Forcepoint

Scheda dati

NGFW Security Management Center

Amministrazione da una console unificata per la massima visibilità su tutta la rete

Vantaggi principali

- Possibilità di gestire da una console unificata fino a 6000 NGFW Forcepoint fisici o virtuali in ambienti distribuiti
- Flessibilità e scalabilità per la distribuzione in grandi reti aziendali
- High Availability opzionale per esigenze di uptime importanti
- Policy intelligenti e automazione efficiente dei flussi di lavoro per una distribuzione e manutenzione rapide e accurate di Forcepoint NGFW
- Contestualizzazione, sensibilizzazione e visibilità di utenti ed endpoint in tutta la rete, dal data center e dal perimetro alle filiali e al cloud
- Scelta di opzioni di implementazione software o tramite appliance

Forcepoint NGFW Security Management Center (SMC) centralizza e unifica la gestione di tutti i modelli di Next Generation Firewall Forcepoint, fisici, virtuali o cloud, in ambienti aziendali di grandi dimensioni e geograficamente distribuiti.

Grazie alla superiorità delle sue caratteristiche di flessibilità, scalabilità e facilità d'uso, Forcepoint Security Management Center (SMC) semplifica la gestione degli ambienti di sicurezza di rete dinamici, preparandoli a supportare piani di crescita aziendale aggressivi. Le policy intelligenti consentono di esprimere i processi aziendali in un linguaggio naturale, mentre i flussi di lavoro ottimizzati snelliscono le attività amministrative quotidiane per un'elevata efficienza e un basso TCO.

SMC offre una visibilità a 360 gradi su tutte le reti aziendali, mediante l'acquisizione di informazioni sulla gestione degli eventi e sul monitoraggio dello stato dagli NGFW Forcepoint, dagli endpoint e da dispositivi di terze parti, per condurre indagini interattive e produrre report dettagliati. Inoltre Forcepoint SMC può aggregare i dati di log NGFW provenienti da svariati log server Forcepoint NGFW distribuiti sul territorio, per generare dei report consolidati e mantenere, nel contempo, la sovranità dei dati.

High availability

Le aziende di oggi hanno una tolleranza zero per le interruzioni, cioè richiedono un accesso H24 alle risorse critiche. L'opzione di elevata disponibilità di Forcepoint SMC offre l'accesso costante alle risorse di log, per garantire la resilienza delle attività di analisi e risposta agli incidenti.

Client di gestione della sicurezza

Indipendentemente dalla posizione geografica, gli amministratori possono accedere in modo sicuro a Forcepoint SMC utilizzandone il client di gestione. Il client mette a loro disposizione una potente interfaccia utente grafica per la configurazione, il monitoraggio, la registrazione, gli avvisi, i report, gli aggiornamenti e gli upgrade dei Next Generation Firewall Forcepoint. Il client di Forcepoint SMC offre agli amministratori una visione olistica della rete e opzioni di drill-down guidate dal contesto per una gestione rapida ed efficace dell'intero ambiente di sicurezza.

Specifiche di Forcepoint NGFW SMC

SERVER DI GESTIONE	
Numero di dispositivi gestiti	Con licenza: da 1 a 6000 nodi con un unico serverdi gestione
Numero di amministratori	Nessun limite
Numero di elementi	Nessun limite
Numero di policy	Nessun limite
Numero di log server	Nessun limite
Numero di Web Portal Server	Nessun limite
Autenticazione dell'amministratore	Database locale, RADIUS. TACACS+, certificato client e Microsoft Active Directory (LDAP)
Connessioni dispositivi	Con crittografia TLS
LOG SERVER	
Numero di dispositivi supportati	Nessun limite
Record di log al secondo	Il sistema di registrazione ad alte prestazioni può ricevere più di 500.000 record al secondo
Connessioni dispositivi	Con crittografia TLS 1.2 e autenticazione con certificati e chiavi X.509v3
Dimensione di archiviazione log	Nessun limite
Numero di inoltro di log per log server	Nessun limite
GENERALE	
Client di gestione	Interfaccia utente basata su HTML5
Application Programming Interface SMC (API SMC)	API documentata che consente una facile integrazione di prodotti e servizi di terze parti. Basata sull'architettura REST, che può utilizzare la codifica dati XML o JSON
Amministratori simultanei	Più amministratori possono apportare modifiche contemporaneamente. Elementi critici come le policy sono protetti da modifiche
Dashboard della schermata Home	Dashboard personalizzabili della schermata Home per NGFW, VPN, utenti e altri elementi
Monitoraggio utenti	In aggiunta ai controlli e alle correlazioni in base al comportamento degli utenti, offre informazioni sullo stato di sicurezza e statistiche sulle applicazioni negli endpoint

