Secure Federal Network Solution with Modern VPN, NGFW, and Zero-Trust

Introduction

Federal requirements are often strict with little room for flexibility. Adoption requires adherence to government and regulatory standards that exist to guarantee a level of security that is consistent and hardened for cybersecurity compliance. Consider the following items that federal installations often require for the adoption of remote access network solutions:

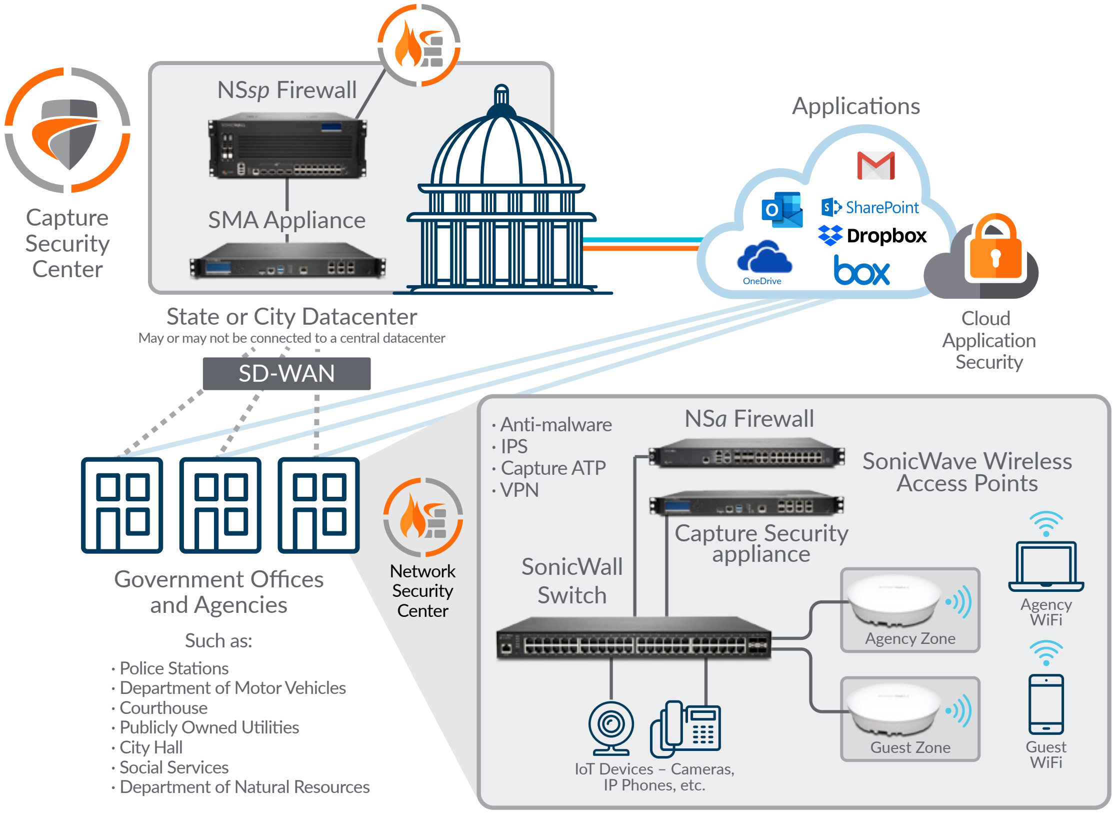
- On-premises network access and control as well as cloud-based options
- Compliance with federal security regulations such as the U.S. Department of Defense Information Network Approved Products List (DoDIN APL), Federal Information Processing Standards (FIPS), and more
- Adherence to the National Institute of Standards and Technology (NIST) firewall guidelines
- Network segregation and segmentation
- Mapping to Federal Information Security Management Act (FISMA) firewall frameworks
- Strong access controls, such as multi-factor authentication and role-based access
- Encryption and HTTPS inspection
- Continuous monitoring
- Regularly applying software updates and patches to address known vulnerabilities

Modern VPN and next-generation firewall (NGFW) technologies play a pivotal role in establishing a secure zero-trust federal network solution. Modern VPN technology enables secure remote mobile access, ensuring that authorized users can connect to the network while implementing strong authentication and encryption protocols and safeguarding data confidentiality and integrity. NGFWs enforce zero-trust principles by implementing stringent application controls, continuous monitoring and network segmentation. They can segment the network into isolated zones, limiting lateral movement and containing potential breaches. By pairing modern VPN and NGFW technology, federal agencies can create a robust network infrastructure that adheres to zero-trust principles and ensures compliance with regulatory requirements.

