FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint NGFW Security Management Center

LA GESTION CENTRALISÉE DE TOUS LES PARE-FEUX DE FORCEPOINT DÉPLOYÉS DANS LES ENVIRONNEMENTS DISTRIBUÉS

FORCEPOINT NGFW SECURITY MANAGEMENT CENTER (SMC)

Forcepoint NGFW Security Management Center (SMC) fournit une gestion centralisée et unifiée de pare-feux Forcepoint NGFW et s'adapte à tous les modes de fonctionnement des grandes entreprises géographiquement dispersées.

Sa flexibilité vous permet de faire évoluer les composants actuels et d'ajouter de nouveaux composants au système sans sacrifier la convivialité. Les workflows liés à l'administration sont optimisés afin d'assurer une gestion quotidienne de la sécurité aussi efficace que possible.

Le SMC assure également la gestion des événements et offre des fonctionnalités de génération de rapports pour les équipements tiers. La collecte de toutes ces informations au sein d'un système centralisé permet aux administrateurs de disposer d'une vue complète sur tous les événements qui se produisent dans leur environnement.

Le SMC inclut au moins un serveur de gestion et un serveur de journaux qui peuvent être installés sur le même serveur ou sur des serveurs distincts

HAUTE DISPONIBILITÉ

Les entreprises d'aujourd'hui exigent un accès 24/7/365 aux ressources critiques. Forcepoint SMC vous permet de développer une infrastructure de gestion extrêmement résiliente, garantissant un accès ininterrompu aux ressources de gestion et de journalisation.

CLIENT DE GESTION DE LA SÉCURITÉ

Grâce à une interface graphique unifiée la configuration, la surveillance, la journalisation, les informations d'état, les alertes, les rapports et les mises à jour peuvent être gérés de façon centralisée pour tous les équipements, indépendamment de leur emplacement physique. Le client Forcepoint de gestion de la sécurité offre aux administrateurs des raccourcis et des fonctions de consultation des détails pour une gestion efficace de l'ensemble de l'environnement de la sécurité.

AVANTAGES CLÉS

- Une interface de gestion centralisée de tous les pare-feux Forcepoint dans les environnements distribués.
- Flexibilité et adaptabilité pour le déploiement en environnements distribués.
- La haute disponibilité répond aux fortes exigences de connexion continue.
- L'automatisation du workflow permet un déploiement rapide et précis et assure la maintenance efficace des pare-feux Forcepoint.
- Offre la visibilité sur l'ensemble du réseau, y compris les succursales et les sites distants

SPÉCIFICATIONS DE FORCEPOINT NGFW SECURITY MANAGEMENT CENTER

SERVEUR DE GESTION	
Nombre d'équipements managés	Licence limitée: 2 à 2,000 noeuds par serveur de gestion
Nombre d'administrateurs	Illimité
Nombre de composants	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 locales, RADIUS
Connexion des équipements	SSL-avec chiffrement
SERVEUR DE LOGS	
Nombre d'équipements pris en charge	Illimité
Enregistrements de journal par seconde	Le système de journalisation hautes performances est capable de traiter plus de 100 000 enregistrements/ seconde.
Connexion des équipements	SSL avec chiffrement IPv4/IPv6
Capacité de stockage des journaux	Illimité
Nombre de redirections de journaux, par serveur	Illimité
FONCTIONNALITÉS	
GÉNÉRAL	
Client de gestion	Programme client Java avec prise en charge de Web Start
API SMC	• API documentée permettant une intégration aisée de serviceset produits tiers. • L'API utilise l'architecture REST lorsque les données peuvent être codées en XML ou JSON.
Administrateurs simultanés	• Plusieurs administrateurs peuvent effectuer des modifications simultanément. • Les éléments critiques tels que les stratégies sont verrouillés pendant les modifications.
Haute disponibilité	Prise en charge de quatre serveurs de gestion en mode veille au maximum.
Mises à jour	Téléchargement automatique des dernières mises à niveau
Sauvegardes	Outil de sauvegarde intégré permettant d'effectuer des sauvegardes du système complet, y compris des configurations des pare-feux
Navigation	Navigation intuitive de type navigateur, avec historique de navigation, onglets et signets
Outils de recherche	Outils de recherche d'éléments et de références ultraperformants
Filtrage rapide	Filtrage des listes d'éléments, des tableaux et des cellules de stratégies avec fonction de saisie semi-automatique
Prise en charge de la sélection multiple	Exécution d'actions et validation des modifications sur des centaines d'éléments à la fois
Outils de nettoyage du système	Les administrateurs peuvent identifier facilement les éléments et les règles inutilisés.
ADMINISTRATION	
Escalade des alertes	Les administrateurs peuvent faire suivre les alertes du systèmes via e-mail, SMS, interruption SNMP, scripts personnalisés
Seuils d'alerte	Seuils d'alerte automatiques pour les statistiques de vue d'ensembles
Journaux d'audit	Informations d'audit approfondies sur toutes les modifications du système
Rapports système	Rapports d'inventaire et d'audit sur les activités des administrateurs
Installation Plug-and-Play	Installation automatique : via le cloud (ou clé USB) avec répartition des stratégies
Tâches automatisées	Actualisation des stratégies ; archivage, exportation et suppression des journaux ; exécution de sauvegardes
Domaines	Division de l'environnement en domaines de configuration isolés
Importation/Exportation	Formats XML and CSV avec gestion intelligente des conflits entre les installations de Forcepoint NGFW SMC