Alta disponibilidad	Hasta cuatro servidores de administración en espera
Actualizaciones	Se pueden descargar automáticamente actualizaciones y paquetes de actualizaciones dinámicas
Respaldos	Herramienta de respaldo integrada para realizar copias de respaldo de todo el sistema, incluso de todas las configuraciones de los firewall de última generación
Navegación	Navegador intuitivo con historial de navegación, pestañas y favoritos
Herramientas de búsqueda de destacados	Herramientas de búsqueda eficientes de referencia y elementos con acciones rápidas contextuales
Filtrado rápido	Filtrado conveniente de escritura anticipada en listas de elementos, tablas y celdas de políticas
Soporte multiselección	Realice acciones e implemente cambios a cientos de elementos simultáneamente
Herramientas de limpieza del sistema	Permiten que el administrador encuentre fácilmente qué elementos y reglas no se utilizan
ADMINISTRACIÓN	
Escalamientos de alertas	Permiten que el administrador reenvíe alertas desde el sistema por medio de correo electrónico, SMS, captura de SNMP y scripts personalizados
Umbrales de alertas	Establecimiento sencillo de umbrales de alertas para revisar las estadísticas
Registros de auditoría	Todos los cambios al sistema se registran en registros de auditoría
Informes del sistema	Informes de auditoría de inventario y cumplimiento sobre las actividades y cuentas de los administradores
Aprovisionamiento sin intervención	Instalación desde la nube (o una unidad USB) con inserción de políticas inicial
Tareas automatizadas	Gestión de datos del registro, archivado y retención, copias de respaldo, actualizaciones y tareas de renovación de políticas automatizadas
Dominios administrativos	Permiten la división del entorno en dominios de configuración aislados
Importación/Exportación	Exportación e importación de XML y CSV en todo momento, en lugar de solo entre instalaciones
Actualizaciones remotas	Actualización remota con un solo clic y a prueba de errores de los NGFW administrados
Control de acceso basado en el rol del administrador	Además de los roles predefinidos, se pueden definir y combinar roles personalizados (p. ej., Propietario, Visualizador, Operador, Editor, Superusuario) para controlar la flexibilidad y precisión de los permisos
Administración de licencias	Informes de estado del contrato de mantenimiento y actualizaciones de licencias en línea y de forma automática
Administración de certificados	Vista consolidada de todos los certificados y las credenciales
Herramientas de resolución de problemas	Amplias capacidades de diagnóstico remoto: herramienta de captura de tráfico integrada, descarga de instantánea de configuración desde el firewall de última generación y vistas de monitoreo de la sesión
Gestión de casos de incidentes	Herramientas integradas para la gestión colaborativa de incidentes de redes