SonicWall SMA 1000 Series

SonicWall's Secure Mobile Access (SMA) 1000 series represents the technology behind the VPN aspect of this pairing. Besides providing secure remote access, the SMA 1000 supports compliance with various federal security regulations, such as FIPS, CSfC, and DoDIN APL. Granular access control and endpoint control (SonicWall EPC) provide a layered approach, where both user and device are evaluated for least privileged access.

SOLUTION BRIEF



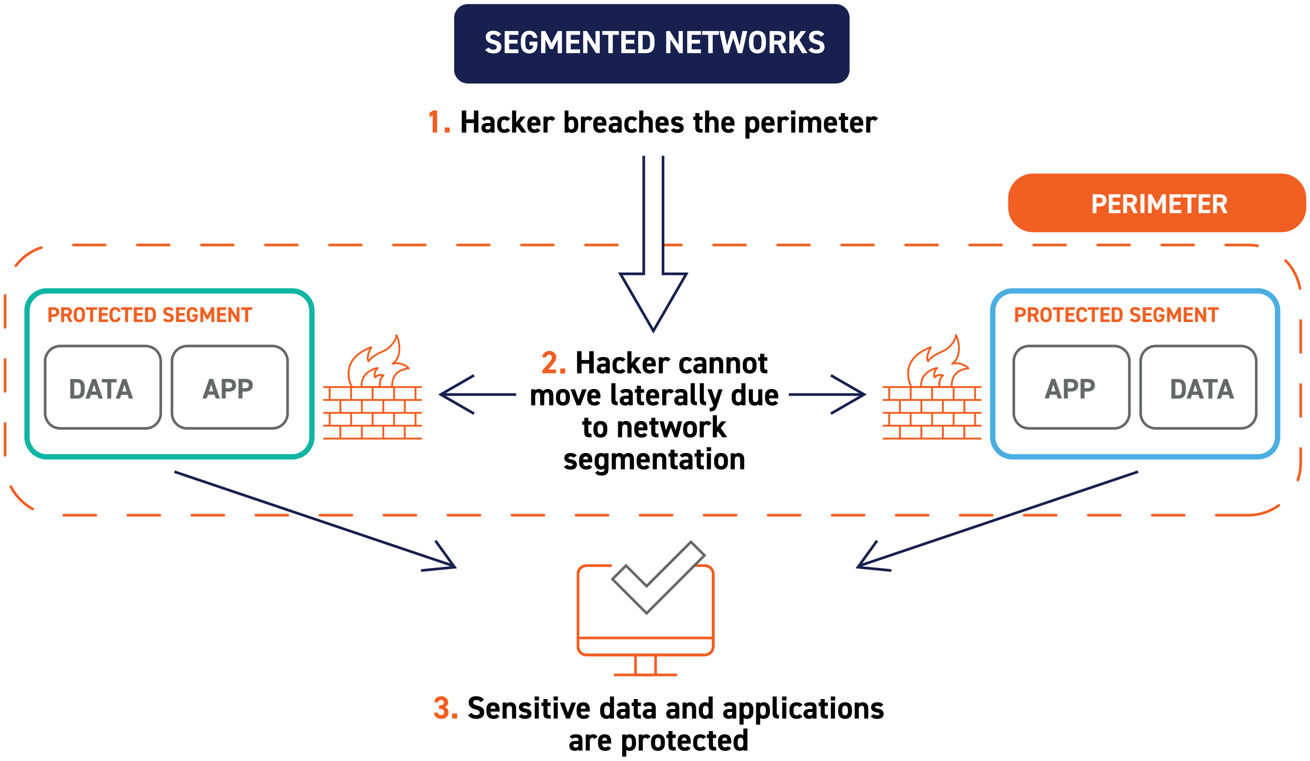
SonicWall NGFW Series

The other side of this pairing includes a SonicWall NGFW. When it comes to zero-trust, an NGFW plays a crucial role in implementing and enforcing zero-trust principles within an organization's network architecture. All the features and benefits of this NGFW zero-trust solution include Content Filtering Services (CFS), Capture Advanced Threat Protection (ATP), Layer 3-7 Access Control, DPI-SSL Application Control, and Network Segmentation, to name a few.

