Forcepoint

Fiche technique

Prévention des intrusions avec le Firewall nouvelle génération de Forcepoint

Forcepoint propose un système de prévention des intrusions (IPS) parmi les plus efficaces du marché. Il est conçu pour protéger les réseaux d'entreprise distribués – en étendant sa protection aux centres de données, aux bureaux distants, à vos succursales et au cloud.

Les solutions de sécurité réseau de Forcepoint vous permettent de profiter de l'un des systèmes de prévention des intrusions les plus robustes du secteur. Le Firewall nouvelle génération de Forcepoint – qui a obtenu la meilleure note lors de tests réalisés par des organismes indépendants – peut être déployé en tant qu'appareil autonome IPS de niveau 2 ou en comme composant d'un Firewall Next-Gen complet de niveau 3, qu'il s'agisse d'environnements physiques, virtuels ou du cloud. Les Firewalls neutralisent les fuites, les failles de sécurité et les malwares que les hackers utilisent pour pénétrer et se propager dans les réseaux d'entreprise.

Une architecture unique, optimisée pour être plus efficace, plus rapide

Le Firewall nouvelle génération de Forcepoint se fonde sur une approche de l'inspection basée sur les flux dynamiques, qui va bien au-delà de la simple inspection des paquets. Il reconstruit et examine les charges réelles, mettant ainsi en échec les techniques d'évasion qui camouflent les failles de sécurité et les malwares.

En outre, le décryptage granulaire à grande vitesse démasque les attaques qui tentent de se dissimuler au sein du trafic SSL/TLS. Forcepoint analyse chaque flux de données, décodant les différentes couches de protocoles pour rechercher des configurations de protocoles, de métadonnées et d'en-têtes anormaux ou mal formés.

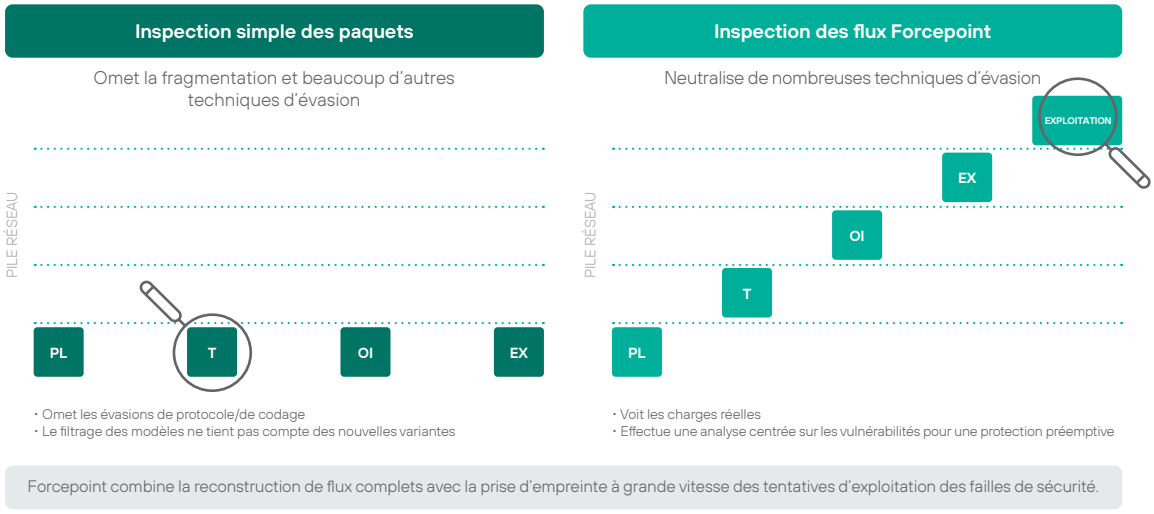
Forcepoint applique ensuite des techniques avancées pour examiner le contenu des transmissions, cherchant les signes d'exploitation les vulnérabilités sur de nombreux types de systèmes. Contrairement aux analyses de signature basées sur des modèles verbeux, l'approche plus sophistiquée de Forcepoint permet l'identification de ces attaques grâce à une empreinte numérique unique et concise. Les empreintes numériques sont mises en correspondance à l'aide d'automates finis déterministes (AFD) à grande vitesse, adaptés à chaque contexte de protocole, ce qui active l'intégration de nouvelles empreintes digitales sans pratiquement aucun impact sur les ressources CPU.