SPÉCIFICATIONS DE FORCEPOINT NGFW SECURITY MANAGEMENT CENTER

Outil de messagerie	Outil de messagerie administrateur intégré
Mises à niveau distantes	Mise à niveau distante sans échec en un clic
Contrôle d'accès basé sur les rôles	Contrôle souple et précis des autorisations des administrateurs
Gestion des licences	Mises à jour des licences en ligne et rapports d'état des contrats de maintenance automatisés
Outils de dépannage à distance	Outil de capture du trafic intégré, diagnostic, téléchargement d'instantanés de configuration provenant du pare-feu, vues de surveillance des sessions
GESTION DE POLITIQUE	
Contextes virtuels	Possibilité de partager un même contexte maître sur plusieurs domaines SMC - jusqu'à 250 contextes virtuels pouvant chacun avoir ses propres stratégies et tables de routage
Gestion hiérarchique des politiques	Les modèles, sous-politiques, alias, et commentaires préservent la clareté et l'organisation
Identification des applications	Possibilité d'identifier les applications selon la charge et de restreindre l'accès en fonction
Filtrage d'URL	Restriction de l'accès selon les catégories d'URL
Noms de domaines	Restriction de l'accès de façon dynamique à l'aide des noms de domaines
Identification des utilisateurs	Création de règles basées sur les utilisateurs, avec ou sans authentification
Zones	Marquage des interfaces par des zones et repérage dans les politiques
Politiques d'inspection	Contrôle granulaire de l'inspection profonde et gestion facilitée des faux positifs
Politiques de qualité de service (QoS)	Configuration des politiques basée sur les classes QoS
Filtrage des fichiers	Définir la manière d'inspecter les fichiers
Translation d'adresse réseau (NAT)	• NAT par défaut • A base de composants • A base de politiques
Outil de validation des politiques	Identification des erreurs de configuration avant l'activation des politiques
Instantanés des politiques	Permettent d'explorer et de comparer l'historique de configuration des pare-feux
Restauration des politiques	Une version antérieure d'une stratégie peut être récupérée et téléchargée sur le firewall
Outil d'optimisation de l'utilisation des règles	Indique combien de fois chaque règle a été appliquée au cours d'une période donnée
Outil de recherche de règles	Recherche des règles dans les politiques
Noms de règles	Création des noms de règles visibles dans les journaux, les statistiques et les rapports
Téléchargement sans échec des politiques	Le système restaure automatiquement la version précédente si la nouvelle version échoue
CONFIGURATION	
Routage	Configuration du routage par glisser-déposer
Anti-usurpation automatique	Configuration anti-usurpation créée automatiquement en fonction du routage
IPsec VPN	Editeur de VPN et diagrammes de VPN faciles à utiliser qui révèlent la topologie sous-jacente
SSL VPN	Configuration se portail SSL VPN Portal et de SSL VPN à base de tunnel
VPN basé sur route	Definition des interfaces tunnel et exploitation en VPN basé sur route
Gestion des Incidents	Outils intégrés pour la gestion collaborative des incidents réseau
Assistant de création d'éléments	Création de centaines d'éléments firewall via un Assistant
Authentification via le navigateur	Configuration et personnalisation d'un service d'authentification convivial sur navigateur