GESTIONE DELLE POLICY	
Motore NGFW virtuale	Condivisione dello stesso contesto master tra diversi domini amministrativi SMC; fino a 250 contesti virtuali, ognuno con le proprie policy e tabelle di routing
Gestione gerarchica delle policy	Le policy sono organizzate e documentate con modelli di policy, policy secondarie, alias e sezioni con i commenti alle regole
Identificazione delle applicazioni	→ Limita l'accesso in base alle applicazioni degli endpoint e/o della rete → Limita gli accessi alle/dalle applicazioni in base al payload → Stabilisci le liste delle applicazioni consentite/bloccate in base al nome e alla versione dell'applicazione forniti da Endpoint Context Agent di Forcepoint
Gestione delle modifiche	La distribuzione delle modifiche è vincolata alla revisione e approvazione di un secondo amministratore
Filtraggio degli URL	Limita l'accesso in base alle categorie di URL
Nomi di dominio	Limitano l'accesso in modo dinamico mediante nomi di dominio che possono essere tradotti in indirizzi IP
Identificazione degli utenti	Abbina le regole basate sugli utenti mediante l'identificazione trasparente degli utenti o l'applicazione di metodi di autenticazione avanzata
Zone	Le interfacce fisiche possono essere contrassegnate con zone a cui fare riferimento nelle policy
Geoprotezione	Limita gli accessi base ai Paesi o alle aree geografiche
Policy di ispezione	Controllo granulare per l'ispezione approfondita dei pacchetti; opzioni semplici consentono di escludere i falsi positivi
Policy QoS (Quality of Service)	Configurazione di policy QoS in base alle classi
Filtraggio dei file in base alle policy	Definisce il modo in cui vengono ispezionati i file utilizzando la reputazione dei file di McAfee Global Threat Intelligence, Anti-Malware Scan e McAfee Advanced Threat Defense
Network Address Translation (NAT)	→ NAT predefinita → NAT basata sugli elementi → Policy NAT
Strumento di validazione delle policy	Aiuta l'amministratore a trovare gli errori di configurazione prima dell'attivazione delle policy
Snapshot delle policy	Consente di esplorare e comparare la cronologia di configurazione dei Next Generation Firewall Forcepoint
Ripristino delle policy	È possibile recuperare una versione precedente delle policy e caricarla sul Next Generation Firewall
Strumento per l'ottimizzazione dell'utilizzo delle regole	Consente agli amministratori di vedere quanti match si sono verificati per ogni regola su un periodo di tempo specificato
Strumento di ricerca delle regole	Strumento integrato per la ricerca di regole nelle policy
Nomi regole	Possibilità di creare nomi di regole visibili nei log, nelle statistiche e nei report
Caricamento di policy a prova di errore	Il sistema ripristina automaticamente la versione precedente delle policy se la nuova versione restituisce un errore

CONFIGURAZIONE	
Routing	Configurazione di routing drag-and-drop per i firewall e widget specifici per aggiungere route e route predefinite
Routing dinamico	Configurazione avanzata dei protocolli OSPF e BGP tramite un'interfaccia utente grafica intuitiva
Anti-spoofing automatico	La configurazione anti-spoofing viene creata automaticamente in base al routing
VPN Site-to-Site	→ VPN IPsec basata su policy → VPN IPsec basata su route e tunneling (GRE)
VPN di accesso remoto	→ Client VPN IPsec (iOS e Windows) → Client VPN SSL (Android, Mac e Windows) → Portale VPN SSL senza client
Gestione di Endpoint Context Agent	Estende la visibilità e il controllo degli accessi alle applicazioni in esecuzione sugli endpoint
Creazione guidata di elementi firewall	Consente di creare centinaia di elementi firewall attraverso una procedura guidata per la creazione di firewall
Autenticazione utenti basata su browser	Consente di configurare e personalizzare facilmente per gli utenti un servizio di autenticazione basato su browser
STATO, STATISTICHE E REPORT	
Monitoraggio dello stato del sistema	Informazioni in tempo reale sullo stato dei dispositivi di rete e le loro connessioni
Monitoraggio dello stato delle appliance	Vista grafica dello stato hardware delle appliance
Diagrammi delle reti	Rappresentazione grafica di configurazioni, topologie e stato della connettività
Monitoraggio sessioni	Viste dedicate a monitorare le connessioni, le associazioni di sicurezza (SA) VPN, gli utenti autenticati, gli avvisi attivi e le route dinamiche e statiche
Panoramiche	Possibilità di personalizzare le dashboard delle statistiche di utenti e rete per il monitoraggio in tempo reale
Geolocalizzazione	Mostra le informazioni sui Paesi per tutti gli indirizzi IP tramite bandiere nazionali e statistiche di geolocalizzazione. Mostra da dove provengono gli attacchi alla rete
Report	È possibile personalizzare e pianificare report che forniscono informazioni dettagliate sulle statistiche di rete
Portale web	Accesso in sola lettura per vedere policy, log e report pianificati