Des mises à jour continues pour garder une longueur d'avance sur les cybercriminels

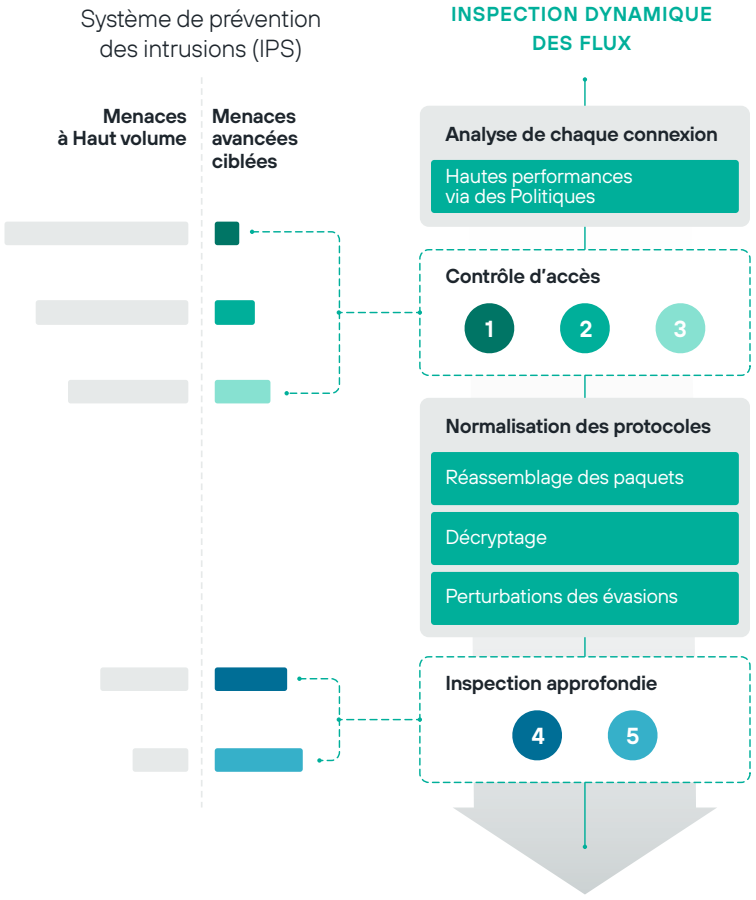
L'équipe de recherche globale Forcepoint examine en permanence les flux de renseignements sur les menaces, les rapports sur les vulnérabilités provenant de différentes sources et divers systèmes de test pour analyser les exploits et les vulnérabilités. De nouvelles empreintes numériques sont publiées selon les besoins via notre service cloud. Elles sont ensuite automatiquement téléchargées par les systèmes de sécurité du réseau Forcepoint. Cette approche proactive donne aux équipes informatiques le temps d'analyser les correctifs nouvellement publiés, afin de mettre en œuvre des mesures correctives sans risque de contamination immédiate.

Stoppe toute menace zero-day et tout contenu indésirable

Les produits de sécurité réseau Forcepoint offrent également plusieurs couches de défense contre des attaques et des contenus indésirables jusqu'ici inconnus. Les fichiers transmis sont soumis à une analyse rigoureuse de leur réputation et à une analyse malware, et les nouvelles menaces comme les attaques zero-day peuvent être signalées et contrées grâce à notre technologie avancée de sandboxing. Forcepoint est l'un des pionniers de la catégorisation et du filtrage des sites Web et du contenu. Grâce à nos appareils IPS et à nos firewalls, les entreprises peuvent plus facilement se conformer aux réglementations en vigueur sur le lieu de travail, limiter l'exposition des données personnelles et empêcher les utilisateurs de se rendre sur des sites Web à contenus dangereux.



Forcepoint combine la reconstruction de flux complets avec la prise d'empreinte à grande vitesse des tentatives d'exploitation des failles de sécurité.



1. Contrôles des connexions
   - Anti-usurpation
   - Réputation des IP
   - Géoprotection
   - Connexions non valides
2. Contrôles d'utilisation
   - Par utilisateur, URL ou application (serveur et terminal)
3. Contrôles de commandes
   - Listes blanches des versions des applications et des commandes
   - Proxies pour empêcher les connexions directes
4. Inspection des vulnérabilités
   - Détection des anomalies et des failles de sécurité
   - Anti-botnet
5. Inspection des malwares
   - Filtrage et indice de réputation des fichiers
   - Analyse Anti-malware
   - Mise en bac à sable

Maintien du trafic en cas de défaillance (Fail-Open)

Les appareils de Forcepoint prennent en charge toute une gamme de cartes réseau modulaires, y compris des interfaces configurées en Fail-open, qui restent ouvertes en cas de défaillance et permettent de maintenir le trafic, même si le firewall n'est plus alimenté.

