SONICWALL

SONICWALL SECURITY HEALTH CHECK-SERVICE

Stellen Sie sicher, dass Sie das Maximum aus Ihrer SonicWall-Investition herausholen, um Ihr Netzwerk optimal zu schützen

Überblick

Der SonicWall Security Health Check-Service bietet Kunden die Möglichkeit, ihr SonicWall-Netzwerksicherheitskonzept umfassend zu prüfen und mögliche Sicherheitslücken zu identifizieren. Der Advanced Services Partner stellt dem Kunden einen Health Check-Bericht mit den Ergebnissen und den empfohlenen Maßnahmen zur Verfügung. Dazu gehören etwa die Optimierung der SonicWall-Konfiguration im Rahmen von Folgeprojekten, aber auch allgemeinere bzw. netzwerkspezifische Optimierungsvorschläge, die Folgeprojekte wie etwa den Umstieg auf eine effizientere Netzwerktopologie nach sich ziehen können. Dieser Leitfaden bietet SonicWall-Kunden einen klaren Überblick über die im Security Health Check-Service enthaltenen Leistungen.

Enthaltene Leistungen

Beim eintägigen **Security Health Check**-Service werden die bestehenden Konfigurationen auf die Einhaltung von Best Practices in den nachfolgend aufgeführten Bereichen geprüft.

Allgemeine Prüfung der Appliance

- Firmwareversion und Prüfung neuer Releases
- Prüfung der Lizenz

Einhaltung von Best Practices im Bereich Netzwerksicherheit

- NAT-Richtlinien und Portweiterleitungen
- Firewall-Zugriffsregeln
- Zugriffsregeln zwischen Netzwerkzonen
- Wireless-Konfiguration
- Allgemeine Einstellungen und Regeln
- Benutzerverwaltung und Zugriffskonfiguration
- Anwendungsvisualisierung und -kontrolle
- VPN-Tunnel- und SSL-VPN-Konfiguration
- HTTP- und WAN-Verwaltung
- Loggingkonfiguration

Prüfung der Sicherheitsservices

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

Der Security Health Check-Servicepartner kann auch Empfehlungen in folgenden Bereichen aussprechen:

- neue Serviceimplementierung (SSO, LDAP, Zwei-Faktor-Authentifizierung)
- neue Produktimplementierung und Netzwerkintegration
- Netzwerksegmentierung, Verschlüsselung während der Datenübertragung und Planung des Remote-Zugriffs (Beispielbericht)
- Planung von Best-Practices-Workshops
- Produktmigration und Übertragung der Konfiguration

Nicht enthaltene Dienstleistungen

Der **Security Health Check** ist als eintägiger Service zur Evaluierung und Validierung der Best Practices rund um das Thema Sicherheit konzipiert.
Der Umfang der Leistungen richtet sich nach der Größe und Komplexität der Kundenumgebung.

Daher umfasst dieser Service keine Vor-Ort-Konfigurations-optimierung. Mögliche Ausnahmen sind – falls erforderlich – die Lizenzsynchronisierung oder die Aktivierung von Capture ATP. Optimierungsservices sind Folgeprojekte, die aufgrund des Health Check-Berichts angestoßen werden.

Die oben beschriebenen im Service enthaltenen Leistungen werden nach dem Best-Effort-Prinzip erbracht. Darüber hinaus konzentrieren wir uns auf die Bereiche, die für die Kundenumgebung relevant sind, sowie auf Elemente mit höherer Priorität.

