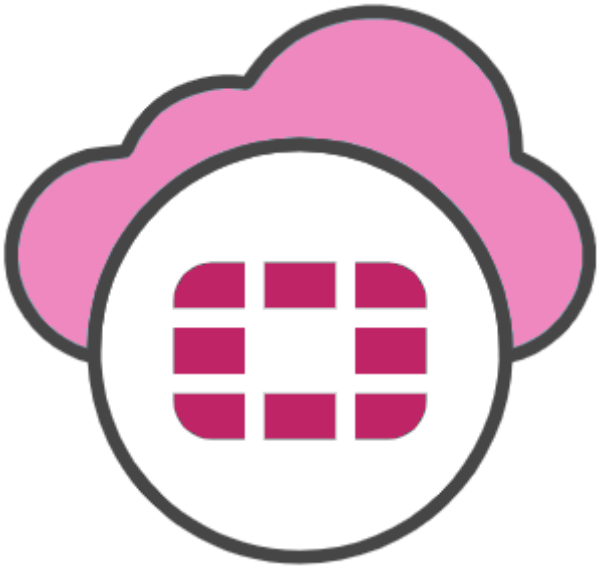
SMART TELECOM



CLOUD FIREWALL

La sécurité de vos connexions à Internet
et de vos ressources partagées

Immeuble le Périclès, 27 avenue des Béthunes – 95310 Saint Ouen l'Aumône
Tél. 01 34 02 44 04 – Fax 01 34 02 44 08 – www.smart-telecom.fr

S.A.S au capital de 66680 € – RCS PONTOISE 431 409 028

TABLE DES MATIERES

INTRODUCTION

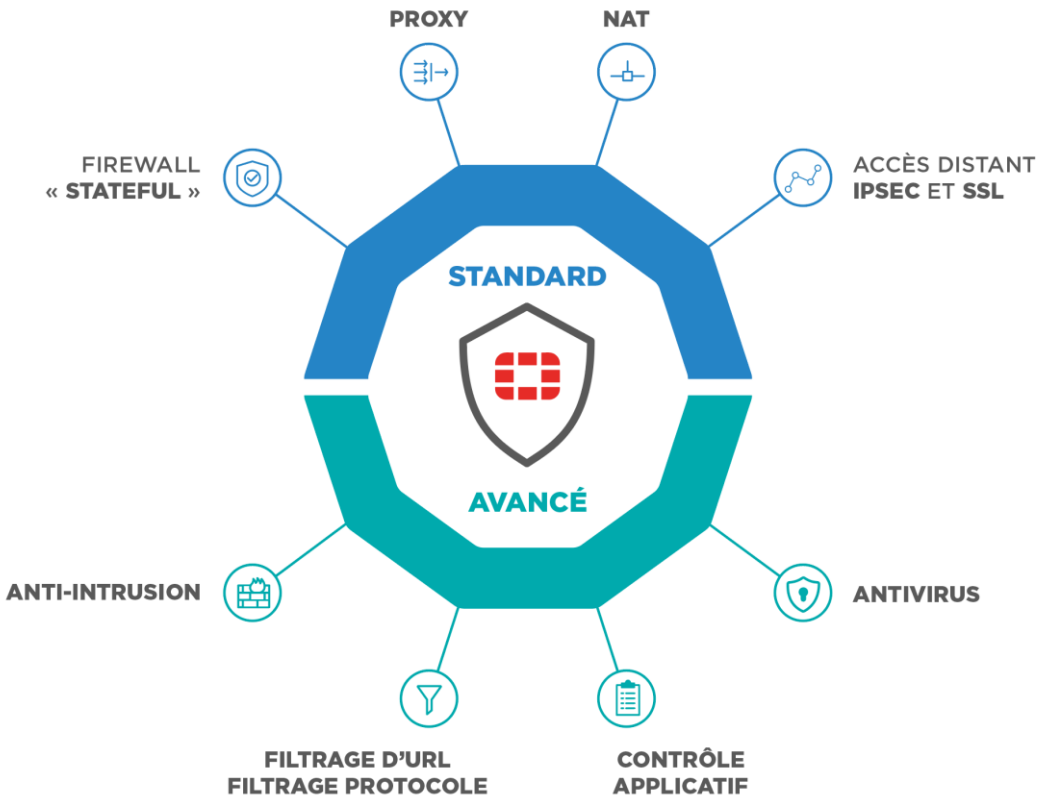
L'offre de sécurité « Cloud Firewall » de Smart Télécom s'appuie sur un cluster de firewalls « Fortinet » en haute-disponibilité, hébergé et centralisé en cœur de réseau, afin de proposer un fonctionnement de type « **Firewall As A Service** », disponible pour l'ensemble des liens d'accès et machines virtuelles proposés.