Une protection assurant le maintien de l'activité de votre entreprise

Chaque jour, les assaillants parviennent à pénétrer dans les réseaux, les applications, les centres de données et les terminaux des entreprises. Une fois à l'intérieur, ils peuvent voler vos propriétés intellectuelles, des informations confidentielles sur vos clients et d'autres données sensibles, causant alors des dégâts irréparables à votre réputation et à la confiance que l'on vous accorde.

Les attaques sur Internet sont maintenant bien plus sophistiquées que de la simple transmission de failles de sécurité. De nouvelles techniques esquivant la détection des appareils traditionnellement utilisés pour la sécurité réseau sont employées, et cela concerne de nombreux firewalls de marques connues.

Ces évasions fonctionnent sur plusieurs niveaux pour camoufler les failles de sécurité et les malwares, les rendant ainsi invisibles lors d'une inspection traditionnelle des paquets basée sur les signatures. Même d'anciennes méthodes d'attaques par évasion, bloquées depuis des années, peuvent soudainement être utilisées pour compromettre les systèmes internes.

Forcepoint adopte une approche différente. Notre moteur IPS, leader du marché, est conçu pour gérer les trois étapes de la défense du réseau : vaincre les attaques par évasion, détecter les exploitations des vulnérabilités et arrêter les malwares. Il peut être déployé facilement derrière les firewalls existants pour ajouter une protection sans interruption, ou dans le cadre de notre solution complète Firewall nouvelle génération pour une sécurité tout-en-un.

Tous les produits de sécurité réseau de Forcepoint sont mis à jour en permanence. Leur gestion centralisée partage de manière transparente les politiques de sécurité et les tableaux de bord sur l'ensemble de votre réseau. Forcepoint vous permet d'assurer la sécurité de votre entreprise – de manière fiable, cohérente et efficace – à travers tous vos centres de données, vos réseaux de bureaux, vos filiales ou vos environnements cloud.

Résultats

- Moins d'intrusions
- La plus haute sécurité, sans perturbations
- Moins d'exposition aux nouvelles vulnérabilités, alors que les équipes informatiques se préparent à déployer de nouveaux correctifs.
- Déploiement plus sûr des filiales, des clouds ou des centres de données.
- Réduction du coût total d'acquisition (CTA) de l'infrastructure et de la sécurisation du réseau.

Fonctions clés

- Déploiement IPS de couche 2, pare-feu Next-Gen de couche 2 ou comme élément d'un firewall nouvelle génération de couche 3.
- Système de détection des intrusions (IDS) et système de prévention des intrusions (IPS) combinés pour assurer à la fois la protection et la défense.
- Inspection du flux qui examine les charges réelles
- Pionnier de la défense contre les évasions
- Décryptage à grande vitesse avec contrôles granulaires de la confidentialité
- Détection des anomalies et des abus de protocole
- Détection des failles de sécurité et des malwares via un DFA à haute vitesse
- Détection des attaques par déni de service (DDoS)
- Défenses anti-bots
- Sandboxing Zero Day via un appareil sur site ou dans le cloud
- Filtrage des URL le plus abouti du secteur
- Interfaces réseau modulaires configurés en Fail-open pour les appareils

Spécifications Firewall nouvelle génération de Forcepoint

PLATEFORMES COMPATIBLES	
Appareils	Des séries d'appareils modulaires, conçus pour être déployés dans vos centres de données, à la périphérie de vos réseaux et dans vos filiales.
Infrastructure cloud	Amazon Web Services, Microsoft Azure
Dispositif virtuel	Systèmes basés sur x86 64 bits ; environnements virtualisés VMware ESXi, VMware NSX, Microsoft Hyper-V et KVM
Modes de déploiement	IPS autonome (couche 2, avec modules d'interface réseau Fail-Open en option), partie de NGFW (couche 3)
Contexte virtuel	Virtualisation pour séparer les contextes logiques avec des interfaces et des politiques distinctes.

