Forcepoint

Fiche technique

Centre de gestion de la sécurité NGFW

Toute l'administration s'effectue via un écran unique, donnant une visibilité maximale sur le réseau

Avantages principaux

- Gestion centralisée, à interface unique, pouvant permettre de gérer jusqu'à 6 000 NGFW physiques ou virtuels Forcepoint dans les environnements distribués
- Flexibilité et évolutivité pour le déploiement dans les grands réseaux d'entreprise
- Option de haute disponibilité pour les exigences de temps de fonctionnement
- Des politiques intelligentes et une automatisation efficace des flux de travail pour un déploiement rapide et une maintenance efficace des firewalls Forcepoint NGFW
- Contexte, sensibilisation et visibilité des utilisateurs et des terminaux sur l'ensemble de votre réseau, du centre de données et de la périphérie jusqu'aux sites secondaires et au cloud
- Choix des options de déploiement du logiciel ou de l'appareil

Le Centre de gestion de la sécurité Forcepoint NGFW (SMC) fournit une gestion unifiée et centralisée de tous les modèles de Firewall Next Generation Forcepoint – physiques, virtuels ou dans le cloud dans les grands environnements d'entreprise géographiquement distribués.

Grâce à une flexibilité, une évolutivité et une facilité d'utilisation supérieures, Forcepoint Security Management Center (SMC) rend les environnements de sécurité réseau dynamiques plus faciles à gérer et capables de prendre en charge des plans agressifs de croissance commerciale. Les Politiques intelligentes permettent le déroulement naturel des processus d'activité, tandis que ses flux de travail optimisés rationalisent les tâches administratives quotidiennes pour une grande efficacité et un faible coût total d'acquisition (CTA).

Le SMC offre une visibilité panoramique, à 360 degrés, sur l'ensemble des réseaux d'entreprise, en recueillant des informations de gestion d'événements et de surveillance de l'état à partir des NGFW Forcepoint, des terminaux et des appareils tiers pour permettre des enquêtes interactives ainsi que des rapports détaillés. En outre, le SMC Forcepoint peut agréger les données des journaux des NGFW provenant de plusieurs serveurs géographiquement distribués, dressant des rapports consolidés tout en maintenant la souveraineté des données.

Haute disponibilité

Les activités commerciales d'aujourd'hui ont une tolérance zéro pour les perturbations et exigent un accès permanent aux ressources essentielles. Grâce à l'option haute disponibilité du SMC de Forcepoint, les organisations conservent un accès continu aux ressources des journaux pour une analyse et une réponse robustes aux incidents.

Client de gestion de la sécurité

Quelle que soit la situation géographique, les administrateurs peuvent accéder en toute sécurité au SMC Forcepoint par l'intermédiaire de son client de gestion. Ce client propose une puissante interface graphique pour la configuration, la surveillance, la journalisation, les alertes, les rapports, les mises à jour et les mises à niveau des firewalls Forcepoint de nouvelle génération. Le client Forcepoint SMC donne aux administrateurs une vue d'ensemble du réseau et des actions contextuelles, assurant une gestion rapide et efficace de l'ensemble de votre environnement de sécurité.

Spécifications du SMC Forcepoint NGFW

SERVEUR DE GESTION	
Nombre d'appareils gérés	Sous licence : 1 à 6 000 nœuds avec un seul serveur de gestion
Nombre d'administrateurs	Illimité
Nombre d'éléments	Illimité
Nombre de politiques	Illimité
Nombre de serveurs de journaux	Illimité
Nombre de Serveurs de Portail Web	Illimité
Authentification de l'Administrateur	Base de données locale, RADIUS. TACACS+, Certificat client et Microsoft Active Directory (LDAP)
Connexions aux appareils	Cryptage TLS
SERVEUR DE CONNEXION	
Nombre d'appareils pris en charge	Illimité
Enregistrements de journaux par seconde	Le système d'enregistrement à haute performance peut traiter plus de 500 000 enregistrements par seconde
Connexions aux appareils	TLS 1.2 chiffré et authentifié en utilisant des clés et certificats X.509v3
Taille de stockage des journaux	Illimité
Nombre de transfert de journaux par Serveur de connexion	Illimité
GÉNÉRAL	
Client de gestion	Interface de commande basée sur HTML 5
Interface de programmation d'applications du SMC (API du SMC)	API documentée permettant une intégration facile de produits et services tiers. Utilise l'architecture REST, avec laquelle les données peuvent être codées en XML ou JSON
Administrateurs simultanés	Plusieurs administrateurs peuvent effectuer des changements en même temps ; des éléments critiques comme les politiques sont verrouillés pour l'édition
Tableaux de bord de l'écran d'accueil	Tableaux de bord personnalisables sur l'écran d'accueil pour les NGFW, les VPN, les utilisateurs et d'autres éléments
Surveillance utilisateur	En plus des corrélations et des vérifications liées au comportement de l'utilisateur, vous recevez des informations sur l'état de la sécurité des terminaux et des statistiques sur les applications des terminaux.