Folgende Services sind nicht im Arbeitsumfang enthalten, können aber auf Kundenanfrage als Folgeleistung erbracht werden:

- Allgemeine Konfiguration und Implementierung
- Global VPN Client / SSL-VPN
- SonicPoint-Konfiguration
- Single-Sign-on (SSO)
- Comprehensive Anti-Spam Service
- GMS
- Analyzer
- Nachbearbeitung und Lösung von Supportanfragen
- LDAP-/Radius-Authentifizierung
- WAN-Beschleunigung
- Virtual Assist
- Enforced Client Anti-Virus
- Schulungen
- Firewall-Sandwich
- Hochverfügbarkeit/Clustering
- Testen der Produktfeatures

Security Health Check-Bericht

Nach Abschluss dieses eintägigen Services erhält der Kunde einen Bericht von seinem SonicWall Advanced Services Partner. Dieser enthält den Status der einzelnen geprüften Sicherheitsservices und Konfigurationen sowie Empfehlungen zur Verbesserung des Sicherheitskonzepts. Die unten stehende Tabelle dient als Beispiel für einen solchen Bericht.

Beispielbericht: Security Health Check – NSA2600

BEST PRACTISES	ZUSTAND VOR DEM SECURITY HEALTH CHECK	EMPFEHLUNGEN/DURCHGEFÜHRTE VERBESSERUNGEN
Allgemeiner Systemstatus	●	LDAP-Verbindung sollte zu TLS geändert werden. Läuft derzeit auf dem ungesicherten Port 389.
Zugriffsregeln zwischen Netzwerkzonen	●	Ungenutzte Zonen löschen (wie z. B. WLAN, das mehrere Zugriffsregeln aktiviert hat).
WAN-Failover und Lastverteilung	Nicht zutreffend	
Routing-Regeln	Nicht zutreffend	
NAT-Richtlinien / Portweiterleitungen	●	Mapping externer Ports (NAT mit Quelle = any) sollte auf bekannte Quell-IPs eingeschränkt werden. Externe RDP-Verbindungen für IT-Administratoren sollten nicht erlaubt sein (stattdessen sollte IPSec/SSL-VPN so konfiguriert sein, dass ein Zugriff von außen auf RDP möglich ist).
DHCP-/DNS-Konfiguration	●	Die beste Wahl wäre die Einrichtung einer internen DNS-Server-IP.
Wireless-Konfiguration	Nicht zutreffend	
Firewall-Zugriffsregeln	●	Die bestehenden Regeln sollten überprüft werden. Für die restlichen Regeln sollten Geo-IP- und Botnet-Schutz-Services aktiviert werden.
Anwendungsvisualisierung und -kontrolle	●	Aktiviert, Neustart ausstehend. Dies ermöglicht weitere detaillierte Einblicke in den Datenverkehr, z. B. die Prüfung des Datenverkehrs nach Ursprungsland.
Firewall-Einstellungen	●	TCP-/UDP-/ICMP-Flood-Schutz aktivieren.
VPN-Tunnel-Konfiguration	Nicht zutreffend	
SSL-VPN-Konfiguration	Nicht zutreffend	
Remote-Verwaltung	Nicht zutreffend	
HTTP(S)-Verwaltung	●	HTTP-Verwaltung weiterhin deaktiviert lassen, nur HTTPS erlauben. HTTPS-Port zu 8443 ändern, falls Sie künftig SSL-VPN nutzen möchten (dieses verwendet TCP 443).
Log-/syslog-Konfiguration	●	Die Mindestlänge für Passwörter sollte vom Standardwert 1 auf vielleicht 8 geändert werden.
Benutzer- und Zugriffskonfiguration	●	Das lokale syslog muss angepasst werden. Das Protokollieren jedes erlaubten Pakets schränkt die Usability ein. Wir haben die aktuellen syslog-Einstellungen übersichtlicher gestaltet. Um die Historie zu verlängern und die Übersicht zu optimieren, wäre dennoch eine bessere Berichtslösung erforderlich (z. B. GMS/Analyzer). Analyzer kann implementiert werden, da in den aktuellen Lizenzen eine Analyzer-Lizenz enthalten ist.
Hochverfügbarkeitsoptionen	Nicht zutreffend	Der Benutzerzugriff erfolgt über SSO/LDAP. Für SR3974813 ist weiterer Support nötig, falls das Problem nach dem Firmware-Upgrade immer noch reproduzierbar ist.
Remote-Access-VPN	Nicht zutreffend	Um Redundanz sicherzustellen und Single Points of Failure zu vermeiden, sollte die Firmenzentrale (NSA2600) mit einer HA-Lösung ausgestattet werden.

