabled firewalls can be sent or brought to forward locations with the organization's preferred configurations without opening and working with the device before deployment.

SONICWALL AND FEDERAL GOVERNMENT

SonicWall offers distributed military forces and agencies with 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-TipOfTheSpear-VG-3938

SONICWALL®