Haute disponibilité	Jusqu'à quatre serveurs de gestion de secours
Mises à niveau	Les mises à jour et les paquets de mise à jour dynamique peuvent être téléchargés automatiquement
Sauvegardes	Outil de sauvegarde intégré permettant d'effectuer des sauvegardes de l'ensemble du système, y compris de toutes les configurations de firewalls nouvelle génération
Navigation	Navigation intuitive de type navigateur avec historique de navigation, onglets et signets
Outils de recherche Spotlight	Des outils efficaces de recherche d'éléments et de références avec des actions rapides adaptées au contexte
Filtrage rapide	Filtrage anticipé pratique dans les listes d'éléments, les tableaux et les cellules de politique
Prise en charge de sélections multiples	Effectuez des actions et engagez des modifications sur des centaines d'éléments simultanément
Outils de nettoyage du système	Permet à l'administrateur de trouver facilement quels éléments et règles ne sont pas utilisés
ADMINISTRATION	
Élévation des alertes	Permet à l'administrateur de transmettre des alertes à partir du système en utilisant le courrier électronique, les SMS, les traps SNMP et les scripts personnalisés
Seuils d'alerte	Seuils d'alerte facilités pour les statistiques de synthèse
Journaux d'audits	Toutes les modifications apportées au système sont enregistrées dans les journaux d'audit.
Rapports système	Rapports d'inventaire et d'audit de conformité sur les comptes et les activités des administrateurs
Déploiement sans contact	Installation via le cloud (ou via une clé USB) avec un envoi de politique initiale
Tâches automatiques	Automatisation de la gestion des données des journaux, de leur archivage et de leur conservation, des sauvegardes, des mises à niveau et des tâches d'actualisation des politiques.
Domaines administratifs	Permet de diviser l'environnement en domaines de configuration isolés
Import/Export	Exportation et importation XML et CSV à tout moment, et plus seulement entre les installations
Mises à jour à distance	Mise à niveau à distance en un clic avec sécurité intégrée des FWNG gérés
Contrôle d'accès basé sur les rôles définis par l'Administrateur	Des rôles personnalisés peuvent être définis et combinés en plus des rôles prédéfinis (par exemple, propriétaire, spectateur, opérateur, éditeur, super utilisateur) pour contrôler les autorisations de manière souple et précise
Gestion de licences	Mises à jour automatiques des licences en ligne et rapports sur l'état des contrats de maintenance
Gestion des certificats	Vue globale de tous les certificats et titres
Outils de dépannage	Capacités étendues de diagnostic à distance : outil intégré de capture de trafic, téléchargement d'instantanés de configuration de firewalls nouvelle génération, visualisation de surveillance de session
Gestion des dossiers d'incidents	Outils intégrés pour la gestion collaborative des incidents réseau

