Forcepoint

Fiche Technique

Forcepoint Secure SD-WAN

Votre réseau d'entreprise est-il optimisé pour relever les défis d'aujourd'hui ?

Forcepoint Secure SD-WAN optimise la connectivité aux environnements cloud privés, publics et hybrides, permettant une performance accrue des applications tout en appliquant les politiques de sécurité sur des milliers de sites, le tout à partir d'un emplacement central.

- **Clustering actif-actif, mixte.** Jusqu'à 16 nœuds de modèles différents exécutant différentes versions peuvent être regroupés ensemble. Cela fournit des performances et une résilience réseau supérieures et permet des mesures de sécurité telle que l'inspection approfondie des paquets et les VPN.
- **Mises à jour des politiques et mises à niveau logicielles en toute transparence.** La disponibilité de pointe Forcepoint permet aux mises à jour des politiques (et même aux mises à niveau logicielles) 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 Secure SD-WAN permet aux organisations distribuées d'améliorer les performances des applications, de simplifier la gestion du réseau et d'augmenter la sécurité – en garantissant que les utilisateurs peuvent accéder en toute sécurité à toute application depuis n'importe où. Il offre un contrôle applicatif sur les liaisons MPLS et Internet haut débit tout en protégeant contre les menaces avancées. Il est conçu dès le départ pour une haute disponibilité et une évolutivité, ainsi qu'une gestion centralisée avec une visibilité complète sur le trafic réseau.

Restez en phase avec les besoins de sécurité en constante évolution

Un noyau logiciel unifié permet à Forcepoint Secure SD-WAN de gérer plusieurs rôles de sécurité, du pare-feu/VPN à l'IPS en passant par un pare-feu de couche 2, dans des environnements d'entreprise dynamiques. Les SD-WAN sécurisés peuvent être déployés de diverses façons (par exemple, appareils physiques, virtuels, cloud), le tout géré à partir d'une console unique.

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

Bloquer les attaques sophistiquées

Les violations de la sécurité continuent de tourmenter les entreprises et les organisations dans tous les secteurs. Augmentez les mesures de sécurité avec une protection par ex-filtration au niveau de l'application. Forcepoint Secure SD-WAN 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 autres appareils terminaux à partir des données contextuelles hautement granulaires du terminal. Il va au-delà de la sécurité réseau typique et empêche les tentatives d'exfiltration d'informations sensibles au niveau des terminaux via des programmes non autorisés, des applications Web, des utilisateurs et des canaux de communication.

Spécifications Forcepoint SD-WAN

PLATEFORMES	
Appareil physique	Options multiples d'appareils matériels, allant des succursales aux installations de centres de données
Infrastructure cloud	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Appareil virtuel	Systèmes basés sur x86 64 bits ; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM et Nutanix AHV
Terminal	Agent de contexte pour terminal (ECA), client VPN
Contextes virtuels	Jusqu'à 250
Gestion centralisée	Système de gestion centralisée à l'échelle de l'entreprise avec des capacités d'analyse des journaux, de surveillance et de création de rapports

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 plusieurs liens ISP › Partage de charge, actif/en 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 basculement automatique › Vérifications de sécurité des clients › Accès au portail VPN TLS

FONCTIONS DE SÉCURITÉ RÉSEAU	
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 (à la fois TLS 1.2 et 1.3), détection des exploits de vulnérabilité, empreinte digitale personnalisée, reconnaissance, anti-botnet, corrélation, enregistrement du trafic, protection DoS/DDoS, méthodes de blocage, mises à jour automatiques, sinkholing DNS
Identification de l'utilisateur	Base de données utilisateur interne, LDAP natif, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, certificats client
Haute disponibilité	› Clustering actif/actif-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, NAT44, NAT64, NAT66, ICMPv6, DNSv6, NAT
Redirection par proxy	Redirection des protocoles HTTP, HTTPS, FTP, SMTP vers Forcepoint ou un service d'inspection de contenu (CIS) tiers 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
Applications de terminaux	Nom et version de l'application
Applications réseau	7400+ applications réseau et cloud
Proxys de sécurité Sidewinder	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

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 sur la base du cloud
Anti-Virus	Moteur d'analyse antivirus local*
Sandboxing Zero Day	Forcepoint AMDP disponible à la fois en tant que service cloud et sur site **

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