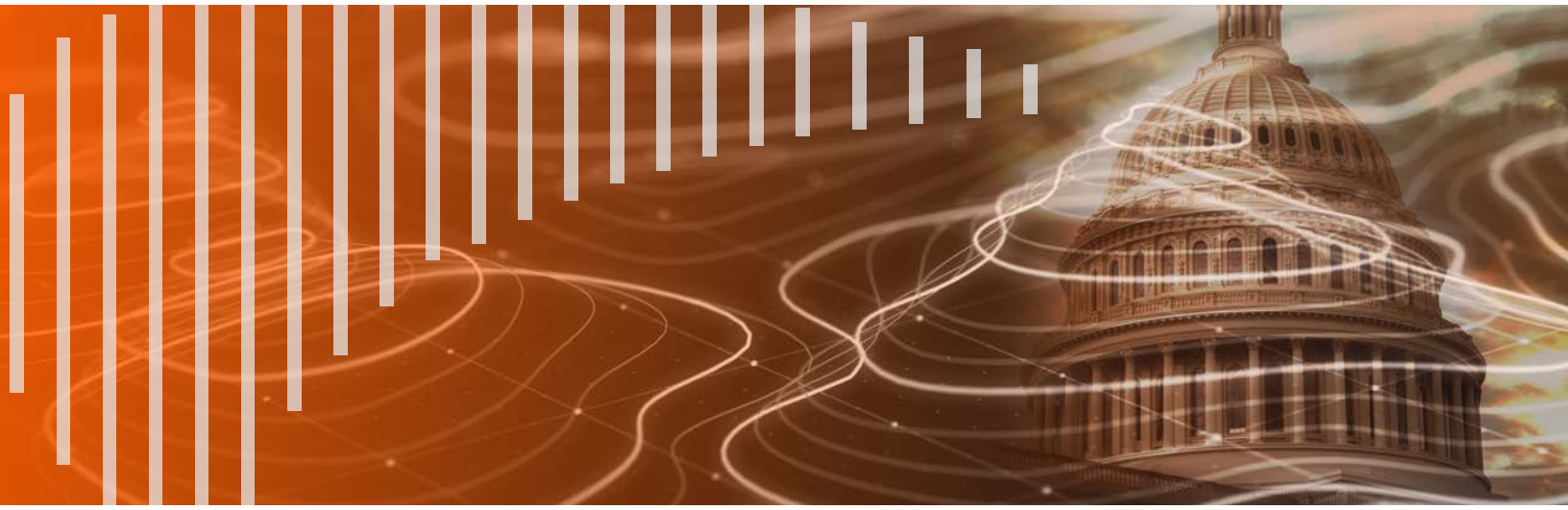


EXECUTIVE BRIEF

Need ZTNA That Complies with Federal Guidelines? Meet the SMA 1000

Intro

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.
- Compliance with federal security regulations such as the U.S. Department of Defense Information Network (DoDIN) Approved Products List (APL), Federal Information Processing Standards (FIPS), Commercial Solutions For Classified Program (CSFC) the new US National Cybersecurity Strategy, and more.
- Strong access controls, such as multi-factor authentication and role-based access.
- Encrypting sensitive data.
- Regularly applying software updates and patches to address known vulnerabilities.

The SMA 1000 Series

SonicWall's Secure Mobile Access (SMA) 1000 series meets these essential requirements along with additional attributes for scalability, ease of management, and deployment. It also includes features that meet Zero-Trust Network Access (ZTNA) standards. At a high level, the SMA 1000 solution meets the following key requirements when it comes to federal installations:

Compliance With Federal Security Regulations: The SMA 1000 supports compliance with a variety of federal security regulations, such as FIPS, CSFC, and DoDIN APL.

Strong Authentication: The solution supports multi-factor authentication, such as username and password, smart card, and biometric authentication to ensure that only authorized users can access the network.

