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. This service will provide the customer with a comprehensive Health Check Report that will include findings and any recommended actions to be taken. This may include specific SonicWall configuration optimizations that identify the need for remediation work. The report will also provide 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 service activity typically consists of 1 day of consulting or project management services. The Activities will be limited to those stated herein.

The planned Activities include:

Pre-Deployment Steps
- Review existing network topology and configuration
- Create a valid design based on customer requirements

Reviewed Health Check Items
- Firmware Version
- Licensing
- NAT Policies & Port Forwards
- Review Validity and Security of each policy
- Access Rules
- Review Validity and Security of each rule
- Inter-Zone Access Policies

- Wireless Configuration (SonicWaves, SonicPoints, and Internal AP only)
- General Settings & Policies
- Users Management & Access Configuration
- Application Visualization & Control
- Enabling this feature will require a reboot, and must be completed by the customer prior to service engagement
- VPN Tunnel & SSL-VPN Configuration
- Logging Configuration
- 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
- Client Authentication Methods
- Single Sign On (SSO)

- LDAP
- Duo-Factor Authentication
- Network Configurations
- Network Segmentation
- Design Best Practices
- High Availability H/A
- Review of PCI-DSS Compliancy
- Review of GDPR Compliancy

Service Delivery
- Provide remote access capabilities to perform service delivery
- Verify inbound/outbound email is functioning properly
- Verify functionality of all configured features
- Provide a comprehensive review document of the Health Check Findings
- Services will be completed during normal business hours 0800 – 1700 hours Monday – Friday Local Standard Time

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

<table>
<thead>
<tr>
<th>SECURITY SERVICES</th>
<th>PRE-ENGAGEMENT STATUS</th>
<th>RECOMMENDATIONS/IMPLEMENTED FIXES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Anti-virus</td>
<td>Partially Enabled</td>
<td>Configure: Enabled CIFS/NetBios</td>
</tr>
<tr>
<td>Intrusion Prevention Service</td>
<td>Enabled</td>
<td>Enable Detect All for High, Med, Low. Enable Prevent All for High, Med. Set Log Redundancy for High/Med to 30s</td>
</tr>
<tr>
<td>Anti-Spyware</td>
<td>Enabled</td>
<td>Enable Detect All for High, Med, Low. Enable Prevent All for High, Med. Set Log Redundancy for Low to 30s.</td>
</tr>
<tr>
<td>Geo-IP Filtering</td>
<td>Enabled</td>
<td>Block origin countries of suspicious traffic seen in the Logs where there is no legitimate business conducted.</td>
</tr>
<tr>
<td>Botnet Filtering</td>
<td>Disabled</td>
<td>Block connections to/from Botnet Command and Control Services with Enable Logging.</td>
</tr>
<tr>
<td>Content Filtering Service</td>
<td>Enabled</td>
<td>In addition to default blocked categories, block the following as well: Malware, Radicalization, Pay2Surf, Hacking &amp; Proxy Avoidance.</td>
</tr>
<tr>
<td>DPI-SSL</td>
<td>Disabled</td>
<td>Subject to SonicWall Certificate distribution through AD. DPI-SSL is highly recommended. 65% of traffic is missed from scanning without DPI-SSL.</td>
</tr>
<tr>
<td>DPI-SSH</td>
<td>Disabled, Not licensed</td>
<td>SSH is the backbone for many configuration, file transfer and VPN services in the wild. Inspection of DPI-SSH traffic is highly recommended.</td>
</tr>
<tr>
<td>Capture ATP</td>
<td>Partially Enabled</td>
<td>CIFS and additional file types: PDF, Office, Archives. Block file until a verdict is returned.</td>
</tr>
<tr>
<td>BEST PRACTICES</td>
<td>PRE-ENGAGEMENT STATUS</td>
<td>RECOMMENDATIONS/IMPLEMENTED FIXES</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>General System Status</td>
<td></td>
<td>LDAP Connection should be changed to TLS. Currently running on unsecured 389.</td>
</tr>
<tr>
<td>Inter-Zone Access Policies</td>
<td></td>
<td>Delete unused Zones (such as WLAN, which had multiple Access Rules set on).</td>
</tr>
<tr>
<td>WAN Failover &amp; Load Balancing</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Routing Policies</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>NAT Policies/Port Forwards</td>
<td></td>
<td>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).</td>
</tr>
<tr>
<td>DHCP/DNS Configuration</td>
<td></td>
<td>As the first choice, an internal DNS Server IP should be set.</td>
</tr>
<tr>
<td>Wireless Configuration</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Firewall Access Rules</td>
<td></td>
<td>A review of existing rules should be done. On remaining rules, enable Geo-IP and Botnet protection services.</td>
</tr>
<tr>
<td>App Visualization &amp; Control</td>
<td></td>
<td>Enabled, pending a reboot. This will allow further flow granularity views, such as inspect flows by country of origin.</td>
</tr>
<tr>
<td>Firewall Settings</td>
<td></td>
<td>Enable TCP/UDP/ICMP Flood Protection.</td>
</tr>
<tr>
<td>VPN Tunnel Configuration</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>SSL/VPN Configuration</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Remote Management</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>HTTP(S) Management</td>
<td></td>
<td>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).</td>
</tr>
<tr>
<td>Log/Syslog Configuration</td>
<td></td>
<td>Enforce minimum pass length should be changed from its default value of 1 to perhaps 8.</td>
</tr>
<tr>
<td>User &amp; Access Configuration</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>High Availability</td>
<td>N/A</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>N/A</td>
<td>Central Site (NSA2600) should be provisioned with an HA setup that will provide redundancy and avoid single points of failure.</td>
</tr>
</tbody>
</table>