GESTION DES POLITIQUES	
Moteur virtuel NGFW	Partage du même contexte maître dans plusieurs domaines administratifs du SMC ; jusqu'à 250 contextes virtuels, chacun ayant ses propres politiques et tables de routage
Gestion hiérarchisée des politiques	Les modèles de politique, les sous-politiques, les alias et les sections de commentaires sur les règles permettent de garder les politiques bien rangées et compréhensibles
Identification d'application	→ Restriction d'accès en fonction des applications du réseau et/ou du terminal → Restreindre l'accès de/vers les applications par charge utile → Listes d'autorisation/blocage par nom et version de l'application à partir de l'agent contextuel Forcepoint Endpoint
Gestion des modifications	Nécessite l'examen et l'approbation d'un deuxième administrateur avant que les changements ne soient déployés
Filtrage des URL	Restriction d'accès selon les catégories des URL
Noms de domaines	Restriction d'accès dynamique en utilisant des noms de domaines qui peuvent être traduits en adresses IP
Identification de l'utilisateur	Correspondance des règles basées sur l'utilisateur via l'identification transparente de l'utilisateur ou l'application de méthodes d'authentification exigeantes
Zones	Les interfaces physiques peuvent être marquées avec des zones et mentionnées dans les politiques
Géoprotection	Restriction d'accès par pays ou régions géographiques
Politiques d'inspection	Contrôle granulaire pour l'inspection approfondie des paquets et moyens simples pour éliminer les faux positifs
Politiques de qualité de service (QoS)	Configuration des politiques basées sur la qualité de Service
Filtrage des fichiers basé sur les politiques	Définissez la manière dont les fichiers sont inspectés en utilisant les indices de réputation des fichiers de McAfee Global Threat Intelligence, Anti-Malware Scan et McAfee Advanced Threat Defense
Traduction d'adresses réseau (NAT)	→ NAT par défaut → NAT selon des éléments → Politiques NAT
Outil de validation des politiques	Aide l'administrateur à trouver les erreurs de configuration avant l'activation de la politique
Instantanés des politiques	Permet d'explorer et de comparer l'historique de la configuration du Firewall nouvelle génération Forcepoint
Restauration de politiques	Une version précédente de la politique peut être récupérée et téléchargée vers le firewall de nouvelle génération
Outil d'optimisation de l'usage des règles	Permet aux administrateurs de voir combien de fois chaque règle a établi une correspondance au cours d'une période donnée
Outils de recherche de règles	Outil intégré pour la recherche de règles dans les politiques
Noms de règles	Possibilité de créer des noms de règles qui sont visibles dans les journaux, les statistiques et les rapports
Déploiement de politiques à sécurité intégrée	Le système restaure automatiquement la version précédente de la politique si la nouvelle version ne marche pas

CONFIGURATION DE	
Redirection	Configuration de la redirection par glisser-déposer pour les firewalls et les widgets spécifiques pour ajouter des itinéraires et établir des itinéraires par défaut
Redirection dynamique	Configuration avancée de OSPF et BGP via une interface utilisateur graphique intuitive
Anti-spoofing automatique	La configuration anti-spoofing est créée automatiquement en fonction de la redirection
VPN site à site	→ VPN à politiques IPsec → VPN et tunneling IPsec basés sur les redirections (GRE)
VPN à accès à distance	→ VPN IPsec client (iOS et Windows) → VPN SSL client (Android, Mac et Windows) → Portail VPN SSL sans client
Gestion des agents de contexte des terminaux	Extension du contrôle d'accès et de la visibilité aux applications s'exécutant sur les terminaux
Assistant de création d'éléments de Firewall	Créer des centaines d'éléments de firewall grâce à un assistant de création de firewalls
Authentification d'utilisateur basée sur le navigateur	Configurer et personnaliser un service d'authentification simple par navigateur pour les utilisateurs
ÉTAT, STATISTIQUES ET RAPPORTS	
Surveillance de l'état du système	Informations en temps réel sur l'état des appareils du réseau et de leurs connexions
Surveillance de l'état de l'appareil	Vue graphique de l'état matériel des appareils
Diagrammes des réseaux	Visualisez les configurations, les topologies et l'état de connectivité
Surveillance des sessions	Vues dédiées pour surveiller les connexions, les associations de sécurité VPN, les utilisateurs authentifiés, les alertes actives et les itinéraires dynamiques et statiques
Vues d'ensemble	Personnalisation des tableaux de bord des statistiques des utilisateurs et du réseau pour une surveillance en temps réel
Géolocalisation	Affichage des informations sur le pays pour toutes les adresses IP à l'aide des drapeaux des pays et des statistiques de géolocalisation. Afficher d'où viennent les attaques subies par le réseau
Création de rapports	Personnalisez et planifiez des rapports qui fournissent des informations détaillées sur les statistiques du réseau
Portail Web	Accès en lecture seule pour voir les politiques, les journaux et les rapports programmés