By leveraging a SonicWall NGFW and SMA 1000, federal agencies can establish a robust zero-trust network architecture that focuses on strict access controls, network segmentation, secure mobile access and threat prevention while maintaining regulatory security compliance. Additional SonicWall cybersecurity solutions can of course be added to the ecosystem depending on requirements and architecture.

Use Case #1: Prevent Outbound Network Traffic

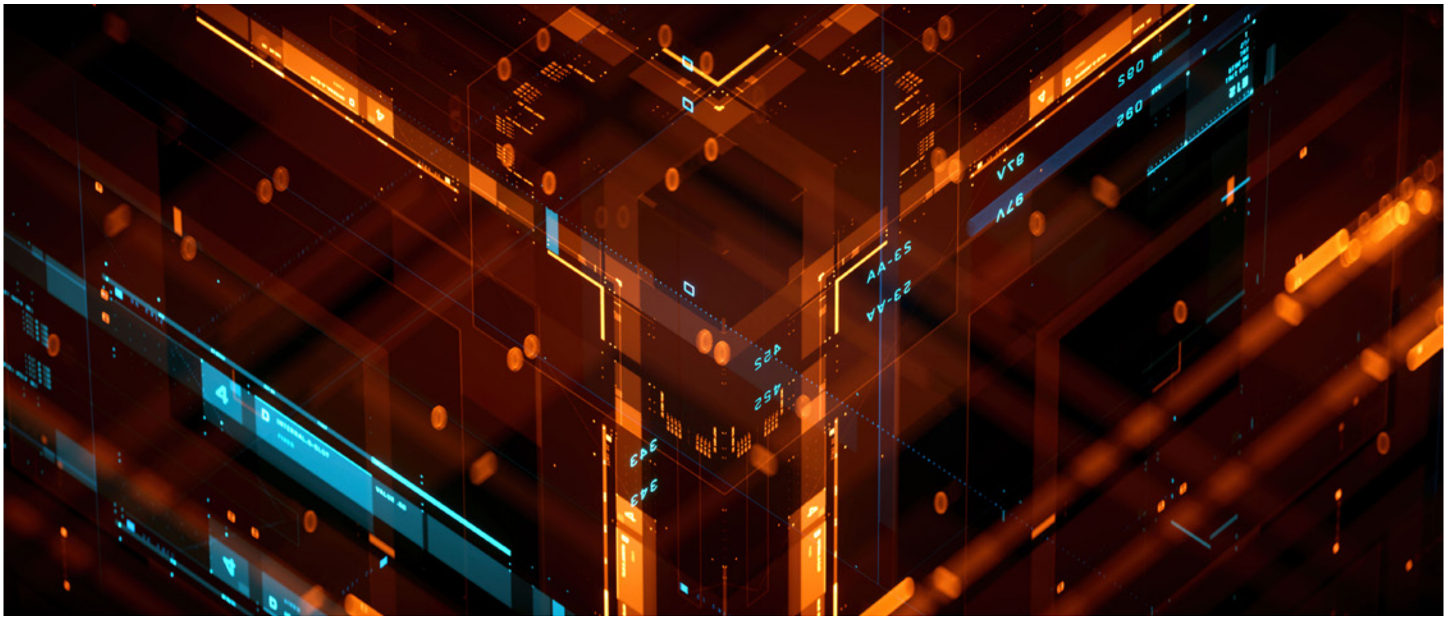
A critical aspect of strong network security is preventing outbound network traffic. Stopping the accidental or intentional exfiltration of sensitive information is of paramount importance. The SMA 1000 can enforce VPN policies (split tunneling for example) that restrict outbound traffic to the VPN tunnel. With the addition of the NGFW, more powerful rules restricting outbound traffic can be achieved. Through Layer 7 inspection, the NGFW can identify and block potentially malicious or unauthorized activities. Enforcement of granular policies through application allow and deny lists and DPI to detect and prevent data exfiltration attempts, malware transmissions, or suspicious network behavior. By pairing an NGFW, organizations get enhanced visibility and control, helping to mitigate security risks and protect sensitive data from leaving the network.