Son rôle principal est de **maitriser les flux** et bloquer les accès non autorisés, rôle qui se complexifie avec le temps et l'apparition de nouvelles menaces et techniques d'évasions ainsi que l'augmentation du volume de données et de la diversité des moyens d'accès.

Les principales fonctionnalités disponibles sur ce service sont les suivantes :

- Pare-feu à états (Firewall Stateful)
- Translation d'adresses et de ports (NAT/PAT)
- Proxy
- VPN IPSec et SSL
- IPS (Intrusion Prevention System)
- Antivirus
- Contrôle des applications
- Filtrage web

Ces fonctionnalités sont réparties en 2 niveaux de services, standard et avancé.



La gestion du Firewall s'appuie sur des ASIC NP (Network Processor) qui permettent d'accélérer de manière matérielle le traitement des données. Ce positionnement, unique sur le marché de la sécurité, offre ainsi la meilleure garantie de disposer de performances, et cela quel que soit la

taille des paquets. L'utilisation d'ASIC apporte aussi une latence de traitement la plus faible du marché.

De plus, FortiOS, le système d'exploitation de Fortinet, permet de gérer facilement des politiques de sécurité qui peuvent être composées de plusieurs milliers de règles. L'utilisation de « glisser/déposer », de menus contextuels, des recherches intelligentes et les diverses possibilités d'annotation, facilité au quotidien le travail des administrateurs.

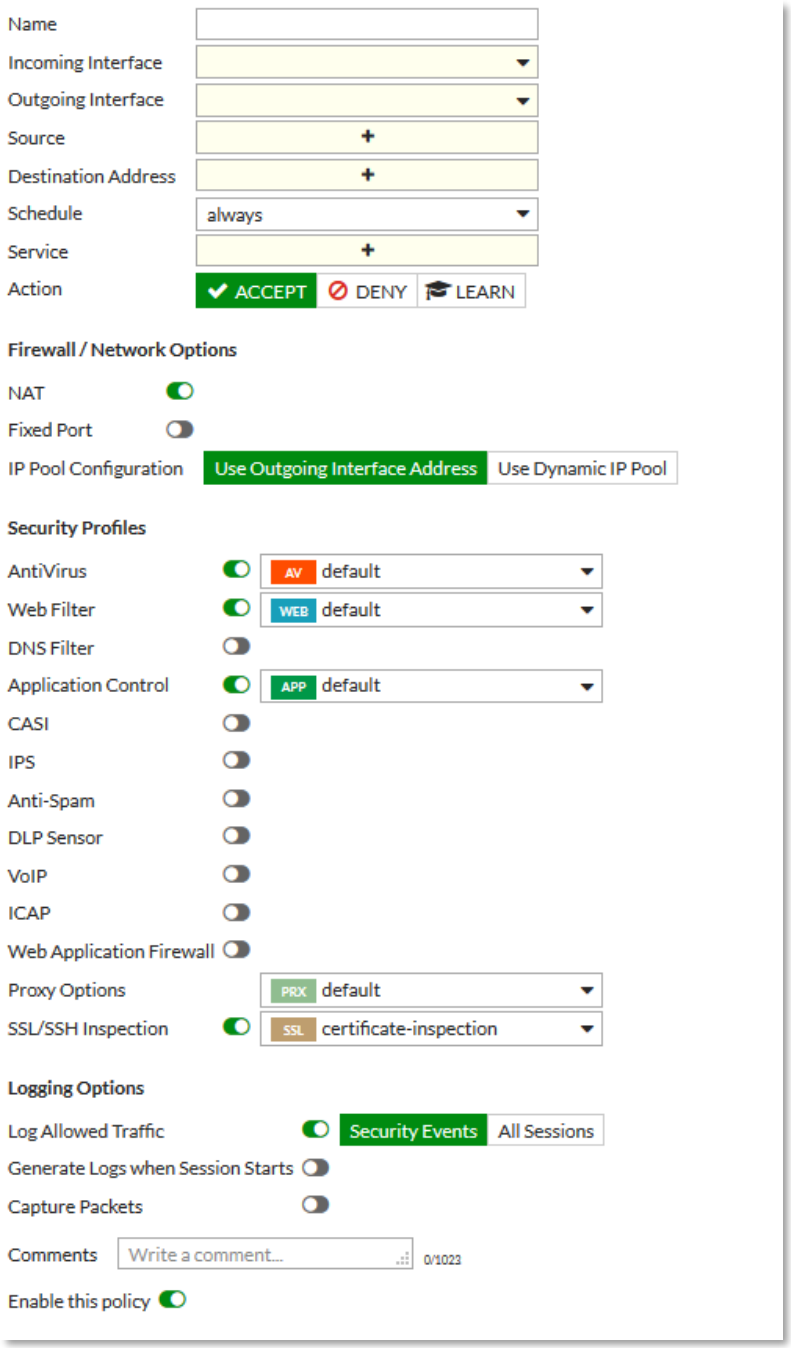
L'offre Cloud Firewall vous donner directement accès à l'interface de gestion « FortiOS » de Fortinet, et vous permet d'accéder en toute autonomie à la configuration et à l'administration de votre politique de sécurité.