INSPECTION	
Normalisation du trafic multicouches/Inspection approfondie de l'ensemble du trafic	› Reconstruit et analyse les charges réelles pour garantir l'intégrité des flux de données. › Élimine les segments dupliqués des niveaux inférieurs, qui pourraient entraîner des ambiguïtés lors du réassemblage.
Défense anti-évasion	Stoppe les fragments non ordonnés, les segments qui se chevauchent, la manipulation du protocole, l'obscurcissement, les astuces de codage.
Détection dynamique contextuelle	Protocole, application, type de fichier
Traitement et inspection du trafic spécifiques au protocole	Encapsulation Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, Inspection intégrée avec proxys Sidewinder Security
Décryptage granulaire du trafic SSL/TLS	› Décryptage haute performance des flux clients et serveurs HTTPS › Des contrôles axés sur les politiques pour protéger la confidentialité des utilisateurs et limiter l'exposition des entreprises aux données personnelles. › Contrôles de validité des certificats TLS et liste d'exemption basée sur le nom de domaine du certificat
Détection d'exploitation des vulnérabilités	› Indépendant du protocole, tout protocole TCP/UDP avec détection et protection contre les évasions. › Prise en charge des intégrations de signatures Snort pour personnaliser et renforcer la doctrine générale de sécurité › L'approche par empreintes numériques élimine le besoin d'utiliser les signatures. › Le moteur de comparaison par automates finis déterministes (AFD) à grande vitesse traite rapidement les nouvelles empreintes numériques. › Mise à jour continue des empreintes numériques par Forcepoint
Prise personnalisée d'empreintes numériques	› Mise en correspondance des empreintes numériques indépendante du protocole › Empreintes numériques basées sur des expressions régulières avec prise en charge d'applications personnalisées
Reconnaissance	Analyse, détection de furtivité et balayage lent TCP/UDP/ICMP en IPv4 et IPv6
Anti-botnet	› Détection basée sur le décryptage et analyse de la séquence de longueur des messages › Mise à jour automatique de la catégorisation des URL afin de bloquer ou d'avertir les utilisateurs de la présence de sites botnet
Corrélation	Corrélation locale, corrélation avec le serveur de journaux.
Protection contre les assauts DoS/DDoS	› Détection des attaques de masse SYN/UDP avec limitation des connexions simultanées, compression du journal selon l'interface. › Protection contre les méthodes à requêtes HTTP lentes, limitation des connexions semi-ouvertes › Séparation du plan de contrôle et du plan de données
Méthodes de blocage	Blocage direct, réinitialisation de la connexion, liste noire (locale et distribuée), réponse HTML, redirection HTTP
Enregistrement du trafic	Enregistrements/mise en exergue automatique des situations inhabituelles de trafic
Mises à jour automatiques	› Mises à jour dynamiques permanentes via le centre de gestion de la sécurité (SMC) de Forcepoint › Mise à jour des correctifs virtuels et détection et prévention des menaces émergentes.

Spécifications Firewall nouvelle génération de Forcepoint, suite

DÉTECTION AVANCÉE DES LOGICIELS MALVEILLANTS ET CONTRÔLE DES FICHIERS	
Protocoles	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtrage des fichiers	Filtrage des fichiers basé sur des règles avec un processus efficace de sélection descendante ; plus de 200 types de fichiers pris en charge dans 19 catégories de fichiers.
Réputation des fichiers	Vérification de la réputation et blocage à grande vitesse des malwares, depuis le cloud
Analyse antivirus des fichiers	Moteur d'analyse antivirus local*
Sandboxing Zero Day	Forcepoint Advanced Malware Detection est disponible pour Forcepoint NGFW sous la forme d'un service cloud, sur site ou même via un mode d'isolation « air-gapped », similaire à celui utilisé par Forcepoint Web Security, Forcepoint Email Security et Forcepoint CASB.

FILTRAGE DES URL	
Catégorisation des URL	Par Forcepoint ThreatSeeker Intelligence, le même système que celui utilisé par Forcepoint Web Security et Forcepoint Email Security.
Mises à jour automatiques	Mise à jour permanente au fur et à mesure que de nouveaux sites sont analysés
Application des politiques d'accès par catégorie	Filtrage des URL pour Forcepoint NGFW en abonnement optionnel

GESTION ET SURVEILLANCE	
Interfaces de gestion	Système de gestion centralisé à l'échelle de l'entreprise avec des fonctions d'analyse des journaux, de surveillance et de création de rapports (voir la fiche technique du Centre de gestion de la sécurité Forcepoint pour plus de détails).
Surveillance SNMP	SNMPv1, SNMPv2c, and SNMPv3
Capture du trafic	Console tcpdump, capture à distance via le Centre de Gestion de la Sécurité Forcepoint
Gestion haute sécurité des communications	Cryptage 256 bits des communications entre le moteur et l'outil de gestion.
Certifications de sécurité	Profil de protection des appareils réseau selon des critères communs avec filtre de trafic dynamique à forfait étendu pour Firewall, certificat cryptographique FIPS 140-2, CSPN par ANSSI, certification de sécurité de premier niveau USGv6.
Agent de contexte pour terminal	Mise sur liste blanche et liste noire des applications clientes fonctionnant sur les machines hôtes et sur les appareils des utilisateurs finaux. Empêche la mise en place de connexions sortantes par des fichiers non fiables, activation des contrôles granulaires personnalisables selon les besoins de votre entreprise.

*L'analyse locale anti-malware n'est pas disponible avec les appareils 110/115.