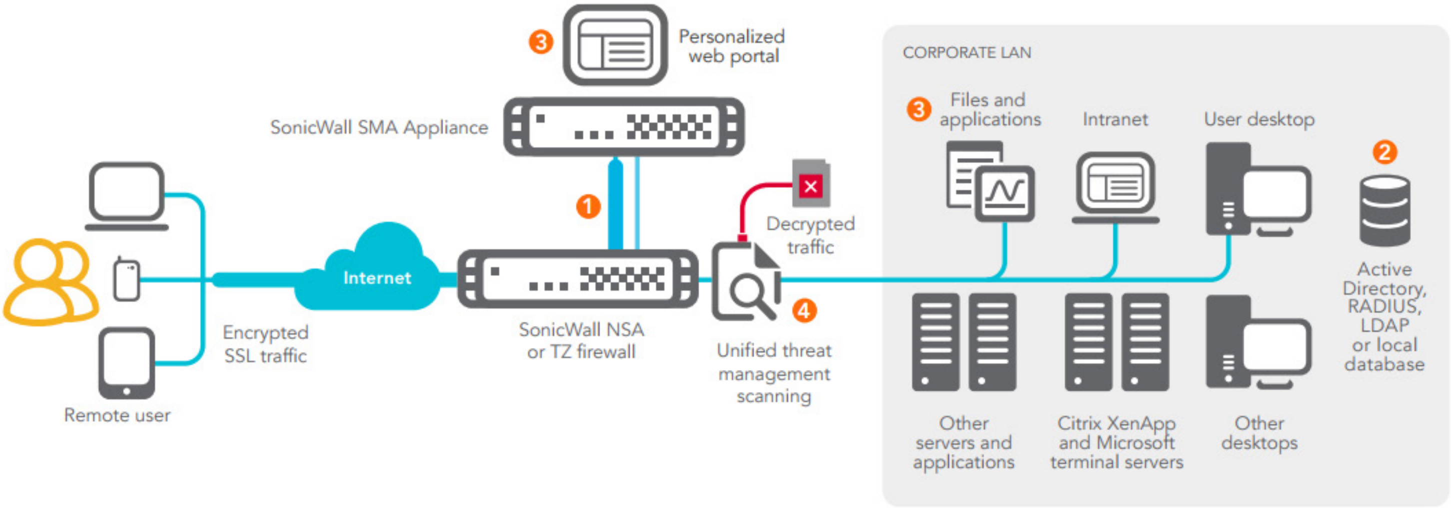

SEGMENTED NETWORKS
1. Hacker breaches the perimeter
PERIMETER
PROTECTED SEGMENT
DATA
APP
2. Hacker cannot move laterally due to network segmentation
PROTECTED SEGMENT
APP
DATA
3. Sensitive data and applications are protected

Use Case #2: Facilitate Network Segmentation

SonicWall NGFWs allow organizations to define and enforce policies that segment the network into isolated zones or micro-perimeters based on factors such as user roles, device types or application requirements. By segmenting the network, organizations can minimize the lateral movement of threats, contain potential breaches and improve overall network security by restricting access to sensitive resources only to authorized entities within specific segments.

Network segmentation is not only a significant component of a zero-trust framework but is also strongly advised by the Federal Government as a best practice for improving cybersecurity. Various Federal Agencies, including the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS), recommend network segmentation as a fundamental security measure.




3
Personalized web portal
SonicWall SMA Appliance
1
Internet
Encrypted SSL traffic
Remote user
SonicWall NSA or TZ firewall
Decrypted traffic
4
Unified threat management scanning
CORPORATE LAN
3
Files and applications
Intranet
User desktop
2
Active Directory, RADIUS, LDAP or local database
Other servers and applications
Citrix XenApp and Microsoft terminal servers
Other desktops

Use Case #3: Clientless Zero-Trust Web Access

Government employees outside the secure network who need to access government resources can securely access them without installing any software on their devices or exposing sensitive data to potential security threats by using clientless web access. Any modern browser that supports HTML5 can be used to authenticate through a secure web portal where the user is provided with a web-based interface allowing them to access the applications and data they need. Clientless web access via the SMA 1000 provides a secure and flexible way for federal employees to access government resources remotely while maintaining the security and integrity of sensitive data and applications.

To learn more, contact your SonicWall representative today or click here.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com