DÉCHIFFREMENT ET INSPECTION DU TRAFIC CHIFFRÉ

Protection hautes performances contre l'usage malveillant du chiffrement

Selon le Rapport SonicWall 2018 sur les cybermenaces, le trafic chiffré représente aujourd'hui près de 70 % des communications Web d'une organisation. Malgré les nombreux avantages du chiffrement des sessions Internet, comme la protection de la confidentialité et de l'intégrité des informations personnelles dans l'échange de données, on constate également l'émergence d'une tendance moins favorable qui consiste à exploiter ce même chiffrement pour dissimuler des logiciels malveillants. Non seulement les agresseurs peuvent contourner les pare-feux et profiter d'angles morts pour infiltrer des malwares qui leur ouvrent grand les portes d'un réseau, mais ils utilisent aussi TLS/SSL pour cacher du trafic C&C et manipuler ainsi les systèmes compromis de quasiment n'importe où. Ne pas inspecter le trafic chiffré revient à négliger une bonne partie de la valeur de son système de pare-feu. C'est renoncer à voir ce qu'il se passe sur ce trafic, repérer les téléchargements de logiciels malveillants, identifier les fichiers nuisibles ou la transmission non autorisée d'informations confidentielles vers des systèmes externes.

Les organisations peuvent protéger leur réseau face à ces risques grâce à l'inspection approfondie des paquets sur TLS/SSL (DPI SSL), un service complémentaire SonicWall disponible sur tous les pare-feux nouvelle génération et appliances de sécurité réseau UTM (Unified Threat Management) SonicWall. Pour assurer une protection évoluée contre les menaces chiffrées, DPI SSL s'appuie sur le moteur RFDPI breveté de SonicWall (Reassembly-Free Deep Packet Inspection), qui analyse un vaste éventail de protocoles de chiffrement – HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS ou encore POPS – quel que soit le port utilisé.

Ce service déchiffre le trafic TLS/SSL, y recherche les menaces puis le rechiffre pour l'envoyer vers sa destination en l'absence de menaces ou de vulnérabilités. C'est un service particulièrement utile pour assurer une sécurité vitale, contrôler les applications et prévenir les fuites de données.

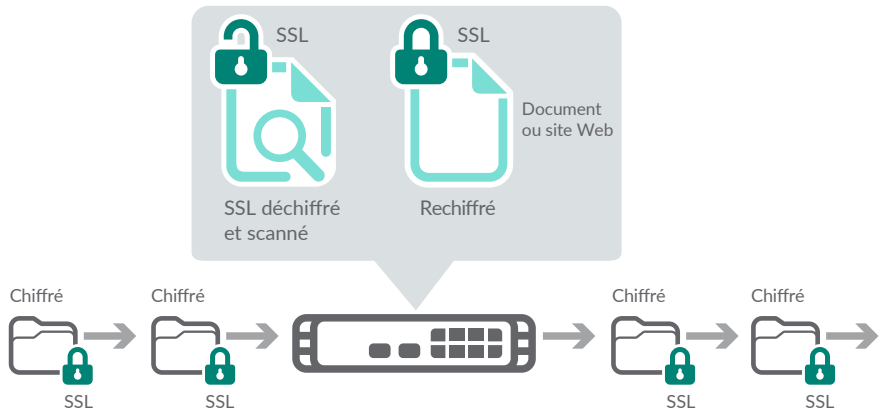
Fonctionnalités

Haute performance et nombre de connexions : les pare-feux de nouvelle

Ce service fournit des fonctionnalités essentielles de sécurité, de contrôle applicatif et de prévention des fuites de données par l'analyse du trafic HTTPS et autres formes de chiffrement TLS/SSL.

Avantages :

- Gain de visibilité sur le trafic chiffré TLS/SSL
- Blocage des téléchargements de logiciels malveillants dissimulés
- Mise en échec des communications C&C et de l'exfiltration de données
- Personnalisation de listes d'inclusion/exclusion pour répondre à des exigences de conformité ou légales



Configuration requise

L'inspection TLS/SSL est disponible avec les pare-feux SonicWall suivants :
SOHO / SOHO W
TZ300 / TZ300 W / TZ300P
TZ400 / TZ400 W
TZ500 / TZ500 W
TZ600 / TZ600P
NSa 2650
NSa 3650
NSa 4650
NSa 5650
NSa 6650
NSa 9250
NSa 9450
NSa 9650
SuperMassive 9800
NSsp 12400
NSsp 12800
NSv 10
NSv 25
NSv 50
NSv 100
NSv 200
NSv 300
NSv 400
NSv 800
NSv 1600

Partner Enabled Services
Vous avez besoin d'aide pour planifier, déployer et optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous offrir des services professionnels de premier ordre. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

génération SonicWall s'appuient sur une architecture de processeurs avancée et sur un très grand nombre de connexions pour améliorer la performance DPI-SSL et la protection sur tous les appareils connectés.