CONFIGURATION D'UNE POLITIQUE DE SECURITE

Une politique de sécurité est constituée d'un ensemble de règles de Firewall.

Les règles sont analysées de haut en bas, en fonction d'un certain nombre de critères, tels que les interfaces source/destination, les IP/utilisateurs/machines source/destination, les services ou encore une notion temporelle de validité des règles.

Ci-dessous une copie d'écran montrant les principaux éléments de configuration d'une règle de Firewall :



Les critères permettant de « matcher » une règle sont les interfaces sources et destinations, les adresses IP/machines/utilisateurs sources, les adresses IP destinations, le service et la plage horaire.

FONCTIONNALITES STANDARD

FIREWALL « STATEFUL »

Le Firewall de FortiOS est de type « Stateful inspection ». Il permet ainsi de contrôler et d'appliquer des règles par session, ceci afin d'améliorer la sécurité et les performances de traitement par rapport à un Firewall « Stateless » qui va traiter les paquets de manière unitaire.

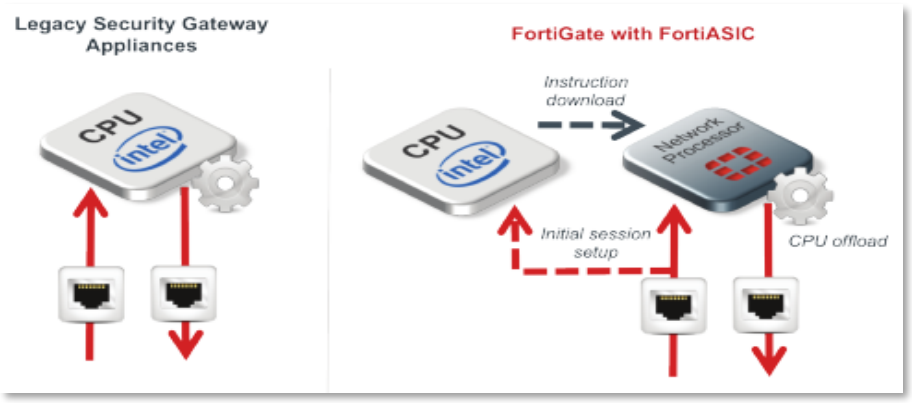
Pour toute nouvelle session acceptée, l'équipement FortiGate ajoute une entrée dans un cache de connexions actives ultra-rapide. Par la suite, les paquets interceptés sont immédiatement acceptés s'ils correspondent à des sessions valides présentes dans le cache.

Le moteur d'analyse Firewall sait reconnaître la plupart des protocoles s'appuyant sur des canaux de signalisations et de données comme le protocole FTP. Son rôle consiste alors à collecter les informations décrivant le canal de données qui est en train d'être négocié afin de le préenregistrer dans le cache de connexions valides. Dans ce cas, même le paquet d'ouverture du canal de données sera immédiatement accepté grâce à l'entrée présente dans ce cache.

PERFORMANCES ET ACCELERATION MATERIELLE

A la réception d'un paquet, le Firewall va l'analyser afin d'en extraire les informations nécessaires à son traitement comme par exemple les adresses IP source et destination ou encore le protocole. Le Firewall va alors déterminer le traitement à lui appliquer, s'il appartient à une session existante ou pas, le bloquer ou l'autoriser avec potentiellement une analyse complémentaire (Antivirus, IPS, contrôle applicatif, …).