GESTIONE DI TERZI	
Monitoraggio dispositivi	Consente all'amministratore di monitorare e visualizzare i cambiamenti di stato nella disponibilità dei dispositivi di terzi
Aggiunta log dispositivi	Analisi e ricezione dei log in formato syslog per dispositivi di terzi e supporto preconfigurato per i formati CEF, LEEF, CLF e WELF
Ricezione NetFlow/IPFIX	Possibilità di ricevere, inoltrare e unificare dati nei formati NetFlow v9 e IPFIX
Statistiche dispositivi	Statistiche grafiche e report basati su dati di log di terzi e contatori SNMP (Simple Network Management Protocol)
Numero di dispositivi supportati	200 per log server
Licenze	Ogni dispositivo di terzi consuma 0,2 unità del numero di dispositivi previsti dalla licenza del server di gestione
LOG	
Browser	Vista granulare per tipi di log separati in aggiunta alla vista di consultazione comune per tutti i dati di log
Filtraggio drag-and-drop	Filtraggio interattivo dei log mediante trascinamento di una cella di dati di log nel pannello delle query
Statistiche	Crea contatori integrati basati sui log e statistiche on-demand per attività di reportistica, monitoraggio e generazione di avvisi
Rappresentazioni grafiche	Trova le anomalie nel traffico registrato usando rappresentazioni grafiche e filtrabili dei log
Analizzatore di log	Crea aggregazioni libere su grandi quantità di dati di log filtrati in base a una colonna qualsiasi
Archiviazione	Duplica o archivia i log nelle directory in base a filtri, tempi o tipi di dati dei log
Backup	Pianificatore di backup integrato per i dati di configurazione e di log del log server
Esportazioni	Esportazione di log in formato CSV, XML e LEEF; i log possono essere anche report di snapshot
Inoltro	Reindirizzamento dei log in tempo reale in syslog; formati CEF, LEEF, XML, CSV, IPFIX, NetFlow e McAfee Enterprise Security Manager; disponibile la configurazione per il filtraggio, il tipo di dati e la selezione del campo di log
Contesti dati	Scorciatoie per consultare diversi tipi di log con set di colonne contestuali e personalizzabili
High Availability	Supporto per assegnare log server primari e di backup per ogni origine di log

Gestione centralizzata di più ambienti dei clienti

I fornitori di servizi di sicurezza gestita (MSSP) hanno l'esigenza di ridurre gli elevati costi amministrativi associati alla gestione di più server su più domini. Forcepoint Administrative Domain License consente di gestire gli ambienti di vari clienti attraverso un unico server di gestione. Le configurazioni possono essere riutilizzate e condivise tra i vari domini per una distribuzione rapida ed efficiente delle modifiche. L'architettura esclusiva della soluzione Forcepoint Administrative Domain License semplifica gli ambienti aziendali ed MSSP, rendendone più facile la manutenzione. Il controllo degli accessi basato sui ruoli (RBAC) assicura una definizione accurata delle responsabilità dell'amministratore e delle limitazioni di accesso ai domini. I clienti basati su domini possono accedere facilmente ai report, alle configurazioni delle policy e ai log tramite un portale web sicuro e leggero.

Specifiche di Forcepoint Administrative Domain License

DOMINI	
Numero massimo	1000
Numero di amministratori	Nessun limite
Numero di dispositivi gestiti	6000
Numero di elementi	Nessun limite
CARATTERISTICHE	
Separazione delle configurazioni	Consente di isolare in domini amministrativi diversi gli ambienti gestiti e di assicurarsi che gli elementi di rete di clienti diversi non si confondano
Condivisione delle configurazioni	Condivisione di elementi, come i modelli di policy, per tutti i domini
Controllo degli accessi	Con l'aiuto di domini amministrativi separati, si possono concedere o limitare i diritti di accesso degli amministratori alla configurazione e la visibilità
Monitoraggio	Monitoraggio dello stato di tutti i domini accordati, con l'aiuto della panoramica sui domini
Personalizzazione con il brand	Report PDF personalizzabili con il brand tramite modelli di stile
Strumenti di migrazione	Consente di spostare elementi tra i domini con lo strumento integrato "move-to"
Importazione/esportazione	Consente di importare ed esportare elementi tra vari domini e installazioni SMC
Motore NGFW virtuale	Condivisione dello stesso contesto master tra i confini dei domini; fino a 250 contesti virtuali, ognuno dei quali può avere le proprie policy e tabelle di routing

Forcepoint Web Portal Server

Forcepoint Web Portal Server fornisce a clienti, amministratori e management degli MSSP un'interfaccia web leggera per la visualizzazione dei log, dei report pianificati, delle policy correnti e della cronologia delle modifiche alle policy. Gli amministratori degli MSSP possono configurare la quantità di informazioni visualizzate sul portale in base alle esigenze del cliente o per ridurre le richieste di assistenza.