SPÉCIFICATIONS DE FORCEPOINT NGFW SECURITY MANAGEMENT CENTER

ETATS, STATISTIQUES ET RAPPORTS	
Surveillance de l'état des systèmes	Informations en temps réel sur l'état des équipements réseaux et leurs connexions
Surveillance de l'état des appliances	Suivi graphique de l'état matériel des boitiers
Diagrammes réseau	Visualisation des configurations, les topologies et l'état de la connectivité à l'aide de graphiques
Surveillance des sessions	Vues dédiées permettant de surveiller les connexions, les associations de sécurité des VPN, les utilisateurs authentifiés, les alertes actives et les itinéraires de routage dynamique et statiques
Vues d'ensemble	Ttableaux de bord des statistiques réseau personnalisés pour la surveillance en temps réel
Géolocalisation	• Identifier les pays correspondant à toutes les adresses IP grâce à des drapeaux et à des statistiques de géolocalisation. • Déterminer l'origine des attaques réseau.
Rapports	Personnaliser et programmer les rapports offrant des informations détaillées sur les statistiques réseau
Rapports	Accès web léger aux politiques, aux journaux et aux rapports
GESTION DES EVENEMENTS TIERS	
Surveillance des équipements tiers	Permet aux administrateurs de surveiller et les changements d'état dans la disponibilité des équipements tiers.
Réception des journaux des équipements tiers	Analyse et réception des journaux au format syslog pour les équipements tiers. Prise en charge native des formats CEF, LEEF, CLF et WELF
Réception NetFlow/IPFIX	Possibilité de recevoir et de consolider les données aux formats NetFlow v9 et IPFIX
Statistiques des équipements tiers	Rapports et statistiques graphiques basés sur les données de journal des équipements tiers et les compteurs SNMP
Nombre d'équipements tiers pris en charge	200 par serveur de logs
Licences	Chaque équipement tiers consomme 0,2 unités du compteur d'équipements sous licence du serveur de gestion
JOURNAUX	
Explorateur de journaux	Vue de navigation commune pour toutes les données de journal
Filtrage par glisser-déposer	Glisser-déposer pour n'importe quelle cellule de données de journal dans le volet de requête
Statistiques des journaux	Créer des statistiques des journaux à la volée et visualiser les principales tendances
Visualisation des journaux	Identifier les anomalies du trafic enregistré grâce aux fonctions de visualisation des journaux avec filtres intégrés
Agrégation des journaux	Regrouper de grandes quantités de données de journal filtrées par colonnes
Archivage	Archiver les journaux dans plusieurs répertoires à l'aide de filtres
Sauvegardes	Mécanisme de sauvegarde intégré pour la configuration des serveurs de journaux et les données de journal
Exportation des journaux	Exportation des journaux aux formats CSV, XML, CEF et LEEF ; les journaux peuvent également être exportés directement dans des fichiers PDF et ZIP à partir de l'explorateur de journaux.
Redirection des journaux	Redirection en temps réel des journaux aux formats syslog, CEF, LEEF, XML, CSV, IPFIX et NetFlow
Contextes de données de journal	Raccourcis permettant de naviguer dans les différents types de journaux avec jeux de colonnes dédiés
Haute disponibilité	Prise en charge de serveurs de journaux redondants

LA LICENCE FORCEPOINT DE L'ADMINISTRATION DE DOMAINES POUR UNE GESTION CENTRALISÉE DE MULTIPLES ENVIRONMENTS

La tâche des fournisseurs de services de sécurité managés (les MSSPs) est souvent compliquée par la charge d'administration et les coûts liés à la gestion de plusieurs serveurs par domaine. Les configurations peuvent désormais être partagées entre les domaines. et permettent des modifications rapides. L' architecture unique de la solution simplifie facilite la gestion et la maintenance des environnements des MSSP. Les responsabilités des administrateurs peuvent être définies de façon précise et l'accès peut être limité aux seuls domaines qu'ils contrôlent. Les MSSP peuvent également fournir à leurs clients des services supplémentaires en leur offrant un accès aux rapports, aux configurations de stratégies et aux journaux via un portail web fiable et léger.