Une fois la session établie au niveau du Firewall, tous les paquets suivants vont être traités non plus par la CPU mais par un ASIC Network Processor. Les avantages sont multiples : décharger le processeur qui peut être utilisé pour d'autres tâches, accélérer le traitement des données et garantir des performances quelle que soit l'application.



TRANSLATIONS D'ADRESSES (NAT) ET DE PORTS (PAT)

FortiOS supporte tous les mécanismes de NAT :

- **Source NAT :** pour masquer les adresses IP sources des paquets sortants. Dans le cas le plus simple, l'adresse IP source originale est remplacée par l'adresse IP de l'interface du Firewall par laquelle le paquet est routé. Mais il est bien sûr possible de choisir une adresse IP de

remplacement spécifique ou même de piocher l'adresse IP de remplacement parmi un groupe d'adresses IP.

- **Destination NAT :** pour remplacer les adresses IP destinations des paquets entrants. Ce mode de translation très complet dispose d'extensions comme le NAPT (Network Address and Port Translation) et le NAPT conditionnel (en fonction des adresses IP sources
- Un même paquet peut être à la fois translaté en source et en destination.

Ces fonctionnalités de NAT peuvent être gérées de manière très granulaire au niveau des règles de Firewall ou bien de manière centrale au niveau de la Central NAT Table. Les mécanismes de NAT sont applicables en mode transparent et en mode routé. La fonction de NAT est complètement supportée dans un contexte VPN : un flux entrant ou sortant d'un tunnel peut être translaté en source et/ou en destination. L'équipement FortiGate supporte les technologies de NAT IPv6.

PROXY TRANSPARENT OU EXPLICITE

FortiGate peut être utilisé comme un proxy transparent ou explicite pour le trafic IPv4 et IPv6. Dans le cas d'un proxy explicite, l'IP du FortiGate doit être déclarée dans les navigateurs des clients.

Dans cette configuration, le FortiGate est capable de mettre en cache sur son disque des pages WEB ou des objets afin d'améliorer les performances de la navigation WEB. La mise en cache WEB ne supporte pas les flux audio, vidéo et les contenus de type « streaming ». Il est possible de définir des exceptions pour des sites ne devant pas être mis en cache

ACCES DISTANTS (VPN)

Deux types de VPN sont décrits dans cette partie bien que d'autres modes soient également disponibles comme les VPN PPTP ou L2TP ou encore GRE. Actuellement, les VPN de type IPsec et SSL sont les plus couramment utilisés pour leurs avantages respectifs.

Fonctionnalités du VPN SSL

HTTPS est un protocole basé sur SSL (Secure Sockets Layer) qui est pris en charge par la plupart des navigateurs web pour l'échange d'informations sensibles en toute sécurité entre un serveur et un client Web. SSL établit un lien chiffré et veille à ce que toutes les données transmises entre le serveur Web et le navigateur client restent privées et sécurisées. L'avantage de cette solution VPN réside principalement dans le fait qu'un client lourd n'a pas besoin d'être installé sur le poste client et que le protocole HTTPS, facile d'utilisation, est couramment autorisé à passer au travers des équipements de sécurité.

Trois modes existent dans la configuration d'un tunnel VPN SSL :

- **Le mode tunnel** : la liaison VPN SSL est effectuée entre un client élaboré (navigateur + activeX, client lourd...) et la passerelle SSL qui décapsule les flux avant de les router vers leur destination. Tous les protocoles IP peuvent être tunnelisés en garantissant ainsi une compatibilité parfaite avec le réseau existant.
- **Le mode portail web :** la liaison VPN SSL est effectuée entre un client simple (navigateur) et la passerelle SSL qui présente un portail web à l'utilisateur. Celui-ci peut ensuite initier des flux depuis ce portail et la passerelle devient alors le client de ces requêtes. En fonction des applications clientes disponibles sur le portail, certaines ressources deviennent accessibles à l'utilisateur ainsi qu'un environnement virtuel. Des fonctions complémentaires peuvent

agrémenter le portail web comme les bookmarks, une personnalisation des liens, des messages d'accueil, etc…

- **Le mode port-forwarding**: le mode tunnel fournit un accès niveau 3 au réseau interne et à toutes les applications mais il nécessite l'installation d'un client. Le mode web quant à lui limite les applications disponibles. Le mode port-forwarding est une solution intermédiaire pour laquelle un port d'écoute est configuré sur le poste de l'utilisateur. Le module VPN SSL redirige ces flux capturés dans le tunnel SSL à destination de la passerelle qui les déchiffre et les transmet au serveur correspondant. Le module de port-forwarding fonctionne avec un applet Java, qui est téléchargé et exécutée sur l'ordinateur de l'utilisateur. L'applet fournit également des statistiques sur les flux envoyés et reçus.