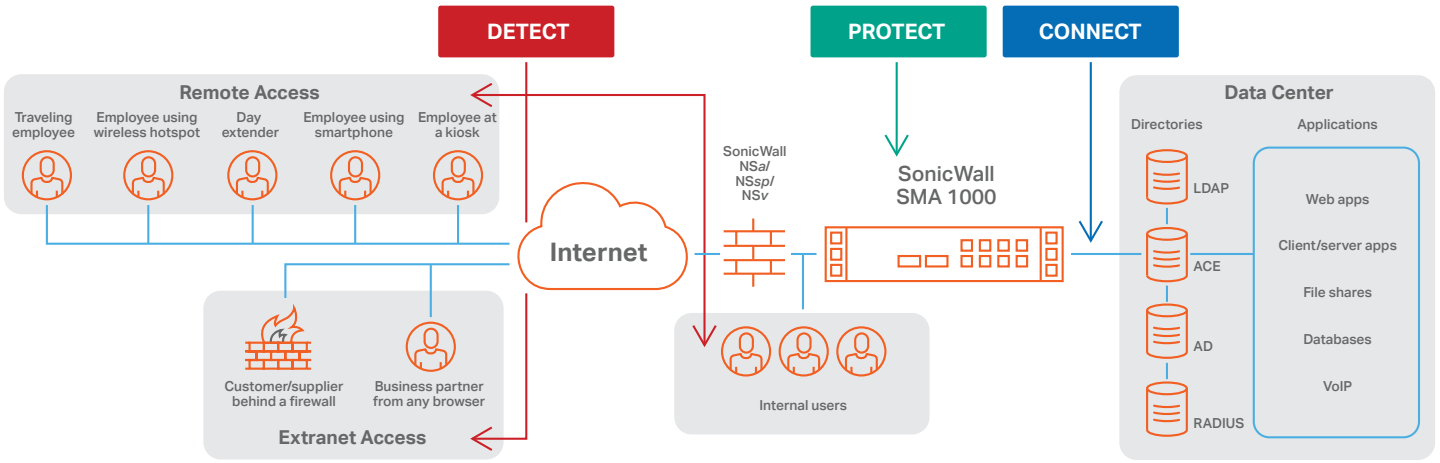
Encryption: The device encrypts data in transit using industry-standard encryption protocols SSL/TLS to protect sensitive data.

Access Control: The SMA 1000 provides granular access controls that allow administrators to control which users can access which resources based on their roles and responsibilities. It also provides End Point Control (EPC) capabilities that enable administrators to control access to the network based on the security posture of the user's device, such as ensuring that the device is running up-to-date antivirus software and has the latest software patches.

Continuous Monitoring and PSIRT Accountability: The solution provides real-time monitoring and reporting capabilities that help federal agencies keep track of user activity, identify potential security threats, and respond quickly to incidents.

Secure Remote Access: The device provides secure and seamless remote access to federal network resources, allowing employees to work from any location.

With all these capabilities, the SonicWall SMA 1000 can help federal agencies secure their on-premises networks while also meeting state, national, and regulatory compliance standards.



DETECT	SonicWall SMA 1000 End Point Control continually detects the identity and security state of the end device
PROTECT	SonicWall SMA 1000 Unified Policy enforces device access control, ensuring users access only to authorized applications
CONNECT	SonicWall SMA 1000 Smart Access and Smart Tunneling ensure easy, secure user access to all network resources

Use Case #1: Remote Desktop Access

Facilitating access and control to resources from another location over the network or internet is a key capability and prerequisite to any secure remote access solution. The SMA 1000 supports Windows 10 & 11, macOS 10.15.X, macOS 11.X, and macOS 12.X. Users can use the browser of their choice with support for up-to-date versions of Edge (Version 96 or later), Chrome (Version 96 or later), Firefox (Version 95 or later), and Safari (Version 15 or later). The remote desktop feature includes secure access. It uses SSL/TLS encryption to secure data in transit and provides strong authentication options like multi-factor authentication to ensure only authorized users can access network resources. The remote desktop feature integrates seamlessly with the SMA 1000 to secure data in transit and allow users to access the network as if they were physically present. The remote desktop feature can be deployed on-premises, in the cloud, or as a hybrid solution, depending on the infrastructure. Through a centralized management console, administrators can manage user accounts, network permissions, and access to network resources all while fully remote. Numerous customization options allow organizations to tailor the interface and experience to their needs.

Use Case #2: Preventing 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. Blocking outbound network traffic can also reduce the risk of spreading malware and viruses beyond the network while simultaneously ensuring the networks run optimally by limiting bandwidth consumption and resources. The SMA 1000 can enforce VPN policies (split tunneling for example) that restrict outbound traffic to the VPN tunnel. With the addition of our NGFW solution, the SMA 1000 can affect more powerful rules restricting outbound traffic through advanced firewall policies, content filtering, and application control.

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 needing to install any software on their personal devices or exposing sensitive data to potential security threats, by using clientless web access. Any modern browser that supports HTML 5 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 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.

SMA 1000 Features At a Glance

This table summarizes both the ZTNA features and regulatory compliance the SMA 1000 series can help support. For more information, and to contact someone on SonicWall's federal team, visit the link here.

SonicWall SMA 1000 Attribute	Zero-Trust Network Access	Supports Regulatory Compliance
Multi-Factor Authentication (MFA) & Role Based Access	Yes	Yes
End Point Control (EPC)	Yes	Yes
Secure Remote Access	Yes	Yes
Monitoring	Yes	Yes
On-premises deployment	NA	Yes
Regulatory Compliance: DoDIN/APL, FIPS, Common Criteria	NA	Yes
Encryption	Yes	Yes
Resource Access Control	Yes	Yes
Flexible Licensing	NA	Yes

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

SONICWALL