Forcepoint

Fiche technique

Next Generation Firewall

Sécurité du réseau d'entreprise avec des capacités SD-WAN natives

Avantages principaux

Une liaison SD-WAN toujours disponible pour les entreprises

Les entreprises d'aujourd'hui exigent des solutions de sécurité réseau entièrement résilientes.Forcepoint Next-Gen Firewall (NGFW) s'appuie sur une évolutivité et une disponibilité élevées à tous les niveaux.

- **Clustering actif-actif et mixte.** Jusqu'à 16 nœuds de différents modèles exécutant différentes versions peuvent être regroupés en cluster. Cela offre des performances et une résilience de réseau supérieures et permet une sécurité telle que l'inspection approfondie des paquets et les VPN.
- **Mises à jour transparentes des politiques et des logiciels.** La disponibilité de pointe de Forcepoint permet aux mises à jour des politiques (et même aux mises à jour des logiciels) d'être transférées de manière transparente vers un cluster sans interrompre le service.
- **Regroupement de réseaux SD-WAN.** Étend la couverture haute disponibilité aux connexions réseau et VPN. Combine une sécurité ininterrompue avec la possibilité de tirer parti des liaisons à large bande locales afin de compléter ou de remplacer les lignes louées coûteuses comme les MPLS.

Forcepoint Next-Gen Firewall fournit une sécurité réseau à la pointe du secteur avec une connectivité SD-WAN rapide et flexible pour relier et protéger les personnes et les données qu'elles utilisent dans les réseaux d'entreprise divers et en évolution. Forcepoint NGFW offre une sécurité, des performances et des opérations cohérentes dans les systèmes physiques, virtuels et cloud. Elle est pensée pour une haute disponibilité et une évolutivité, une gestion centralisée et une visibilité complète à 360°.

Les clients qui passent à Forcepoint NGFW Les clients qui passent à Forcepoint NGFW signalent une baisse de 86 % des cyberattaques, une charge informatique réduite de 53 %, et une durée de maintenance réduite de 70 %.*

Suivez le rythme des besoins de sécurité changeants

Un noyau logiciel unifié permet à Forcepoint de gérer plusieurs rôles de sécurité,du pare-feu/VPN et du connecteur d'application ZTNA au système de prévention des intrusions (IPS) et au pare-feu de niveau 2, dans des environnements d'entreprise dynamiques. Forcepoint peut être déployé de diverses façons (par exemple, appareils physiques, virtuels et cloud), le tout géré à partir d'une seule console.

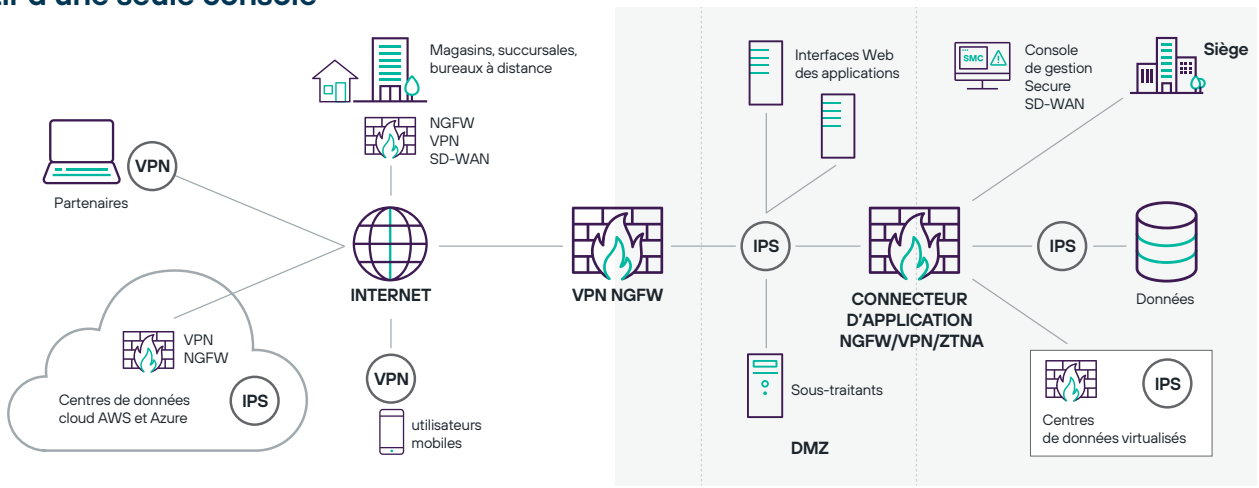
Forcepoint adapte de manière unique le contrôle d'accès et l'inspection approfondie pour chaque connexion afin de fournir des performances et une sécurité élevées. Elle combine le contrôle d'application granulaire, les défenses IPS, le contrôle de réseau privé virtuel (VPN) intégré et les proxys d'application critiques dans un design efficace, extensible et hautement évolutif. Nos puissantes technologies anti-évasion décryptent et normalisent le trafic réseau avant l'inspection et sur toutes les couches de protocole pour exposer et bloquer les méthodes d'attaque les plus avancées.