Fonctionnalités du VPN IPsec

FortiOS supporte les tunnels VPN IPsec dont la phase1 est basée sur le protocole IKE (version 1 ou 2) ainsi que les fonctions de « *NAT Traversal* » pour la négociation des paramètres du tunnel, l'authentification, la génération des clefs de chiffrement des données, l'établissement du tunnel et le protocole ESP pour la transmission des données (ip-protocol 50).

Toutes ces fonctions sont réalisées au travers des FortiASIC implantés dans les équipements et peuvent ainsi bénéficier d'une accélération matérielle et d'un niveau de performance accrue. Grâce à la performance du hardware, le niveau de sécurité peut être renforcé sans dégradation des performances globales du système. Le FortiOS supporte les algorithmes de chiffrement et d'authentification élevés tels que AES256, SHA512 ou les groupes Diffie Hellmann 1 à 21.

Les standards IPsec sont bien entendu respectés tout en conservant une grande souplesse de configuration par le support de différents modes de configuration :

- IKE mode config
- mode Policy server pour les tunnels « *Dialup* » des utilisateurs nomades
- fourniture automatisée des adresses au travers du tunnel (DHCP over IPsec)

La configuration des tunnels est facilitée par des assistants de configuration en 3 à 5 étapes basées sur des modèles de configuration avec des équipements Fortinet ou tiers.

Client VPN pour postes clients

Les utilisateurs distants peuvent utiliser le logiciel FortiClient pour initier un tunnel VPN SSL et se connecter au réseau interne. FortiClient utilise le port TCP local 1024 pour établir une connexion chiffrée SSL avec le FortiGate, sur le port TCP 443. Lors de cette connexion, le FortiGate authentifie la demande du FortiClient VPN SSL basée sur les options de groupes d'utilisateurs. Le FortiGate établit un tunnel avec le client et lui attribue une adresse IP virtuelle. Une fois le tunnel établi, l'utilisateur peut accéder au réseau derrière le FortiGate. Le logiciel FortiClient est disponible au téléchargement sur www.forticlient.com pour les OS Windows, Mac OS X, Apple iOS et Android.

Clients VPN pour Terminaux Mobiles

Le FortiClient existe également en version mobile pour Android, Windows et iOS.

FONCTIONNALITES AVANCEES

ANTIVIRUS

L'Antivirus, développé par Fortinet, fournit une solution complète et intégrée au Firewall afin d'éliminer un large spectre d'attaques et d'activités malicieuses incluant les virus, les chevaux de Troie, les vers, les spyware, les botnets, les graywares ou encore les adwares. L'Antivirus Fortinet utilise une double détection basée à la fois sur une base de signatures et via un algorithme d'analyse heuristique.

Le haut niveau de performance du moteur est notamment dû au langage CPRL « Content Pattern Recognition Language » permettant d'accélérer le scan Antivirus ainsi qui la détection d'anomalie.

Protocoles analysés

FortiGate est capable de scanner un grand nombre de protocoles :

- HTTP
- HTTPS (Avec déchiffrement SSL)
- SMTP
- POP3
- IMAP
- MAPI
- FTP
- NNT

Ainsi que certains formats de compression fréquemment utilisés notamment dans le cadre de techniques d'évasions :

- GZIP
- RAR
- IZH
- IHA
- CAB
- ARJ
- ZIP

La performance

Le FortiASIC Content Processor assiste le CPU dans l'analyse des flux pour identifier et bloquer les menaces. Cet ASIC permet notamment d'accélérer le scan qu'il soit à base de signature ou d'heuristique. Les boîtiers FortiGate bénéficiant du FortiASIC CP bénéficient de performances améliorées.

Inspection en mode « Flow »

En plus du mode proxy standard d'analyse Antivirus, FortiGate embarque un moteur d'analyse dit « à la volée » ou « flow ». Ce mode signifie que le FortiGate sera capable d'analyser les flux et les fichiers indépendamment de leur taille. De plus, le mode « Flow » est également capable de scanner les fichiers compressés.