SPÉCIFICATIONS DE DOMAINES FORCEPOINT

DOMAINES	
Nombre maximum de domaines	200
Nombre d'administrateurs	Illimité
Nombre d'équipements managés par domain	Illimité
Nombre d'éléments par domaine	Illimité
FONCTIONNALITÉS	
Séparation des configurations	Isolez les environnements clients dans des domaines différents de sorte que les composants réseau des clients ne se confondent jamais.
Partage des configurations	Partagez des éléments tels que les modèles de stratégies pour tous les domaines.
Contrôle d'accès	Configurez la visibilité et les responsabilités des administrateurs à l'aide des domaines.
Surveillance	Surveillez l'état de tous les domaines alloués à l'aide de la vue d'ensemble des domaines.
Personnalisation	Personnalisez les modèles de style PDF.
Outils de migration	Déplacez les composants entre les domaines grâce à l'outil de déplacement intégré.
Importation/Exportation	Importez et exportez des réseaux entre différents domaines et installations de Forcepoint SMC
Contextes virtuels	Partagez un même contexte maître sur les domaines pour 250 contextes virtuels au maximum, chacun pouvant disposer de ses propres stratégies et tables de routage

FORCEPOINT SMC WEB PORTAL

Le portail web offre aux clients et aux administrateurs une solution légère pour scruter les journaux, les rapports programmés, les politiques actuelles, et l'historique de changement de politiques. Les administrateurs MSSP ont la possibilité deparamétrer la quantité d'informations affichées sur le portail et l'adapter aux besoins des clients finaux.

Forcepoint SMC Web Portal peut être utilisé en anglais, français et espagnol. D'autres langues peuvent.être ajoutées à la demande.

AVANTAGES CLÉS

- Accès en lecture seule aux journaux, rapports, politiques, et historique de changement de politiques.
- Etat du réseau en temps réel selon les droits utilisateurs.
- Prise en charge d'appareils mobiles.

LES SPÉCIFICATIONS DE FORCEPOINT SMC WEB PORTAL

SPÉCIFICATIONS	
Nombre maximal d'utilisateurs simultanés	250 par licence
Nonmbre d'administrateurs	Illimité
Nombre d'utilisateurs du portail web	Licence limitée
Authentification des utilisateurs	Base de donnée de serveur de gestion, RADIUS TACACS+
Connexion des équipements	SSL avec chiffrement
FONCTIONNALITÉS	
Politiques de sécurité	Affichez les dernières configurations des pare-feux de nouvelle génération au format HTML.
Rapports	Affichez les rapports dont la publication est planifiée dans Forcepoint SMC Web Portal au format HTML.
Navigation dans les journaux	Naviguez dans les journaux en appliquantdes filtres au format HTML.
Détails du journal	Affichez les visualisations du journal des événements et d'autres détails des journaux dans une page HTML distincte.
Exportation au format PDF	Imprimez les rapports et les journaux au format PDF.
Annonces	Les administrateurs peuvent spécifier des annonces à afficher dans Forcepoint SMC Web Portal.
Comparaison de politiques	Comparez les différentes versions des configurations des pare-feux pour voir si votre demande de modification a été implémentée.
Traduction	Le portail web peut être facilement traduit dans n'importe quelle langue
Personnalisation	Personnalisez l'aspect du portail Web

CONTACT

www.forcepoint.com/contact

A PROPOS DE FORCEPOINT

[DATASHEET_FORCEPOINT_NGFW_SECURITY_MANAGEMENT_CENTER_FR] 100030FR.030117