Bloquez des attaques sophistiquées de violation de données

Les violations de données de grande ampleur continuent d'affecter les entreprises et les organisations dans tous les secteurs d'activité. Combattre cette menace avec une protection d'exfiltration de la couche d'application. Forcepoint autorise ou bloque de manière sélective et automatique le trafic réseau provenant d'applications spécifiques sur des PC, des ordinateurs portables, des serveurs, des partages de fichiers et d'autres terminaux en se basant sur des données contextuelles très détaillées. Elle va au-delà des pare-feu typiques pour prévenir les tentatives d'exfiltration des données sensibles des terminaux via des programmes non autorisés, des applications web, des utilisateurs et des canaux de communication.

* « Quantifier les résultats opérationnels et de sécurité du passage à Forcepoint NGFW », R. Ayoub & M. Marden, IDC Research, mai 2017.

Une seule plateforme avec de nombreuses options de déploiement, toutes gérées à partir d'une seule console



Protection inégalée

Les attaquants sont devenus des experts dans la pénétration des réseaux d'entreprise, des applications, des centres de données et des terminaux. Une fois à l'intérieur, ils volent la propriété intellectuelle, les informations des clients et d'autres données sensibles, causant des dommages irréparables aux entreprises et à leur réputation respective.

Les nouvelles techniques d'attaque peuvent échapper à la détection par les appareils du réseau de sécurité traditionnels, y compris de nombreux pare-feu de marque, allant au-delà de la simple transmission des exploits de vulnérabilité.

Les évasions fonctionnent à plusieurs niveaux pour camoufler les exploits et les programmes malveillants, en les rendant invisibles à l'inspection des paquets basée sur les signatures traditionnelles. Même les attaques bloquées depuis des années peuvent être réemballées avec des évasions pour compromettre les systèmes internes.

Forcepoint adopte une approche différente. Notre moteur de sécurité de pointe du secteur est créé pour les trois étapes de la défense du réseau : pour vaincre les évasions, détecter les exploits des vulnérabilités et stopper les programmes malveillants. Elle peut être déployée de manière transparente derrière les pare-feu existants pour ajouter une protection sans perturbation, ou en tant que pare-feu d'entreprise complet pour une sécurité tout-en-un.

En outre, Forcepoint fournit un déchiffrement rapide du trafic chiffré, y compris les liaisons web HTTPS, combiné à des commandes de protection de la vie privée granulaires qui protègent votre entreprise et vos utilisateurs dans un monde en évolution rapide. Elle peut même limiter l'accès à partir d'applications de terminaux spécifiques pour verrouiller les appareils ou empêcher l'utilisation de logiciels vulnérables.

Avantages commerciaux

- → Déploiement plus rapide des succursales, des clouds ou des centres de données
- → Moins d'arrêt
- → Une sécurité accrue sans perturbation
- → Moins d'intrusions
- → Moins d'exposition aux nouvelles vulnérabilités pendant que les équipes informatiques se préparent à déployer de nouveaux correctifs
- → Réduction du CTP pour l'infrastructure et la sécurité du réseau

Fonctionnalités clés

- → La connectivité SD-WAN à l'échelle de l'entreprise
- → Intégration SASE/SSE pour le web, le cloud et la sécurité des applications privées
- → IPS intégré avec défenses anti-évasion
- → Clustering haute disponibilité des appareils et des réseaux
- → Mises à jour automatisées et sans interruption
- → Gestion centralisée axée sur les politiques
- → Visibilité à 360° pratique et interactive
- → Proxies de sécurité Sidewinder pour les applications critiques
- → Contexte de l'utilisateur et du terminal
- → Déchiffrement haute performance avec des commandes granulaires de protection de la vie privée
- → Autoriser/bloquer par application et version client
- → Surveillance de l'état des applications
- → Intégration du CASB et de la sécurité Web
- → Sandboxing Anti-Malware
- → Logiciel unifié pour les déploiements physiques, AWS, Azure, VMware
- → Moins d'exposition aux nouvelles vulnérabilités pendant que les équipes informatiques se préparent à déployer de nouveaux correctifs
- → Réduction du CTP pour l'infrastructure et la sécurité du réseau

