Mitigating Cyber Risks for Remote Federal Workers

While remote work arrangements have become common over the past decade, this shift hasn't been adopted uniformly. Due to the sensitive information they handle, the heightened risks associated with failing to secure this information, and the need to comply with stringent regulations, the federal sector has been among the last mandating fully office-centric work.

This has worked well as a risk-management tactic. However, recent events have demonstrated a growing need for flexibility. Agencies need to address this emerging new normal by mitigating the security risks of remote and mobile access.

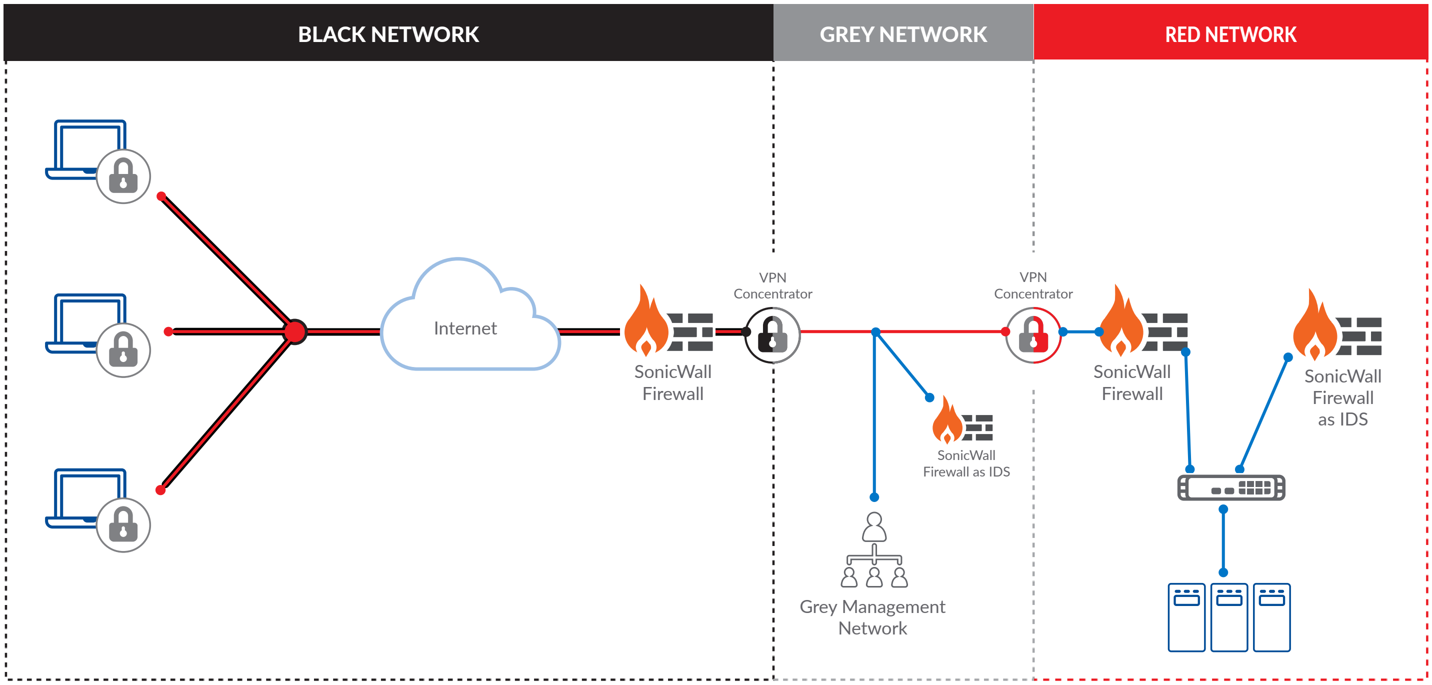
SONICWALL AND FEDERAL GOVERNMENT

While remote work arrangements can still introduce an element of risk, the good news is that these risks can be largely mitigated. SonicWall's Boundless Cybersecurity offers unified visibility and control while identifying evasive and cutting-edge threats, allowing the federal sector to secure remote employees and safeguard sensitive and classified data. SonicWall offers federal agencies a cost-effective, automated, real-time prevention platform for defense, connectivity and management — one that's **FIPS 140-2, Common Criteria, UC APL, and CSfC certified.**

By using SonicWall with other Commercial Solutions for Classified (CSfC) certified solutions, you can build out dual-tunnel architecture to meet the standards of the CSfC compatibility packages — effectively securing valuable data from bad actors.

USE CASE EXAMPLE

SonicWall's Boundless Cybersecurity allows government employees and officials to access sensitive data while abiding by the guidelines and restriction of the CSfC.



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

Misc-MitigatingCyberRisks-US-VG-2020