SONICWALL

# SONICWALL SECURITY HEALTH CHECK SERVICE

**Ottimizza l'investimento nelle soluzioni SonicWall per proteggere la tua rete**

## Introduzione

Il servizio Security Health Check di SonicWall è concepito per fornire ai clienti una panoramica completa della propria struttura di sicurezza di rete SonicWall e individuare eventuali problemi da risolvere. L' Advanced Services Partner fornirà al cliente un Health Check Report contenente i risultati e le misure raccomandate da adottare. Queste possono includere sia ottimizzazioni di configurazioni SonicWall specifiche, che possono evolvere in progetti successivi di remediation, sia suggerimenti di ottimizzazione più generali o specifici della rete che possono dar luogo a progetti di follow-up come la migrazione della rete in una topologia più efficiente. Questa guida ha lo scopo di far comprendere in modo chiaro ai clienti SonicWall cosa include il Security Health Check Service.

## Attività incluse

Il **Security Health Check** è un servizio della durata di un giorno che esamina le configurazioni in essere per verificare che siano adottate le migliori pratiche nelle aree seguenti.

### Verifica dello stato complessivo delle appliance

- Versioni firmware e revisione delle nuove release
- Analisi delle licenze

### Verifica delle best practice per la sicurezza di rete

- Policy NAT e port forwarding
- Regole di accesso firewall
- Policy di accesso interzona
- Configurazione wireless
- Impostazioni e policy generali
- Gestione utenti e configurazione degli accessi
- Controllo e visualizzazione delle applicazioni
- Configurazione tunnel VPN e VPN SSL
- Gestione HTTP e WAN
- Configurazione del sistema di logging

### Verifica dello stato dei servizi di sicurezza

- Content Filtering Service (CFS)
- Gateway Anti-Virus (GAV)
- Intrusion Prevention Service (IPS)
- Antispyware
- Filtraggio GeoIP
- Filtraggio botnet
- Ispezione deep packet del traffico SSL (DPI-SSL)
- Ispezione deep packet del traffico SSH (DPI-SSH)

Il partner abilitato al servizio Security Health Check può anche fornire raccomandazioni relative alle aree seguenti:

- Implementazione di nuovi servizi (SSO, LDAP, autenticazione a due fattori)
- Installazione e integrazione nella rete di nuovi prodotti
- Segmentazione della rete, crittografia dei dati in transito e pianificazione dell'accesso remoto (vedi report allegato)
- Pianificazione di workshop sulle best practice di progettazione
- Migrazione dei prodotti e conversione della configurazione

## Attività non incluse

Il **Security Health Check** è ideato come servizio della durata di un giorno per la valutazione e la convalida delle misure di sicurezza in conformità alle best practice.
L'ambito del servizio viene determinato in base alle dimensioni e alla complessità dell'ambiente del cliente.

Questo servizio non comprende quindi l'ottimizzazione delle configurazioni in loco, fatta eccezione per l'eventuale sincronizzazione di licenze o l'attivazione di Capture ATP, qualora necessarie. I servizi di correzione (remediation) sono progetti successivi basati sulle conclusioni dell'Health Check Report.

Le suddette attività incluse saranno gestite al meglio per garantire la massima efficacia, con una particolare attenzione alle aree rilevanti per l'ambiente del cliente e agli elementi ritenuti di priorità assoluta.

L'ambito di questo intervento non include i seguenti servizi, che tuttavia possono essere offerti come attività di follow-up su richiesta del cliente:

- Configurazione e implementazione generale
- Global VPN Client / SSL-VPN
- Configurazione dei SonicPoint
- Single Sign-On (SSO)
- Comprehensive Anti-Spam Service
- GMS
- Analyzer
- Follow-up e risoluzione di una richiesta di assistenza
- Autenticazione LDAP/Radius
- Accelerazione WAN
- Virtual Assist
- Enforced Client Anti-Virus
- Formazione
- Firewall sandwich
- Alta disponibilità/clustering
- Verifica delle funzionalità del prodotto

## Report di Security Health Check

Al termine di questo servizio della durata di un giorno, il cliente riceverà un report dal proprio Advanced Services Partner di SonicWall in cui è documentata la situazione di ogni servizio di sicurezza e configurazione sottoposto a verifica. Il report conterrà anche dei suggerimenti per migliorare il proprio assetto di sicurezza. La tabella seguente illustra un esempio di questo report.