CONTROLE DES APPLICATIONS OU APPLICATION CONTROL

La reconnaissance des flux applicatifs est basée sur l'analyse en temps réel du trafic et la mise en correspondance avec une base de données de signatures embarquées sur l'équipement et référençant plus de 3500 applications. Cette base est mise à jour via le service FortiGuard.

La gestion du filtrage applicatif est réalisée à partir de la définition de profils contenant un ou plusieurs filtres de détection. Les profils peuvent être utilisés de manière très souple et granulaire en les appliquant au niveau d'une règle de Firewall, offrant ainsi une inspection différenciée par règle.

Chaque filtre est défini soit sur une sélection d'applications parmi la base mise à jour en permanence via FortiGuard (contenant actuellement plus de 3500 applications) soit sur la base de la sélection d'un groupe d'applications avec les critères de sélection suivants :

- Catégories (Botnet, Game, FileSharing, P2P, Business …)
- Editeurs (AOL, Adobe, Google, Apple, IBM, Cisco, Citrix, …)
- Technologies (Browser-Based, Client-Server, Network-Protocol, Peer-to-Peer)
- Protocoles (BO, DCERPC, DHCP, DNP3, DNS, FTP, H323, HTTP, SIP, SSH, SMTP …)
- Popularité (de 1 à 5)

Pour chaque filtre, plusieurs actions sont possibles : autoriser, surveiller, bloquer, envoyer un reset.

Le profil est ensuite associé à une politique de sécurité, comme c'est également le cas pour les autres fonctionnalités avancées, ce qui permet de contrôler très finement les comportements des applications.

FILTRAGE D'URL ET FILTRAGE PROTOCOLAIRE

Le filtrage Web est utilisé pour contrôler les requêtes des utilisateurs vers les sites Internet.

Le contrôle de la navigation permet d'éviter :

- La perte de productivité liée aux employés accédant à Internet pour des raisons personnelles ou non liées à l'activité de l'entreprise.
- La congestion réseau : Lorsqu'une grande partie de la bande passante est consommée pour de mauvaises raisons, les applications légitimes en souffrent.
- La perte ou l'exposition d'informations confidentielles à travers des sites de chat, des systèmes de messagerie non approuvés ou des partages en « peer to peer ».
- L'augmentation des risques d'exposition aux menaces liées à l'utilisation de site douteux.
- La responsabilité légale de l'entreprise liée à l'accès ou au téléchargement de contenus protégés ou illégaux.

Les différents modes de filtrage

Les équipements FortiGate disposent de plusieurs types de filtrage :

- Filtrage par URL,
- Filtrage par catégories (FortiGuard),
- Filtrage des contenus,

- Filtrage des scripts.

Il est possible d'utiliser les différents types de filtrage simultanément sur les flux associés.

Filtrage par URL

Cette méthode permet d'autoriser, d'interdire, de surveiller ou d'exempter une URL ou un domaine de tout autre contrôle.

Les entrées peuvent-être soit une URL simple et unique, soit s'appliquer un ensemble d'URL en utilisant des métas caractères (Wildcard ou expressions régulières). Il s'agit en fait de listes blanches et de listes noires avec un fonctionnement plus riche qu'en simple mode tout ou rien.

Filtrage par catégories

Il s'agit d'un mode de filtrage basé sur des catégories d'URL fournies par FortiGuard. Les bénéfices de ce mode de filtrage sont multiples. D'une part, les équipes de FortiGuard Labs travaillent 24h sur 24 afin d'assurer des mises à jour constantes des bases de données permettant d'avoir ainsi un classement au plus près de la réalité. D'autre part, la gestion des serveurs qui fournissent la base de données des pages web classifiées est effectuée par Fortinet et n'est plus à la charge de l'entreprise. Celle-ci s'affranchit ainsi de l'installation d'un serveur sur le réseau local, de son exploitation et de sa maintenance.

Fonctionnement du filtrage FortiGuard

Le FortiGate intercepte les requêtes Web des utilisateurs et détermine s'ils sont en droit de consulter la page. Les serveurs FortiGuard maintiennent une base de données de plusieurs centaines de millions de pages.

