SONICWALL®

SERVICE SECURITY HEALTH CHECK SONICWALL

L'optimisation totale de votre investissement SonicWall pour protéger votre réseau

Présentation

Le service Security Health Check de SonicWall offre aux clients la possibilité d'analyser entièrement leur système de sécurité réseau SonicWall et d'identifier toute lacune en matière de sécurité. Les Partenaires de services avancés fournissent à leurs clients un rapport Health Check comportant les résultats de l'analyse et les actions recommandées. Il peut s'agir de l'optimisation de configurations SonicWall spécifiques dans le cadre de projets de correction et de suivi, mais également de suggestions d'optimisation plus générales ou spécifiques à un réseau qui peuvent s'inscrire dans des projets de suivi, comme la migration vers une topologie de réseau plus efficace. Le présent guide a pour but de présenter en détail aux clients SonicWall ce qu'englobe le service Security Health Check.

Prestations incluses

Security Health Check est un service d'une journée qui vérifie les configurations existantes afin de garantir le respect des pratiques d'excellence dans les domaines suivants.

Vérification générale des appliances

- Version de firmware et vérification des nouvelles versions
- Vérification des licences

Respect des pratiques d'excellence en sécurité réseau

- Règles NAT et redirections de ports
- Règles d'accès du pare-feu
- Règles d'accès inter-zones
- Configuration sans fil
- Paramètres généraux et règles
- Gestion utilisateurs et configuration des accès
- Visualisation et contrôle applicatifs
- Tunnel VPN & configuration SSL-VPN
- Gestion HTTP et WAN
- Configuration de la journalisation

Vérification des services de sécurité

- Content Filtering Service (CFS)
- Antivirus de passerelle
- Service de prévention des intrusions (IPS)
- Anti-logiciels espions
- Filtrage Geo-IP
- Filtrage de botnets
- Inspection approfondie des paquets pour le trafic SSL – DPI-SSL
- Inspection approfondie des paquets pour le trafic SSH – DPI-SSH

Le partenaire du service Security Health Check peut également fournir des recommandations dans les domaines suivants :

- Implémentation de nouveaux services (SSO, LDAP, authentification à deux facteurs)
- Déploiement de nouveaux produits et intégration réseau
- Segmentation réseau, chiffrement en transit et planification de l'accès distant (annexe)
- Planification des pratiques d'excellence
- Migration de produits et transfert de configuration

Prestations non incluses

Le service **Security Health Check** est un service d'une journée conçu pour évaluer et valider les pratiques d'excellence en matière de sécurité.
Les prestations incluses dans le service sont déterminées par la taille et la complexité de l'environnement client.

Par conséquent, ce service n'inclut pas l'optimisation de la configuration sur site, avec exception possible, le cas échéant, pour la synchronisation de licence ou l'activation de Capture ATP. Les services de correction sont des projets de suivi issus des conclusions du rapport Health Check.

Les prestations incluses listées ci-dessus seront réalisées selon le principe du « best effort ». L'attention sera portée sur les domaines pertinents pour l'environnement du client ainsi que sur les éléments à priorité élevée.

La configuration des services suivants n'est pas incluse dans les prestations proposées, mais elle peut être réalisée dans le cadre d'un suivi, sur demande du client :

- Configuration générale et implémentation
- Global VPN Client / SSL-VPN
- Configuration Sonic Point
- Single Sign-On (SSO)
- Comprehensive Anti-Spam Service
- GMS
- Analyzer
- Suivi des dossiers de support et résolution
- Authentification LDAP/Radius
- Accélération WAN
- Virtual Assist
- Antivirus client appliqué
- Formation
- Pare-feu sandwich
- Haute disponibilité/clustering
- Tests des fonctionnalités produit

Rapport Security Health Check

Après exécution de ce service d'une journée, le client reçoit un rapport de son Partenaire de services avancés SonicWall. Ce rapport documente l'état de chacun des services de sécurité et de chacune des configurations vérifiées ainsi que toutes les recommandations applicables dans le cadre de la stratégie de sécurité. Le tableau ci-dessous est un exemple de ce type de rapport.

