SONICWALL SECURITY HEALTH CHECK SERVICE

Ensure your SonicWall investment is fully optimized to protect your network

Overview

The SonicWall Security Health Check Service is designed to provide customers with a comprehensive review of their SonicWall network security posture and identify any security gaps that need to be addressed. The Advanced Services Partner will provide their customer with a Health Check Report that will include findings and any recommended actions to be taken. This may include specific SonicWall configuration optimizations that can evolve in follow-up remediation projects, but also more general and network-specific optimization suggestions that may result in follow-up projects such as network migration to a more efficient network topology. This guide is intended to provide SonicWall customers with a clear understanding of what the Security Health Check Service entails.

In-Scope Activities

The **Security Health Check** is a one-day service that reviews existing configurations to ensure best practices are followed in following areas.

Overall Appliance Status Check

- Firmware Version & Review of New Releases
- Licensing Review

Network Security Best Practices Checks

- NAT Policies & Port Forwards
- Firewall Access Rules
- Inter-Zone Access Policies
- Wireless Configuration
- General Settings & Policies
- Users Management & Access Configuration
- Application Visualization & Control
- VPN Tunnel & SSL-VPN Configuration
- HTTP & WAN Management
- Logging Configuration

Security Services Status Checks

- Content Filtering Service (CFS)
- Gateway Anti-Virus (GAV)
- Intrusion Prevention Service (IPS)
- Anti-Spyware
- Geo-IP Filtering
- Botnet Filtering
- Deep Packet Inspection for SSL Traffic – DPI-SSL
- Deep Packet Inspection for SSH Traffic – DPI-SSH

The Security Health Check Service partner may also provide recommendations around the following areas:

- New service implementation (SSO, LDAP, Two-Factor Authentication)
- New product deployment and network integration
- Network segmentation, encryption in transit and remote access planning (Annex)
- Design best practice workshop planning
- Product migration and configuration translation

Out-Of-Scope Activities

The **Security Health Check** is designed to be a one-day, best-practice security evaluation and validation service. The scope of the service is determined based on size and complexity of customer environment.

As such, this service does not include on-site configuration optimization, with the possible exception of license syncronization or Capture ATP activation, should either be necessary. Remediation services are follow-up projects derived from conclusions of the Health Check Report.

The above in-scope activities will be treated as best effort and focus will be given to areas relevant to the customer environment and elements deemed higher priority.

Configuration of the following services is not included in the scope of this work, but can be offered as follow-up activities per customer request:

- General Configuration & Implementation
- Global VPN Client / SSL-VPN
- Sonic Point Configuration
- Single Sign-On (SSO)
- Comprehensive Anti-Spam Service
- GMS
- Analyzer
- Support Case Follow-Up & Fix
- LDAP/Radius Authentication
- WAN Acceleration
- Virtual Assist
- Enforced Client Anti-Virus
- Training
- Sandwich Firewall
- High-Availability / Clustering
- Product Feature Testing

Security Health Check Report

At the conclusion of this one-day service, the customer can expect to receive a report from their SonicWall Advanced Services Partner. This report will document the status of each of the security services and configurations that were checked and offer any recommendations for security posture improvements. The table below provides an example of such a report.

Sample Report: Security Health Check – NSA2600

BEST PRACTICES	PRE-ENGAGEMENT STATUS	RECOMMENDATIONS/IMPLEMENTED FIXES
General System Status	🟡	LDAP Connection should be changed to TLS. Currently running on unsecured 389.
Inter-Zone Access Policies	🟡	Delete unused Zones (such as WLAN, which had multiple Access Rules set on).
WAN Failover & Load Balancing	N/A	
Routing Policies	N/A	
NAT Policies/Port Forwards	🟡	External port-mapping (NAT w/ source = any) should be limited to known source IPs. External RDP connections for IT admin should not be allowed (instead, IPSec/SSL-VPN should be configured to allow access from the outside to RDP).
DHCP/DNS Configuration	🟡	As the first choice, an internal DNS Server IP should be set.
Wireless Configuration	N/A	
Firewall Access Rules	🟡	A review of existing rules should be done. On remaining rules, enable Geo-IP and Botnet protection services.
App Visualization & Control	🟢	Enabled, pending a reboot. This will allow further flow granularity views, such as inspect flows by country of origin.
Firewall Settings	🟡	Enable TCP/UDP/ICMP Flood Protection.
VPN Tunnel Configuration	N/A	
SSL-VPN Configuration	N/A	
Remote Management	N/A	
HTTP(S) Management	🟢	Keep HTTP Management disabled. Allow only HTTPS. Change HTTPS port to 8443 in case you want to use SSL-VPN in the future (that'll use TCP: 443).
Log/Syslog Configuration	🔴	Enforce minimum pass length should be changed from its default value of 1 to perhaps 8.
User & Access Configuration	🟡	Local syslog needs to be customized. Logging for each and every packet allowed will limit its usability. We've de-cluttered current syslog settings. Nonetheless, for longer history and better views, a better report solution should be adopted (e.g., GMS/Analyzer). Analyzer can be deployed, as current license set does contain an Analyzer license.
High Availability	N/A	User Access is done through SSO/LDAP. Case SR3974813 should be further pursued with support if the problem is still reproducible after the firmware upgrade.
Remote Access VPN	N/A	Central Site (NSA2600) should be provisioned with an HA setup that will provide redundancy and avoid single points of failure.