Lorsqu'un navigateur Web interroge une URL, la requête est traitée par le réseau comme suit :

1. L'équipement FortiGate intercepte la requête sur le réseau local.
2. Si le FortiGate a déjà en cache le nom de la catégorie correspondant à la page Web, ce nom est immédiatement comparé à ceux des catégories autorisées.
3. Si cette catégorie est autorisée, la requête Web est transmise au site cible. Si le nom de la catégorie n'est pas en cache, la requête Web n'est pas transmise au site cible, et une demande de classification est transmise simultanément à un serveur FortiGuard.
4. Le FortiGate reçoit du serveur FortiGuard le nom de la catégorie à laquelle appartient la page. Cette catégorie est comparée à la liste des catégories autorisée. En parallèle, le FortiGate reçoit les données du site Web interrogé.
5. Si la politique est d'autoriser la consultation de cette page, la réponse du site Web est transmise à l'utilisateur. Sinon, un message de remplacement personnalisable lui est envoyé, et l'événement est enregistré en log.

Le système FortiGuard dispose de 78 catégories classées dans 6 groupes principaux :

- Risques de Sécurité
- Intérêt Général – Business
- Intérêt Général – Personnel
- Contenu Adulte
- Consommation de bande passante
- Legal / Potentiellement Responsable

Cette liste est consultable à l'adresse suivante :

http://www.fortiguard.com/static/webfiltering.html

La configuration des droits d'accès associés à chaque catégorie se fait simplement au niveau de profil de filtrage web, où pour chaque catégorie et/ou chaque groupe, il suffit de définir l'action correspondante :

- Accès autorisé
- Accès interdit (blocage)
- Accès surveillé (log)
- Accès authentifié (SSO ou connexion)
- Accès éduqué (message d'attention)
- Accès limité (quota)

Filtrage des contenus

Il est possible de contrôler le contenu des pages auxquelles les utilisateurs accèdent en bloquant les sites qui contiennent des mots ou des modèles de mots spécifiques. Cela prévient l'accès à des pages avec des contenus douteux.

Cette analyse est configurée à travers des filtres de contenu, définis par la correspondance avec des mots, des phrases, des métas caractères et des expressions régulières de type « Perl ». Chaque profil de filtrage Web peut disposer de son propre filtre de contenu. Cette fonction de filtrage analyse le contenu de chaque page accédée.

L'administrateur spécifie une liste de mots, de phrases ou d'expressions bannie et associe à chaque élément de la liste une valeur numérique, ou un score, dépendant de l'importance de chaque occurrence de la liste.

A chaque fois que le système de filtrage de contenu rencontre une correspondance dans une page, il augmente le score de la page, si la valeur de la somme finale du score de la page est supérieure au seuil défini par l'administrateur, la page sera bloquée.

Filtrage des scripts et options du proxy

Les fonctions de filtrage permettent pour chaque profil de filtrage Web de positionner des options au niveau du proxy (non disponible en mode DNS ou flux). Il y a de nombreuses options de sécurité tel que :

- Forcer les recherches sécurisées sur les moteurs de recherche
- Filtres Youtube
- Logger toutes les mots clefs de recherche
- Bloquer les URLs invalides
- Effectuer des filtrages d'URL par paternes simples, regular expressions ou Wildcards
- Bloquer les URLs malicieuses découvertes par la FortiSandbox
- Recherche de mots clefs dans les URLs
- Evaluer les URLs par domaine et adresse IP
- Bloquer les redirects HTTP en fonction de leur réputation
- Evaluer les images en fonction des URLs et les remplacer si nécessaire

D'autres options de filtrage sont disponibles comme :

- Restreindre l'utilisation des comptes Google à des domaines spécifiques
- Afficher les détails des erreurs HTTP des séries 400 et 500
- Bloquer les POST HTTP
- Supprimer les applets Java, Cookies et ActiveX

Mise en place d'une politique de filtrage web

Comme l'ensemble des fonctions d'analyse approfondie associées aux Firewalls de nouvelle génération, le filtrage Web se configure en associant un profil Web à une règle de Firewall.

Il est possible de distinguer les règles en fonction de l'identité des utilisateurs, de la source, de la destination etc.

C'est notamment au niveau du profil que l'administrateur va définir les catégories et les actions associées, les listes blanches et noires (filtrage par URL), les options éventuelles de filtrage du contenu et les options avancées.

ANTI INTRUSION IPS (INTRUSION PREVENTION SYSTEM)

Le module IPS intégré à FortiOS permet de protéger les réseaux contre les attaques des cybers criminels en analysant le trafic et en bloquant les menaces avant qu'elles puissent atteindre des ressources potentiellement vulnérables.

La partie IPS de FortiGuard permet ainsi de bloquer 190 000 tentatives d'intrusion chaque minute. La base de protection embarque plus de 15000 règles utilisées dans plus de 7500 signatures et chaque semaine une centaine de règles sont mises à jour ou créées.