Exemple de rapport : Security Health Check – NSA2600

PRATIQUES D'EXCELLENCE	ÉTAT AVANT VÉRIFICATION	RECOMMANDATIONS/AMÉLIORATIONS APPORTÉES
État général du système		La connexion LDAP doit être basculée sur TLS. Actuellement sur le port 389 non sécurisé.
Règles d'accès inter-zones		Supprimer les zones non utilisées (par ex. WLAN, plusieurs règles d'accès activées).
Basculement et équilibrage de charge WAN	N/D	
Règles de routage	N/D	
Règles NAT/redirections de ports		Le mapping de ports externes (NAT avec source = any) doit être limité aux IP source connues. Les connexions RDP externes pour les administrateurs ne doivent pas être autorisées (le réseau IPSec/SSL-VPN doit être configuré de façon à permettre l'accès à RDP depuis l'extérieur).
Configuration DHCP/DNS		L'idéal est l'utilisation d'une adresse IP de serveur DNS interne.
Configuration sans fil	N/D	
Règles d'accès du pare-feu		Les règles existantes doivent être vérifiées. Pour les autres règles, activer les services de protection Geo-IP et Botnet.
Visualisation et contrôle applicatifs		Activés, en attente d'un redémarrage. Cela permet de connaître plus précisément les flux de données, notamment leur vérification par pays d'origine.
Paramètres de pare-feu		Activer la protection saturation TCP/UDP/ICMP.
Configuration tunnel VPN	N/D	
Configuration SSL-VPN	N/D	
Télégestion	N/D	
Gestion HTTP(S)		Laisser désactivée la gestion HTTP. Autoriser uniquement HTTPS. Modifier le port HTTPS sur 8443 si vous voulez utiliser SSL-VPN ultérieurement (qui utilise donc TCP 443).
Configuration Log/Syslog		Remplacer la valeur par défaut (1) pour la longueur minimale des mots de passe et choisir par exemple 8.
Configuration utilisateurs et accès		Le syslog local doit être personnalisé. La journalisation pour chacun des paquets autorisés va limiter son utilisabilité. Nous avons élagué les paramètres syslog actuels. Il convient néanmoins d'adopter une meilleure solution de reporting pour un historique plus approfondi et des vues améliorées (par ex. GMS/Analyzer). Analyzer peut être déployé, car la licence actuelle ne contient pas de licence Analyzer.
Haute disponibilité	N/D	L'accès utilisateur s'effectue via SSO/LDAP. Le cas SR3974813 nécessite davantage de support si le problème est toujours reproductible après mise à jour du firmware.
VPN accès distant	N/D	Le site central (NSA2600) doit être équipé d'une configuration HA qui assurera la redondance et évitera les points de défaillance.

SERVICES DE SÉCURITÉ	ÉTAT AVANT VÉRIFICATION	RECOMMANDATIONS/AMÉLIORATIONS APPORTÉES
Antivirus de passerelle	Partiellement activé	Configurer : activer CIFS/NetBios
Service de prévention des intrusions	Activé	Activer l'option Detect All for High, Med, Low. Activer l'option Prevent All for High, Med. Définir la redondance de journalisation pour High/Med sur 30 sec.
Anti-logiciels espions	Activé	Activer l'option Detect All for High, Med, Low. Activer l'option Prevent All for High, Med. Définir la redondance de journalisation pour Low sur 30 sec.
Filtrage Geo-IP	Activé	Bloquer les pays d'origine du trafic suspect détectés dans les journaux et dans lesquels aucune activité légitime n'est réalisée.
Filtrage de botnets	Désactivé	Bloquer les connexions de/vers Botnet Command and Control Services avec Enable Logging.
Content Filtering Service	Activé	Outre les catégories bloquées par défaut, bloquer également : malware, radicalisation, Pay2Surf, piratage et anonymiseurs.
DPI-SSL	Désactivé	Selon distribution de certificat SonicWall via AD, DPI-SSL est hautement recommandé. Sans DPI-SSL, 65 % du trafic échappe à l'analyse.
DPI-SSH	Désactivé, pas de licence	SSH est la base de nombreux services de configuration, de transfert de fichiers et de services VPN « in the wild ». L'inspection du trafic DPI-SSL est hautement recommandée.
Capture ATP	Partiellement activé	CIFS et autres types de fichiers : PDF, Office, archives. Bloquer le fichier jusqu'au verdict.

