# Defense-in-Depth Layered Firewall Strategy for Federal Agencies

A single-vendor firewall solution can leave your network and resources vulnerable to inside, outside, and partner-sourced attacks while also being a single point of failure.

A defense-in-depth strategy using multiple vendor firewalls can reduce cybersecurity risks and protect your onsite and remote employees, customers, integrators and contractors – as well as your reputation – with the following advantages.

## CONFIDENTIALITY & INTEGRITY

A dual-vendor firewall solution with your current solution and SonicWall products can effectively isolate and protect enclave traffic and resources while also managing integrator and contractor access.

## AVAILABILITY & FAULT TOLERANCE

One system can continue to protect the networks if the other dies. While both are functional, each can lighten the load of the other by focusing on different missions and traffic types and sources. SonicWall provides further fault-tolerance with dual-WAN and High Availability (HA) firewall pairs.

## FLEXIBILITY

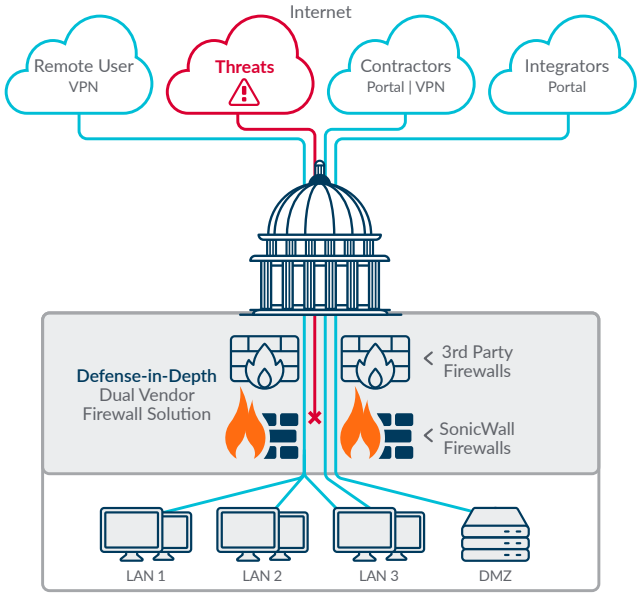
Each can focus on different network players and types of traffic. For instance, an existing firewall may do stateful inspections and routing while a SonicWall HA pair performs deep packet inspection and SSL decryption for inspection. Or, while both vendors do deep packet inspection, each can target different applications and file types.

## MULTI-VECTOR PROTECTION

In addition to integrator and contractor isolation, a SonicWall solution may also allow IPSec or SSL VPN connectivity while the other takes care of content filtering and additional application monitoring.

## HOLISTIC SECURITY

Catch the software-defined (SDx) wave. A dual-vendor solution using SonicWall firewalls can help cover software-defined and traditional security needs as well as conventional secure networking capabilities.




## WHY SONICWALL?

SonicWall can prevent advanced threats using SonicWall's on-prem Capture Security Appliance running Real-Time Deep Memory Inspection (RTDMI) and on-box threat prevention featuring Reassembly-Free Deep Packet Inspection (RFDPI), anti-malware, intrusion prevention, web filtering and more.

SonicWall products are on the DISA Approved Products List. Certifications include FIPS 140-2, Common Criteria, DOD UC-APL, Commercial Solutions for Classified (CSfC), USGv6, and ICSA.

Contact your local SonicWall reseller for more information!

888-977-1062

FederalTeam@SonicWall.com

Learn more at
www.sonicwall.com/solutions/government-federal-institutions/

**SonicWall, Inc.**
13155 Noel Rd., Ste. 800 | Dallas, TX 75240
Refer to our website for additional information.
www.sonicwall.com/federal



Misc-DefenseInDepth-Fed-US-COG-2143