Le module IPS est composé de différentes fonctionnalités activables à la demande et facilement configurables, et ceci de manière granulaire. Ces fonctionnalités sont la détection d'anomalies protocolaires et la gestion de sondes IPS.

Le module IPS peut être déployé et utilisé de manière très flexible dans différents environnements, en mode routé ou transparent, ou encore en mode « one-arm » ou « sniffer ». Il s'appuie sur la technologie FortiASIC afin de rendre un service de protection efficace, s'appuyant sur le centre de recherche FortiGuard, tout en assurant de très hautes performances et une latence extrêmement faible.

Configuration d'une sonde IPS

La configuration de l'IPS est basée sur la notion de sondes IPS, et est réalisée de manière très souple et granulaire en associant une sonde IPS à une règle de Firewall, la même sonde pouvant être associée, si besoin, à plusieurs règles de Firewall.

S'il est souhaité d'avoir une analyse IPS plus globale et non lié spécifiquement à une règle de Firewall, il est également possible d'appliquer un profil IPS à des règles dites « interface policies » et dont l'objectif est de permettre d'appliquer globalement des profils de protection tels que l'IPS, le DLP ou le filtrage web.

Une sonde IPS est constituée d'un ensemble de filtres paramétrables et ordonnés. Chaque filtre peut être facilement configuré sur la base de différents critères proposés ou bien en spécifiant explicitement les signatures à intégrer au filtre. Chaque filtre est également associé à une action.

Les critères sont les suivants :

- **La sévérité** : critique, haute, moyenne, basse, information ;
- **La cible** : client, serveur;
- **L'OS** : BSD, Linux, MacOS, Solaris, Windows et autre ;
- **L'application** : Adobe, Apache, Apple, CGI_app, Cisco, HP, IBM, IE, IIS, Mozilla, MS_Office, Novell, Oracle, PHP_app, Sun, ASP_app, CA, DB2, IM, Ipswitch, MailEnable, MediaPlayer, MS_Exchange, MSSQL, MySQL, Netscape, P2P, PostgreSQL, Real, Samba, SAP, SCADA, Sendmail, Veritas, Winamp, autre ;
- **Les protocoles** : DNS, FTP, HTTP, ICMP, IMAP, LDAP, POP3, SCCP, SIP, SMTP, SNMP, SSH, SSL, TCP, UDP, BO, DCERPC, DHCP, DNP3, H323, IM, MSSQL, NBSS, NNTP, P2P, RADIUS, RDT, RPC, RTCP, RTP, RTSP, TELNET, TFN, autre.

Pour chaque filtre, les actions possibles sont :

- Appliquer le paramétrage par défaut défini par Fortinet
- Surveiller
- Bloquer
- Bloquer avec envoi d'un reset
- Mise en quarantaine pendant une durée paramétrable

Détection d'anomalies protocolaires et décodeurs

Le module IPS embarqué dans FortiOS embarque également des fonctionnalités de détection d'anomalies protocolaires et de décodeur. Cela permet de bloquer des données malformées permettant ainsi de protéger les ressources situées derrière l'équipement FortiGate d'attaque de ce type. Par exemple, le décodeur protocolaire HTTP va permettre d'identifier les paquets HTTP ne respectant pas les standards du protocole HTTP.

Fail open

Si, pour une quelconque raison, le module IPS cessait de fonctionner, il est configuré pour passer par défaut en mode « fail open », laissant alors passer le trafic sans analyse IPS, ceci afin de permettre au Firewall de continuer de fonctionner sans bloquer le trafic légitime. Dans ce cas, nous sommes dans des environnements où la productivité est préférée à la sécurité. Dans le cas contraire, pour plus de sécurité, il est possible de configurer le module IPS en mode « fail closed », le trafic étant alors bloqué tant qu'il n'a pas été soumis à une analyse IPS.

Une protection IPS efficace, testée et certifiée

Le module IPS, comme les autres modules de protection embarquée dans FortiOS, est basé sur notre service FortiGuard qui fournit à nos clients en temps réel les dernières défenses contre les menaces. FortiGuard fournit des mises à jour en continu du moteur et de la base de signatures embarquées sur un équipement FortiGate. Le travail du centre de recherche FortiGuard va permettre de se protéger très efficacement des menaces non connues en mettant à jour la base IPS au plus tôt, idéalement avant l'apparition des premiers exploits.