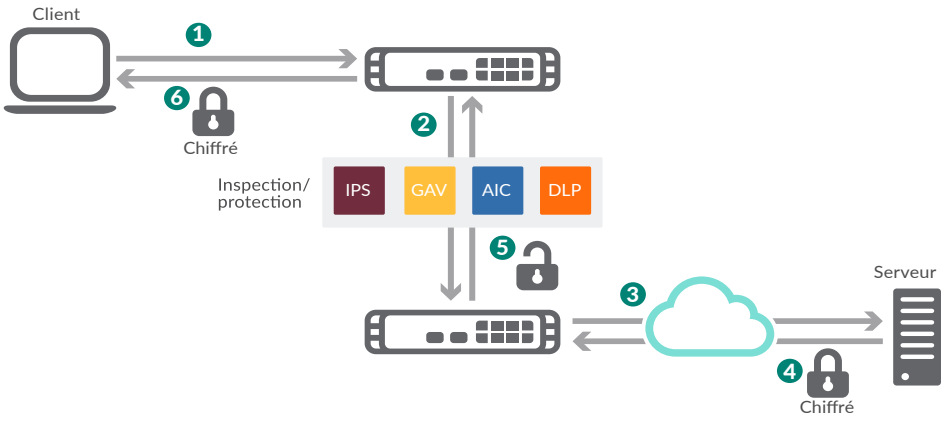
Configuration simple et sécurisée : le service de déchiffrement et d'inspection DPI SSL protège les utilisateurs du réseau avec un minimum de configuration et en toute simplicité.

Liste d'inclusion/exclusion : pour les déploiements à fort trafic, les administrateurs peuvent exclure des sources fiables afin d'optimiser les performances réseau. Ils peuvent aussi cibler un certain trafic à soumettre à l'inspection TLS/SSL en personnalisant une liste qui spécifie des objets ou des groupes d'adresses, de services ou d'utilisateurs afin de respecter des exigences de confidentialité et/ou légales.

Mode de déploiement client : inspecte le trafic TLS/SSL lorsque le client est sur le LAN du pare-feu et accède à des contenus situés sur le WAN. Une fois que l'appliance a déchiffré et inspecté le trafic, elle réécrit le certificat envoyé par le serveur distant et signe le certificat généré à l'aide du certificat spécifique à l'utilisateur. Par défaut, il s'agit de l'autorité de certification de l'appliance (CA), mais il est possible de sélectionner un certificat différent.

Mode de déploiement serveur : inspecte le trafic TLS/SSL lorsque des clients à distance se connectent via le WAN pour accéder à des contenus situés sur le LAN du pare-feu, permettant à l'administrateur de configurer des jumelages entre un objet d'adresse et un certificat. Lorsque l'appliance détecte des connexions TLS/SSL vers l'objet d'adresse, elle présente le certificat jumelé et négocie la connexion TLS/SSL avec le client. Dans ce cas de figure, le détenteur du pare-feu de nouvelle génération SonicWall possède les certificats et les clés privées des serveurs de contenu d'origine.

Services de support complets : ils comprennent la prévention des intrusions et des logiciels malveillants, le contrôle applicatif, le filtrage de contenu/d'URL et la prévention des communications C&C.



Inspection TLS/SSL – mode de déploiement client

1. Le client initie un handshake TLS/SSL avec le serveur
2. Le pare-feu de nouvelle génération demande et établit une session avec ses propres certificats à la place du serveur
3. Le pare-feu de nouvelle génération initie un handshake TLS/SSL avec le serveur pour le compte du client avec le certificat TLS/SSL défini par l'administrateur
4. Le serveur termine le handshake et établit un tunnel sécurisé entre lui-même et le pare-feu de nouvelle génération
5. Le pare-feu de nouvelle génération rechiffre le trafic et l'envoie au client
6. Le pare-feu déchiffre et inspecte tout le trafic en provenance ou à destination du client à la recherche de menaces et de violations des règles

Configuration requise

L'inspection TLS-SSL est disponible avec les pare-feux de nouvelle génération SonicWall suivants :

PARE-FEU	LICENCE UNIQUE
SOHO / SOHO W	01-SSC-0723
TZ300 / TZ300 W	Incluse dans l'abonnement aux services de sécurité
TZ400 / TZ400 W	Incluse dans l'abonnement aux services de sécurité
TZ500 / TZ500 W	Incluse dans l'abonnement aux services de sécurité
TZ600 / TZ600P	Incluse dans l'abonnement aux services de sécurité
NS*a* 2650	Incluse dans l'abonnement aux services de sécurité
NS*a* 3650	Incluse dans l'abonnement aux services de sécurité
NS*a* 4650	Incluse dans l'abonnement aux services de sécurité
NS*a* 5650	Incluse dans l'abonnement aux services de sécurité
NS*a* 6650	Incluse dans l'abonnement aux services de sécurité
NS*a* 9250	Incluse dans l'abonnement aux services de sécurité
NS*a* 9450	Incluse dans l'abonnement aux services de sécurité
NS*a* 9650	Incluse dans l'abonnement aux services de sécurité
SuperMassive 9800	Incluse dans l'abonnement aux services de sécurité
NS*sp* 12400	Incluse dans l'abonnement aux services de sécurité
NS*sp* 12800	Incluse dans l'abonnement aux services de sécurité
NSv 10	Incluse dans l'abonnement aux services de sécurité
NSv 25	Incluse dans l'abonnement aux services de sécurité
NSv 50	Incluse dans l'abonnement aux services de sécurité
NSv 100	Incluse dans l'abonnement aux services de sécurité
NSv 200	Incluse dans l'abonnement aux services de sécurité
NSv 300	Incluse dans l'abonnement aux services de sécurité
NSv 400	Incluse dans l'abonnement aux services de sécurité
NSv 800	Incluse dans l'abonnement aux services de sécurité
NSv 1600	Incluse dans l'abonnement aux services de sécurité

À propos de nous

SonicWall s'engage depuis plus de 27 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 automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

DataSheet-DecryptionAndInspection-US-VG-MKTG4095