

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 Authorized 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 SonicWall specific 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 network optimization projects such as network migration to a more efficient network topology. This guide is intended to provide Authorized Services Partners and SonicWall customers with clear guidelines and expectations to ensure successful delivery of the Security Health Check Service.

In-Scope Activities

The **Security Health Check** is a one day service containing a review of existing configuration and the resulting best practice advisory around the 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 Antivirus - 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, 2-Factor)
- 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

Security Health Check Report











At the conclusion of this one-day service, the customer can expect to receive a report from their SonicWall Authorized Security 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

SECURITY SERVICES	PRE-ENGAGEMENT STATUS	RECOMMENDATIONS/IMPLEMENTED FIXES
Gateway Antivirus	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.

Sample Report: Security Health Check - NSA2600 Cont.

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.

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 go-through existing rules should be done, and on remaining rules, enable Geo-IP and Botnet protection services.
App Visualization & Control		Enabled, pending a Reboot. This will allow further flow granularity view, 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 Mgmt. disabled, allow only HTTPS. Change HTTPS port to 8443 in the light that you will want to use SSL-VPN in the future (that'll use TCP: 443). Enforce min. pass length should be changed from its default value of 1, to perhaps 8.
Log/Syslog 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 view, a better report solution should be adopted (such as GMS/Analyzer). Analyzer can be deployed, as current license set does contain an Analyzer license.
User & Access Configuration		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.
High Availability	N/A	Central Site (NSA2600) should be provisioned with an HA setup that will provide redundancy and avoid single point of failure.
Remote Access VPN	N/A	Depending on number of users, Central Site Remote Access can be deployed on a separate Appliance, to off-load Remote Access VPN off the existing NSA2600. Two Factor Authentication is a recommended option for such deployment. Please, see Observations below for more details.

Out-Of-Scope Activities

The Security Health Check is designed to be a one day best effort 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 onsite configuration optimization, with the possible exception of license synchronization 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 customer environment and to elements deemed higher priority.

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

- General Configuration and Implementation
- Global VPN Client / SSL-VPN
- Sonic Point Configuration
- Single-Sign-On
- Comprehensive Anti-span Service
- GMS
- Analyzer
- Support logged case follow-up and fix
- LDAP/Radius Authentication
- WAN Acceleration
- Virtual Assist
- Enforced Client Anti-Virus
- Training
- Sandwich Firewall
- High-Availability / Clustering
- Product feature testing

Observations:

- While on-site, we've operated 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 solution will provide opportunity to enforce the Client Endpoint to have the latest Operating System Patch/Update applied, to have the Antivirus/Antispyware Endpoint Software enabled with latest updates, and can restrict resource access in the event that 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

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 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.
- SonicWall can help with:
 - a) New Security Access Gates between business modules
 - b) Protect data on Mobile Devices & Remote Offices similar to data held centrally
 - c) New access policy enforcement across file sharing or other shared services or assets

For additional detail on SonicWall Partner Enabled Service offerings visit www.sonicwall.com or contact your SonicWall Authorized Services Partner.