GESTION DE LA SURVEILLANCE	
D'appareil tiers	Permet à l'administrateur de surveiller et de visualiser les changements d'état de la disponibilité des appareils tiers
Injection des journaux de log des appareils	Analyse et réception dans les journaux au format syslog pour les appareils tiers et prise en charge directe des formats CEF, LEEF, CLF et WELF
Réception NetFlow/IPFIX	Possibilité de recevoir en amont et de consolider des données aux formats NetFlow v9 et IPFIX
Statistiques appareils	Statistiques et rapports graphiques basés sur des données de journal de tiers et des compteurs simples du protocole de gestion de réseau (SNMP)
Nombre d'appareils pris en charge	200 par serveur de journaux
Octroi de licences	Chaque appareil tiers consomme 0,2 du nombre de licences d'appareils du serveur de gestion
JOURNAUX	
Navigateur	Vue granulaire pour les différents types de journaux en plus de la vue de navigation commune pour toutes les données du journal
Filtrage par glisser-déposer	Filtrage interactif des journaux – Faites des glisser/déposer sur n'importe quelle cellule de données de journaux dans le panneau de recherche
Statistiques	Construisez des compteurs intégrés basés sur les journaux et des statistiques à la demande pour la création de rapports, la surveillance et les alertes
Visualisations	Trouvez les anomalies dans le trafic enregistré dans des visualisations de journaux filtrables
Analyseur de journaux	Agrégation libre de la grande quantité de données de journaux filtrées par n'importe quelle colonne
Archivage	Duplication ou archivage des journaux dans des répertoires par type de données de journal, par heure ou par filtres.
Sauvegardes	Calendrier de sauvegarde intégré pour la configuration du serveur de journalisation et les données de journaux
Exports	Exportation de CSV, XML, LEEF et de journaux – les journaux peuvent également être des rapports instantanés.
Transfert	Redirection du journal en temps réel dans syslog ; formats CEF, LEEF, XML, CSV, IPFIX, NetFlow et McAfee Enterprise Security Manager ; configuration pour le filtrage, type de données et sélection des champs du journal
Contexte des données	Raccourcis permettant de parcourir les différents types de journaux avec des ensembles de colonnes contextuelles personnalisables
Haute disponibilité	Prise en charge de l'attribution de serveurs de journaux primaires et de secours pour chaque source de journalisation

Gestion centralisée de plusieurs environnements de clients

Les prestataires de services de sécurité gérés (MSSP) doivent réduire les coûts administratifs élevés associés à la gestion de plusieurs serveurs sur plusieurs domaines. La licence de domaine administratif Forcepoint Administrative Domain License permet de gérer plusieurs environnements clients par le biais d'un seul serveur de gestion. Les configurations peuvent être réutilisées et partagées entre les domaines pour une distribution rapide et efficace des changements. L'architecture de Forcepoint Administrative Domain License simplifie les environnements d'entreprise et des MSSP, ce qui en facilite la maintenance. Le contrôle d'accès basé sur les rôles (RBAC) assure une définition précise des responsabilités de l'administrateur et des limites d'accès au domaine. Les clients basés dans un domaine peuvent accéder facilement aux rapports, aux configurations de politiques et aux journaux via un portail Web léger et sécurisé.

Spécifications Forcepoint Administrative Domain License

DOMAINES	
Nombre maximum	1 000
Nombre d'administrateurs	Illimité
Nombre d'appareils gérés	6 000
Nombre d'éléments	Illimité
FONCTIONNALITÉS	
Séparation des configurations	Isolez les environnements gérés en fonction des différents domaines administratifs et assurez-vous que les éléments du réseau des clients ne sont jamais mélangés
Partage de configuration	Mettez en commun des éléments tels que les modèles de politique pour tous les domaines
Contrôle d'accès	Accordez ou limitez les droits d'accès des administrateurs à la configuration et à la visibilité, à l'aide de domaines administratifs distincts.
Surveillance	Surveillez les états de tous les domaines autorisés à l'aide de l'aperçu des domaines
Branding	Rapports PDF de marque avec des modèles de style personnalisés
Outils de migration	Déplacez des éléments entre les domaines avec l'outil intégré « Déplacer vers »
Import/Export	Importez et exportez des éléments entre différentes installations et domaines du SMC
Moteur virtuel NGFW	Partagez le même contexte maître à travers les limites de domaine (jusqu'à 250 contextes virtuels) ; ces domaines peuvent chacun avoir leurs propres politiques et leurs tables de routage

Forcepoint Web Portal Sunucusu

Forcepoint Web Portal Server fournit aux clients, aux administrateurs et aux cadres utilisant un MSSP une interface de commande web légère permettant de consulter les journaux, les rapports programmés, les politiques actuelles et l'historique des modifications des politiques. Les administrateurs du MSSP peuvent configurer la quantité d'informations affichées sur le portail en fonction des besoins des clients ou pour réduire les demandes d'assistance.

Forcepoint Web Portal Server prend en charge l'anglais, l'espagnol et le français, avec la possibilité d'ajouter de nouvelles langues.