**Esempio di report: Security Health Check – NSA2600**

| BEST PRACTICE | STATO PRE-INTERVENTO | RACCOMANDAZIONI/SOLUZIONI IMPLEMENTATE |
|---|---|---|
| Stato generale del sistema | 🟡 | Modificare la connessione LDAP in TLS. Attualmente viene eseguita sulla porta non sicura 389. |
| Policy di accesso interzona | 🟡 | Cancellare le zone non utilizzate (come ad es. la WLAN, per la quale erano impostate diverse regole di accesso). |
| Failover WAN e bilanciamento del carico | N/D | |
| Policy di routing | N/D | |
| Policy NAT / port forwarding | 🟡 | Limitare il mapping di porte esterne (NAT con origine = qualsiasi) a IP da origine conosciuta. Le connessioni RDP dall'esterno per l'amministrazione IT non devono essere autorizzate (configurare invece IPSec/SSL-VPN per consentire l'accesso a RDP dall'esterno). |
| Configurazione DHCP/DNS | 🟡 | Come prima scelta si deve impostare un IP per il server DNS interno. |
| Configurazione wireless | N/D | |
| Regole di accesso firewall | 🟡 | Eseguire una verifica delle regole esistenti. Per le regole rimanenti, abilitare i servizi di protezione Geo-IP e Botnet. |
| Controllo e visualizzazione delle applicazioni | 🟢 | Abilitato, in attesa di un riavvio. Ciò consente di ottenere ulteriori viste granulari sul flusso, come ad esempio la possibilità di ispezionare i flussi di traffico in base al paese di origine. |
| Impostazioni firewall | 🟡 | Abilitare la protezione da flooding TCP/UDP/ICMP. |
| Configurazione tunnel VPN | N/D | |
| Configurazione VPN SSL | N/D | |
| Gestione remota | N/D | |
| Gestione HTTP(S) | 🟢 | Mantenere disabilitata la gestione HTTP. Abilitare solo HTTPS. Modificare la porta HTTPS in 8443 nel caso si voglia utilizzare VPN SSL in futuro (il quale utilizzerà TCP: 443). |
| Configurazione log/syslog | 🔴 | La lunghezza minima imposta della passphrase deve essere modificata dal valore predefinito 1 probabilmente al valore 8. |
| Configurazione utenti e accesso | 🟡 | Il syslog locale deve essere personalizzato. La creazione di log per ogni singolo pacchetto consentito limiterebbe la sua usabilità. Abbiamo ottimizzato le attuali impostazioni syslog, ma per ottenere una cronologia più lunga e viste migliori, è consigliabile adottare una soluzione di reporting migliore (ad es. GMS/Analyzer). È possibile utilizzare Analyzer in quanto il set di licenze attuale contiene una licenza Analyzer. |
| Alta disponibilità | N/D | L'accesso degli utenti è realizzato tramite SSO/LDAP. Se il problema è ancora riproducibile dopo l'aggiornamento del firmware, contattare l'assistenza per risolvere il caso SR3974813. |
| VPN di accesso remoto | N/D | Eseguire il provisioning del sito centrale (NSA2600) con una configurazione ad alta disponibilità per fornire ridondanza ed evitare singoli punti di guasto. |

| SERVIZI DI SICUREZZA | STATO PRE-INTERVENTO | RACCOMANDAZIONI/SOLUZIONI IMPLEMENTATE |
|---|---|---|
| Gateway Anti-Virus | Parzialmente abilitato | Configurare come segue: CIFS/NetBios abilitati |
| Servizio di prevenzione intrusioni | Abilitato | Abilitare Detect All for High, Med, Low.<br>Abilitare Prevent All for High, Med.<br>Impostare Log Redundancy for High/Med a 30 s |
| Antispyware | Abilitato | Abilitare Detect All for High, Med, Low.<br>Abilitare Prevent All for High, Med.<br>Impostare Set Log Redundancy for Low a 30 s. |
| Filtraggio GeoIP | Abilitato | Bloccare i paesi di origine del traffico sospetto elencati nei log con i quali non si hanno rapporti commerciali legittimi. |
| Filtraggio botnet | Disabilitato | Bloccare le connessioni da/verso servizi di comando e controllo botnet con Enable Logging. |
| Content Filtering Service | Abilitato | Oltre alle categorie bloccate di default, bloccare anche le seguenti: Malware, Radicalization, Pay2Surf, Hacking & Proxy Avoidance. |
| DPI-SSL | Disabilitato | Soggetto alla distribuzione del certificato SonicWall tramite AD; si consiglia vivamente l'uso di DPI-SSL. Senza DPI-SSL, il 65% del traffico non viene analizzato. |
| DPI-SSH | Disabilitato, nessuna licenza | SSH è l'elemento portante di molti servizi di configurazione, trasferimento di file e VPN. L'ispezione del traffico DPI-SSL è altamente consigliata. |
| Capture ATP | Parzialmente abilitato | CIFS e altri tipi di file: PDF, Office, archivi. Blocco del file finché non viene identificata la sua natura. |