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.
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 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 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. Please note that additional fees may be incurred.

General SonicWall configuration and implementation activities

Configuring the below Appliance features which are covered by the Firewall Remote Implementation Services:

- Applications or Services on the Security Appliance
- Global VPN Client/SSL-VPN
- SonicWave, SonicPoint, and Internal Wireless
- SSO
- Comprehensive Anti-Spam Service
- LDAP/Radius Authentication
- WAN Acceleration
- Virtual Assistant
- Enforced Client Anti-Virus
- H/A Clustering
- Product Feature Testing
- Training
- Firewall Sandwich
- Support Case Follow-Up & Fix
- GMS/Analyzer
- Rebooting the firewall
- On-site services

Post-Implementation

- No post-implementation support is included. The customer should contact SonicWall support for product-related issues. Additional implementation support or management services (beyond 30 days) may be available for purchase (additional fees may apply).
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.

Prerequisites

• The customer shall ensure that the existing infrastructure and hardware configuration is sufficient to support the environment

• The customer shall commit a technical resource on a full-time basis to provide SonicWall or the Partner with the assistance required

• The customer environment is in a normal working configuration state without issues in the current firewall configuration

Other terms

• Customer must provide PCI and security compliance specifications for the PCI-DSS Firewall. SonicWall is not responsible for ensuring Customer’s compliance with data security and PCI requirements.

• Customer must provide GDPR Compliancy Specifications. The Health Check does not certify the Compliancy standards. Review must be completed by the reviewing compliancy organization.

• It is the customer’s responsibility to ensure it has the appropriate agreements with the provider of the Activities.

• The provision of the Activities does not include the development of any intellectual property. All right, title and interest arising from the performance of Activities shall vest in SonicWall.

• SonicWall and/or the provider of the Activities may require execution of additional documentation before performance of the Activities begin. This additional documentation may include (without limitation) dates for the work to begin. If the provider of the Activities can accommodate a change in schedule related to the Activities, the provider may require a two (2) week lead time (or more before Activities can be performed. If a customer makes any changes during or after the Activities begin, additional charges and/or schedule changes may apply.

• Only configured features publicly posted by SonicWall in the Datasheets may be configured.

• All Activities will be performed remotely utilizing the phone and web conferencing.

• The information provided herein is a general description of Activities. Any services delivered that are not explicitly outlined herein are not a part of this offer.

• The duration for the provision of Activities may vary based on many factors including, but not limited to, the complexity of the customer’s environment.

• SonicWall is not responsible for ensuring Customer’s compliance with data privacy, security and PCI requirements.

• Customer agrees that additional fees may be due and payable if Customer makes any such changes or otherwise fails to meet the prerequisites set forth herein.

• Only authorized SonicWall providers may provide the Activities described by this offer.

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.
© 2018 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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 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.
1033 McCarthy Boulevard
Milpitas, CA 95035

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