SECURITY SERVICES	PRE-ENGAGEMENT STATUS	RECOMMENDATIONS/IMPLEMENTED FIXES
Gateway Anti-virus	Partially Enabled	Configure: Enabled CIFS/NetBios
Intrusion Prevention Service	Enabled	Enable Detect All for High, Med, Low. Enable Prevent All for High, Med. Set Log Redundancy for High/Med to 30s
Anti-Spyware	Enabled	Enable Detect All for High, Med, Low. Enable Prevent All for High, Med. Set Log Redundancy for Low to 30s.
Geo-IP Filtering	Enabled	Block origin countries of suspicious traffic seen in the Logs where there is no legitimate business conducted.
Botnet Filtering	Disabled	Block connections to/from Botnet Command and Control Services with Enable Logging.
Content Filtering Service	Enabled	In addition to default blocked categories, block the following as well: Malware, Radicalization, Pay2Surf, Hacking & Proxy Avoidance.
DPI-SSL	Disabled	Subject to SonicWall Certificate distribution through AD, DPI-SSL is highly recommended. 65% of traffic is missed from scanning without DPI-SSL.
DPI-SSH	Disabled, Not licensed	SSH is the backbone for many configuration, file transfer and VPN services in the wild. Inspection of DPI-SSL traffic is highly recommended.
Capture ATP	Partially Enabled	CIFS and additional file types: PDF, Office, Archives. Block file until a verdict is returned.

Observations

- While on-site, we implemented some of the above recommended changes. However, most of them should be done during a change window with due-diligence in place (config/firmware backup taken before changes).
- Remote Access VPN is the preferred method to access internal/centralized resources (such as internal File Sharing facilities or internal Remote Desktop Servers). Such a solution will provide opportunity to enforce the client endpoint to: have the latest operating system patch or update applied; have the anti-virus/anti-spyware endpoint software enabled with the latest updates; and restrict resource access in the event the client endpoint does not meet all the security policy criteria.
- Proper network segmentation with intra-zone traffic scanning should further more limit any potential threat spread horizontally.

Summary

- Segmented networks will slow down data breach attacks.
- Preventing lateral movement is ideal as there is a bigger chance for a threat to be spotted if it stays in the system longer while having its harm capabilities diminished.
- Network segmentation will stop an unpatched and exploited system from accessing and infecting every machine in the network (typical for ransomware).

Takeaway

SonicWall can help deliver network segmentation, traffic encryption, intrusion detection and prevention, zero-day threat protection and global threat intelligence protection against data exfiltration and extortion.

These services can significantly reduce the attack surface around protected services and also reduce the number of assets falling in-scope of becoming PCI (or other equivalent standards) compliant.

Security Compliance Requirements

The Security Health Check Service can assist customers with PCI: DSS or GDPR compliance requirements.

PCI: DSS Security Compliance

Requirements

- Do not store sensitive authentication data once the card authorization process has been completed. Protect actual card number with encryption.
- Hardened card data storage must be protected within a defined security perimeter, through a specific set of controls maintaining network security.
- The network must also be segmented and protected, including separation of wireless networks with firewalls. Additional security elements such as intrusion detection and prevention, including other alerting mechanisms, are recommended.
- Remote access must use two-factor authentication. These extensive access controls must also be augmented by physical security countermeasures, including use of cameras and methods to monitor access to sensitive areas.
- You are required to undertake penetration testing, both annually and after major system changes. In addition, you need to undertake both internal (network and application) and external quarterly vulnerability scans.
- Your validation is only confirmation of your compliance at a single point in time. You need to ensure continual compliance to manage your ongoing risk of breach.

GDPR Security Compliance

- Audit current approach to managing data.
- Establish current position and existing processes around data protection
- Audit of all customer data sets held across the business, including areas where PII might NOT be adequately protected.

With SonicWall, you can:

- Implement network segmentation and security access gates between business modules
- Protect data on mobile devices and remote offices in a similar manner to centrally held data
- Secure remote access and encrypt data in transit
- Access policy enforcement across file-sharing and other network-shared services and assets

For additional details on SonicWall Partner-Enabled Service offerings visit www.sonicwall.com or contact your SonicWall Advanced Services Partner.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com