## Osservazioni

- Durante la permanenza in loco abbiamo implementato alcune delle modifiche suggerite sopra indicate, ma la maggior parte di esse dovrebbe essere apportata in un intervallo di tempo con due-diligence in atto (con backup della configurazione/firmware prima di apportare le modifiche).
- La VPN con accesso remoto è il metodo consigliato per accedere alle risorse interne/centralizzate (come sistemi interni di condivisione file o remote desktop server interni). Una soluzione di questo tipo consente di applicare criteri per verificare che sul terminale client sia installata l'ultima patch o aggiornamento del sistema operativo e sia attivo il software antivirus/antispyware con gli aggiornamenti più recenti; nel caso in cui il terminale client non soddisfi tutti i criteri delle policy di sicurezza, verrà limitato l'accesso alle risorse.
- Una corretta segmentazione della rete, con analisi del traffico all'interno delle singole zone, dovrebbe inoltre limitare la diffusione orizzontale di potenziali minacce.

## Riepilogo

- Le reti segmentate consentono di attenuare gli attacchi con violazione dei dati.
- La soluzione ideale consiste nel prevenire i movimenti laterali, in quanto è più probabile riuscire a individuare una minaccia se questa rimane più a lungo nel sistema, riducendo al contempo la sua capacità di causare danni.
- La segmentazione della rete impedisce a un sistema privo di patch e compromesso di accedere alla rete e infettare tutte le macchine collegate (comportamento tipico di un ransomware).

## Punti chiave

SonicWall consente di fornire servizi di segmentazione della rete, crittografia del traffico, rilevamento e prevenzione delle intrusioni, protezione contro le minacce e protezione contro il furto e l'estorsione dei dati grazie a tecniche di intelligence delle minacce a livello globale.

Questi servizi possono ridurre notevolmente la superficie di attacco dei servizi protetti e il numero di asset che devono essere conformi a PCI (o ad altre norme equivalenti).

## Requisiti di conformità di sicurezza

Il servizio Security Health Check può supportare i clienti a soddisfare i requisiti di conformità PCI-DSS o GDPR.

### Conformità ai requisiti di sicurezza PCI-DSS

**Requisiti**

- Non memorizzare dati sensibili di autenticazione una volta completato il processo di autenticazione. Proteggere i numeri delle carte tramite crittografia.
- Un sistema potenziato di archiviazione dei dati delle schede deve essere protetto entro un perimetro di sicurezza definito, mediante una serie di controlli specifici, per garantire la sicurezza della rete.
- Anche la rete deve essere protetta e segmentata, inclusa la separazione delle reti wireless con i firewall. Si consiglia inoltre l'uso di elementi di sicurezza aggiuntivi, quali sistemi di rilevamento e prevenzione delle intrusioni e altri meccanismi di avviso.
- L'accesso remoto deve utilizzare l'autenticazione a due fattori. Questi esaustivi controlli degli accessi vanno integrati con contromisure di sicurezza fisiche quali telecamere e altri metodi per monitorare l'accesso ad aree sensibili.
- È necessario eseguire test di penetrazione un volta all'anno e dopo ogni modifica di sistema rilevante. Inoltre è necessario effettuare scansioni di vulnerabilità sia interne (rete e applicazioni) che esterne una volta ogni tre mesi.
- La convalida è solo una conferma della conformità in un momento specifico. Per gestire il rischio continuo di violazioni è necessario garantire una conformità continuativa.

### Conformità ai requisiti di sicurezza GDPR

- Controllare l'approccio corrente alla gestione dei dati.
- Stabilire la posizione attuale e i processi esistenti relativi alla protezione dei dati.
- Controllare tutti i set di dati dei clienti gestiti all'interno dell'azienda, incluse le aree in cui le informazioni personali (PII) potrebbero NON essere protette in modo adeguato.

## Con SonicWall è possibile:

- Implementare la segmentazione della rete e gateway di accesso sicuro tra i vari moduli aziendali
- Proteggere i dati sui dispositivi mobili e nelle filiali remote in modo simile a quelli nella sede centrale
- Proteggere l'accesso remoto e crittografare i dati in transito
- Applicare le policy a tutti i servizi di condivisione file e ad altre risorse condivise in rete

Per ulteriori dettagli sul servizio SonicWall Partner-Enabled Service visitare www.sonicwall.com o contattare il proprio SonicWall Advanced Services Partner.

## Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

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

Per maggiori informazioni consultare il nostro sito web.
**www.sonicwall.com**





Brochure-SecurityHealthCheck-IMAG-A4-MKTG868