SICHERHEITSSERVICES	ZUSTAND VOR DEM SECURITY HEALTH CHECK	EMPFEHLUNGEN/DURCHGEFÜHRTE VERBESSERUNGEN
Virenschutz am Gateway	Teilweise aktiviert	Konfigurieren: CIFS/NetBios aktivieren
Intrusion-Prevention-Service	Aktiviert	„Detect All for High, Med, Low“ aktivieren „Prevent All for High, Med“ aktivieren Protokollredundanz für „High/Med“ auf 30 Sek. stellen
Anti-Spyware	Aktiviert	„Detect All for High, Med, Low“ aktivieren „Prevent All for High, Med“ aktivieren Protokollredundanz für „Low“ auf 30 Sek. stellen
Geo-IP-Filtering	Aktiviert	Ursprungsländer mit verdächtigem Verkehr blockieren, die in den Protokollen erscheinen und in denen keine Geschäftsaktivitäten stattfinden.
Botnet-Filtering	Deaktiviert	Verbindungen von/zu Botnet-Command-and-control-Services mit „Enable Logging“ blockieren.
Content Filtering Service	Aktiviert	Zusätzlich zu den standardmäßig blockierten Kategorien sollten auch die folgenden Kategorien blockiert werden: Malware, Radikalisierung, Pay2Surf, Hacking & Proxy-Umgehung.
DPI-SSL	Deaktiviert	Im Fall einer SonicWall-Zertifikatsverteilung durch AD ist DPI-SSL sehr zu empfehlen. Ohne DPI-SSL werden 65 % des Datenverkehrs nicht geprüft.
DPI-SSH	Deaktiviert, nicht lizenziert	SSH ist eine zentrale Komponente für viele Konfigurationen, Dateiübertragungen und VPN-Services „in the wild“. Die Prüfung von DPI-SSL-Verkehr ist sehr zu empfehlen.
Capture ATP	Teilweise aktiviert	CIFS und zusätzliche Dateitypen: PDF, Office, Archive. Datei bis zur Klärung des Sicherheitsstatus blockieren.

Beobachtungen

- Während unseres Einsatzes vor Ort haben wir einige der oben empfohlenen Änderungen implementiert. Allerdings sollte der Großteil von ihnen innerhalb eines Zeitfensters mit entsprechender Due-Diligence-Prüfung vorgenommen werden (Konfiguration/Firmware-Back-up vor den Änderungen durchgeführt).
- Remote-Access-VPN ist die bevorzugte Methode, um auf interne/zentrale Ressourcen zuzugreifen (z. B. interne Filesharing-Systeme oder interne Remote-Desktop-Server). Durch eine solche Lösung können Sie auf dem Client-Endpunkt den neuesten Patch bzw. das neueste Update für das Betriebssystem anwenden, die Anti-Virus-/Anti-Spyware-Endpunkt-Software mit den neuesten Updates versorgen und den Zugriff auf Ressourcen eingrenzen, falls der Client-Endpunkt nicht alle Sicherheitskriterien erfüllt.
- Eine geeignete Netzwerksegmentierung mit Prüfung des Datenverkehrs innerhalb von Zonen sollte eine horizontale Ausbreitung von Bedrohungen weiter eingrenzen.

Zusammenfassung

- Durch eine Segmentierung des Netzwerks lassen sich Datenlecks und Angriffe eindämmen.
- Es kommt besonders darauf an, eine seitliche Ausbreitung zu verhindern, da Bedrohungen mit größerer Wahrscheinlichkeit erkannt werden, wenn sie sich länger im System aufhalten, während ihre gefährlichen Funktionen abgeschwächt werden.
- Die Netzwerksegmentierung verhindert, dass ein ungepatchtes System, das angegriffen wurde, auf alle Rechner im Netzwerk zugreift und sie infiziert (das ist typisch für Ransomware).