Avantages principaux

- → Accès en lecture seule et sans client aux journaux, rapports et politiques et historique des changements de politique
- → État du réseau en temps réel disponible pour des utilisateurs définis
- → Prise en charge des appareils mobiles

Spécifications de Forcepoint Web Portal Server

SPÉCIFICATIONS	
Nombre maximal d'utilisateurs concurrents	250 par portail de serveur web
Nombre d'administrateurs	Illimité
Nombre d'utilisateurs Web Portal	Illimité
Authentification d'utilisateurs	Base de données du serveur de gestion, RADIUS, TACACS+
Connexions aux appareils	Cryptage TLS
FONCTIONNALITÉS	
Politiques de sécurité	Visualisation des dernières configurations des firewalls de nouvelle génération au format HTML
Rapports	Affichage des rapports qui doivent être publiés dans le portail Web au format HTML
Consultation des journaux de log	Parcourez et filtrez les journaux au format HTML
Détails des journaux	Surveillez les états de tous les domaines autorisés à l'aide de l'aperçu des domaines
Exportation en PDF	Exportation PDF permettant de télécharger le rapport au format PDF
Annonces	Les administrateurs peuvent spécifier les annonces à afficher dans le portail Web
Comparaison des politiques	Comparez les différentes versions de configuration des firewalls nouvelle génération pour voir si la demande de changement a été implémentée
Localisation	Le portail Web est disponible en anglais, en espagnol et en français, et peut être facilement traduit pour la prise en charge d'autres langues
Personnalisation	Personnalisez l'aspect et la convivialité des portails Web

Forcepoint SMC Aracı

L'appareil Forcepoint Security Management Center (SMC) est un appareil dédié tout-en-un pour configurer, gérer et surveiller les firewalls Forcepoint NGFW – physique, virtuel, et basé sur le cloud. Forcepoint SMC offre une facilité de déploiement pour vous permettre d'être rapidement opérationnel, en combinant le serveur de gestion NGFW et le serveur de journaux de Forcepoint en un seul package plug and play fonctionnant sur du matériel 1U optimisé.

Options de déploiement du SMC Forcepoint NGFW

Il existe trois façons de déployer Forcepoint SMC : sur vos systèmes, sur votre matériel nu ou votre hyperviseur, ou sous forme d'appareil tout-en-un.[1]

1 Une licence de logiciel SMC doit être achetée séparément pour les 3 options de déploiement. Un appareil seul n'inclut aucune licence.

	OPTIONS DE DÉPLOIEMENT DU SMC FORCEPOINT NGFW		
COMPOSANTS	**LOGICIELS**	**IMAGE ISO**	**APPAREIL**
Logiciel SMC	●	●	●
Système d'exploitation	Fourni par le client	●	●
Matériel/Plateforme	Fourni par le client	Fourni par le client	●

Spécifications Appareil SMC Forcepoint

PERFORMANCE	
Firewalls gérés	2 000
Domaines maximum	200
Journaux indexés par seconde	80 000
Événements par jour	6 912 000 000
Taille du journal par jour (Go)	690

Spécifications Appareil SMC Forcepoint

PHYSIQUE	
Encombrement	1U
Processeur	2 x Intel Xeon®
Mémoire	32 Go
Stockage (HDD)	Capacité 900 Go (4 X 300 Go, RAID-5), remplaçable à la volée
Unité d'alimentation	2 x 550 W (100V~240V) remplaçable à la volée
Dimensions	60,7cm P x 43,42cm L x 4,28cm H (23,9" P x 17,09" L x 1,68" H)
Poids	28,26 lb. 12,82 kg
Règlementation et conformité	FCC/ICES/EN55022/VCCIBSMI/C-Tick/SABS / CCC/MIC Class A et UL60950-1/Vérification de la conformité avec la directive RoHS

Commander Forcepoint SMC

COMMANDER	N° DE RÉFÉRENCE
Forcepoint NGFW Security Management Center (logiciel)	SMCX
Appareil Forcepoint NGFW Security Management Center 1000	SMCAP
Forcepoint NGFW Security Management Center Haute disponibilité (uniquement disponible pour les logiciels et les déploiements d'images ISO)	SMCHAX
Serveur de connexion supplémentaire Forcepoint SMC	ALSX
Domaines SMC Forcepoint (jusqu'à 200 domaines)	ODFSMCX
Portail Web Forcepoint SMC	OWPSX

Forcepoint

forcepoint.com/fr/contact

© 2022 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques déposées par Forcepoint. Toutes les autres marques citées dans ce document appartiennent à leurs propriétaires respectifs. [FP-NGFW-Security-Management-Center-Datasheet-FR] 5Oct2022