Spécifications de Forcepoint NGFW

PLATEFORMES	
Appareil physique	Plusieurs options d'appareils matériels, allant de la succursale aux installations de centres de données
Appareil virtuel	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Virtual Appliance	Systèmes x86 64 bits ; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM et Nutanix AHV
Terminal	Agent contextuel du terminal (ECA), Client VPN
Contextes virtuels	Jusqu'à 250
Gestion centralisée	Système de gestion centralisée au niveau de l'entreprise avec des capacités d'analyse des journaux, de surveillance et de création de rapports. Voir la fiche technique du Centre de gestion de sécurité Forcepoint pour plus de détails.

CARACTÉRISTIQUES DU PARE-FEU	
Inspection approfondie des paquets	Normalisation du trafic multicouche/inspection approfondie complète, défense anti-évasion, détection dynamique du contexte, traitement et inspection du trafic spécifiques au protocole, décryptage granulaire du trafic SSL/TLS (TLS 1.2 et 1.3), détection des failles de vulnérabilité, empreinte digitale personnalisée, reconnaissance, anti-botnet, corrélation, enregistrement du trafic, protection DoS/DDoS, méthodes de blocage, mises à jour automatiques
Identification de l'utilisateur	Base de données interne des utilisateurs, LDAP natif, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Certificats clients
Haute disponibilité	› Regroupement de pare-feu active-active/active-standby jusqu'à 16 nœuds › SD-WAN › Basculement d'état (y compris les connexions VPN) › Équilibrage de la charge du serveur › Agrégation de liens (802.3ad) › Détection des défaillances de liaison
Attribution d'adresse IP	› IPv4 statique, DHCP, PPPoA, PPPoE, IPv6 statique, SLAAC, DHCPv6 › Services : Serveur DHCP pour IPv4 et relais DHCP pour IPv4 et IPv6
Routage	› Routes statiques IPv4 et IPv6, routage basé sur des politiques, routage multicast statique › Routage dynamique : RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, proxy IGMP › Routage sensible aux applications
IPv6	Double pile IPv4/IPv6, NAT 44, NAT64, NAT66, ICMPv6, DNSv6, NAT, fonctionnalités NGFW complètes
Redirection de proxy	Redirection des protocoles HTTP, HTTPS, FTP, SMTP vers Forcepoint ou un service d'inspection de contenu tiers (CIS) sur site et dans le cloud
Géoprotection	Pays ou continent source/destination mis à jour dynamiquement
Liste d'adresses IP	Catégories IP prédéfinies ou à l'aide de listes d'adresses IP personnalisées ou importées
Filtrage des URL (abonnement séparé)	Listes d'URL personnalisées ou importées ; prend en charge QUIC et HTTP/3
Applications du terminal	Nom et version de l'application
Applications réseau	Plus de 7400 applications réseau et cloud
Proxies de sécurité Sidewinder	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

INTÉGRATION SASE	
Transfert du trafic Web	Tunnels GRE et IPsec vers les plateformes Security Service Edge (SSE) telles que Forcepoint ONE
Connecteur d'application ZTNA	Permet aux applications privées dans les centres de données internes de se relier à Zero Trust de Forcepoint ONE
SD-WAN	
Protocoles	IPsec et TLS
VPN site à site	› VPN basé sur des politiques et des routes › Réseau en étoile, maillage complet, maillage partiel, topologies hybrides › Sélection dynamique de liens multiples FAI › Partage de charge, actif/veille, agrégation de liens › Surveillance en direct et rapports sur la qualité de la liaison des FAI (délai, gigue, perte de paquets)
Accès à distance	› Client VPN Forcepoint pour Microsoft Windows, Android et Mac OS › Tout client IPsec standard › Haute disponibilité avec reprise automatique › Vérifications de sécurité des clients › Accès au portail VPN TLS

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 politiques avec processus de sélection efficace. Plus de 200 types de fichiers pris en charge dans 19 catégories de fichiers
Réputation des fichiers	Vérification et blocage à grande vitesse de la réputation des programmes malveillants depuis le cloud
Anti-Virus	Moteur d'analyse antivirus local*
Zero-Day Sandboxing	Forcepoint Advanced Malware Detection and Protection disponible à la fois en tant que service cloud et sur site

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