Die wichtigsten Punkte

SonicWall hilft bei der Netzwerksegmentierung, der Entschlüsselung des Datenverkehrs und der Erkennung und Abwehr von Eindringversuchen. Darüber hinaus bietet SonicWall Schutz vor Zero-Day-Bedrohungen sowie vor globalen Angriffen, bei denen Daten herausgeschleust und Organisationen erpresst werden.

Diese Services können die Angriffsfläche bei geschützten Systemen um ein Vielfaches reduzieren. Außerdem sind weniger Ressourcen nötig, die den PCI-Standard (oder andere ähnliche Standards) erfüllen.

Security-Compliance-Anforderungen

Der Security Health Check-Service hilft Kunden bei ihren PCI-DSS oder DSGVO-Compliance-Anforderungen.

Security-Compliance – PCI-DSS

Anforderungen

- Speichern Sie keine sensiblen Authentifizierungsdaten, nachdem die Kartenautorisierung abgeschlossen ist. Schützen Sie die Kartennummer durch Verschlüsselung.
- Der verstärkte Kartendatenspeicher muss innerhalb einer festgelegten Sicherheitsgrenze durch einen bestimmten Satz an Netzwerksicherheitskontrollen geschützt werden.
- Das Netzwerk muss auch segmentiert und geschützt werden. Dazu gehört etwa die Trennung von Drahtlosnetzwerken mit Firewalls. Es werden auch zusätzliche Sicherheitselemente wie die Erkennung und Abwehr von Eindringversuchen einschließlich weiterer Warnmechanismen empfohlen.
- Für den Remote-Zugriff ist eine Zwei-Faktor-Authentifizierung erforderlich. Diese umfassenden Zugriffskontrollen müssen auch durch physische Sicherheitsmaßnahmen verstärkt werden, zum Beispiel durch Kameras und durch Überwachung des Zugriffs auf sensible Bereiche.
- Sie müssen jährlich sowie nach jeder größeren Systemänderung Eindringversuche durchführen. Darüber hinaus müssen Sie vierteljährlich sowohl interne (Netzwerk und Anwendung) als auch externe Prüfungen auf Schwachstellen vornehmen.
- Die Validierung bestätigt lediglich, dass Sie die Compliance zu einem bestimmten Zeitpunkt einhalten. Um das Risiko eines Datenlecks dauerhaft zu minimieren, müssen Sie eine kontinuierliche Compliance sicherstellen.

Security-Compliance – DSGVO

- Überprüfen Sie Ihren aktuellen Ansatz zur Datenverwaltung.
- Stellen Sie fest, welche aktuellen Richtlinien und Prozesse rund um den Datenschutz bestehen.
- Führen Sie Audits aller Kundendatensätze im Unternehmen durch, auch in solchen Bereichen, in denen personenbezogene Daten möglicherweise NICHT angemessen geschützt werden.

Mit SonicWall können Sie:

- Netzwerksegmentierung und Funktionen für einen sicheren Zugriff zwischen Business-Modulen implementieren
- Daten auf Mobilgeräten und in Außenstellen auf ähnliche Weise wie zentral gehaltene Daten schützen
- einen sicheren Remote-Zugriff gewährleisten und Daten während der Übertragung verschlüsseln
- über Filesharing- und andere über das Netzwerk bereitgestellte Services und Ressourcen hinweg auf die verwendeten Regeln zugreifen

Weitere Einzelheiten zu den SonicWall Partner Enabled Service-Angeboten erhalten Sie unter www.sonicwall.com oder bei Ihrem SonicWall Advanced Services Partner.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

Brochure-SecurityHealthCheck-IMAG-A4-MKTG868