Forcepoint Web Portal Server supporta l'inglese, lo spagnolo e il francese in nativo, con la possibilità di aggiungere altre lingue.

Vantaggi principali

- → Accesso senza client e in sola lettura a log, report, policy e cronologia delle modifiche alle policy
- → Stato della rete in tempo reale disponibile per utenti specifici
- → Supporto per dispositivi mobili

Specifiche di Forcepoint Web Portal Server

SPECIFICHE	
Numero massimo di utenti simultanei	250 per Web Portal Server
Numero di amministratori	Nessun limite
Numero di utenti del portale web	Nessun limite
Autenticazione utenti	Database del server di gestione, RADIUS, TACACS+
Connessioni dispositivi	Con crittografia TLS
CARATTERISTICHE	
Policy di sicurezza	Visualizza le configurazioni più recenti dei Next Generation Firewall in formato HTML
Report	Visualizza i report di cui è pianificata la pubblicazione nel portale web in formato HTML
Consultazione dei log	Consultazione e filtraggio dei log in formato HTML
Dettagli dei log	Monitoraggio dello stato di tutti i domini accordati, con l'aiuto della panoramica sui domini
Esportazione PDF	L'esportazione PDF consente di scaricare i report in formato PDF
Annunci	Gli amministratori possono impostare la visualizzazione degli annunci nel portale web
Confronto tra policy	Confronta le diverse versioni della configurazione dei Next-Generation Firewall per vedere se la richiesta di modifica è stata implementata
Localizzazione	Il portale web supporta l'inglese, lo spagnolo e il francese e può essere facilmente tradotto per supportare altre lingue
Personalizzazione	L'aspetto dei portali web è personalizzabile

Appliance Forcepoint SMC

L'appliance Forcepoint SMC (Security Management Center) è un dispositivo dedicato all-in-one per la configurazione, la gestione e il monitoraggio degli NGFW Forcepoint fisici, virtuali e basati su cloud. Forcepoint SMC offre una distribuzione semplificata per un'operatività immediata, combinando il log server e il server di gestione dell'NGFW di Forcepoint in un unico pacchetto plug-and-play funzionante su hardware 1U ottimizzato.

Opzioni di distribuzione di Forcepoint NGFW SMC

Forcepoint SMC può essere distribuito in tre modi: sui sistemi, sull'hardware o hypervisor oppure come appliance all-in-one[1].

1 Deve essere acquistata una licenza software SMC distinta per ognuna delle tre opzioni di distribuzione. Le singole appliance non includono licenze.

	OPZIONI DI DISTRIBUZIONE DI FORCEPOINT NGFW SMC		
COMPONENTI	SOFTWARE	IMMAGINE ISO	APPLIANCE
Software SMC	●	●	●
Sistema operativo	Fornito dal cliente	●	●
Hardware/piattaforma	Fornito dal cliente	Fornito dal cliente	●

Specifiche dell'appliance Forcepoint SMC

PRESTAZIONI	
Firewall gestiti	2.000
Numero massimo domini	200
Log indicizzati al sec.	80.000
Eventi giornalieri	6.912.000.000
Dimensione log giornaliero (GB)	690

Specifiche dell'appliance Forcepoint SMC

SPECIFICHE FISICHE	
Formato	1U
Processore	2x Intel Xeon
Memoria	32 GB
Archiviazione (HDD)	Capacità di 900 GB (4x 300 GB, RAID-5), hot-swap
Alimentazione	2x 550 W (100 V ~ 240 V), hot-swap
Dimensioni	Profondità 60,7 cm x larghezza 43,42 cm x altezza 4,28 cm
Peso	28.26 lbs. 12,82 kg
Normative e conformità	FCC / ICES / EN55022 / VCCIBSMI / C-Tick / SABS / CCC / MIC Classe A e UL60950-1 / Conforme alla Direttiva RoHS

Ordinazione di Forcepoint SMC

ORDINAZIONE	N. PARTE
Forcepoint NGFW Security Management Center (software)	SMCX
Forcepoint NGFW Security Management Center 1000 Appliance	SMCAP
Forcepoint NGFW Security Management Center High Availability (disponibile solo per distribuzione di immagine ISO e software)	SMCHAX
Forcepoint SMC Additional Log Server	ALSX
Forcepoint SMC Domains (fino a 200 domini)	ODFSMCX
Forcepoint SMC Web Portal	OWPSX