Observations

- Pendant l'intervention sur site, nous avons implémenté certaines des modifications recommandées ci-dessus. Pour la majorité d'entre elles, il faut toutefois opérer sur une fenêtre de temps appropriée avec vérification préalable (sauvegarde config/firmware avant modifications).
- Le VPN d'accès distant est la méthode privilégiée pour accéder aux ressources internes/centralisées (par ex. systèmes de partage de fichiers ou serveurs internes Bureau à distance). Avec une solution de ce type, vous pouvez utiliser sur le terminal client le correctif ou la mise à jour de système d'exploitation les plus récents, activer les logiciels antivirus/anti-logiciels espions avec les dernières mises à jour et limiter l'accès aux ressources si le terminal client ne répond pas à tous les critères de sécurité.
- Une segmentation réseau appropriée avec analyse du trafic intrazone doit permettre de limiter encore toute propagation horizontale des menaces.

Résumé

- La segmentation du réseau permet de diminuer les failles de données et les attaques.
- Il est particulièrement important d'empêcher toute propagation latérale car les chances de détecter une menace sont plus grandes si elle reste dans le système plus longtemps tandis que ses capacités nuisibles sont diminuées.
- La segmentation du réseau empêche qu'un système non équipé de correctifs et pris pour cible n'accède et n'infecte chacune des machines du réseau (ce qui est typique des ransomwares).

Ce qu'il faut retenir

Les solutions SonicWall permettent la segmentation du réseau, le chiffrement du trafic ainsi que la détection et la prévention des intrusions. Elles protègent également des menaces zero-day et des attaques globales qui pratiquent l'exfiltration et l'extortion des données.

Ces services peuvent considérablement réduire la surface d'attaque pour les systèmes protégés ainsi que diminuer le nombre de ressources nécessaires pour assurer la conformité à la norme PCI (ou autres normes équivalentes).

Conditions requises de sécurité et de conformité

Le service Security Health Check permet de faciliter la mise en conformité des clients avec les normes PCI- DSS ou RGPD.

Mise en conformité PCI-DSS

Conditions requises

- Ne stockez aucune donnée d'authentification sensible une fois que le processus d'authentification de carte est terminé. Protégez le numéro de carte à l'aide du chiffrement.
- Le stockage renforcé des données de carte doit être protégé dans un périmètre de sécurité défini, via un ensemble spécifique de contrôles assurant la sécurité du réseau.
- Le réseau doit également être segmenté et protégé, et cela inclut la séparation des réseaux sans fil avec pare-feux. Il est recommandé d'utiliser des éléments de sécurité supplémentaires comme la détection et la prévention des intrusions, avec notamment des mécanismes d'alerte.
- L'accès distant doit utiliser l'authentification à deux facteurs. Ces contrôles d'accès étendus doivent également être renforcés par des mesures de sécurité physiques, notamment l'utilisation de caméras et de méthodes de surveillance des accès aux domaines sensibles.
- Vous devez effectuer des tests d'intrusion une fois par an et après chaque modification majeure du système. Tous les trimestres, vous devez aussi effectuer des analyses de vulnérabilité internes (réseau et application) et externes.
- Votre validation sert simplement à confirmer le respect de la conformité à un moment défini. Vous devez veiller au respect continu de la conformité afin de réduire durablement le risque de faille.

Conformité avec la norme de sécurité RGPD

- Vérifiez votre approche actuelle en matière de gestion des données.
- Déterminez les principes appliqués et les processus existants pour la protection des données.
- Procédez à des audits de tous les ensembles de données clients dans l'entreprise, y compris dans les domaines pour lesquels les données d'identification personnelle (PII) risquent de ne PAS être protégées de manière adéquate.

Avec SonicWall, vous pouvez :

- implémenter la segmentation réseau et des fonctions d'accès sécurisé entre les modules métier
- protéger les données sur les appareils mobiles et les bureaux distants de la même manière que les données centralisées
- sécuriser l'accès distant et chiffrer les données en transit
- accéder aux règles appliquées via le partage de fichiers et autres services et ressources partagées sur le réseau

Pour plus de détails sur les offres Partenaires de services SonicWall, consultez le site : www.sonicwall.com ou contactez votre Partenaire de services avancés SonicWall.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

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

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Brochure-SecurityHealthCheck-IMAG-US-MKTG868

SONICWALL®