

NGFW Security Management Center

Administración desde un único panel para una visibilidad máxima de la red

Principais beneficios

- › Administración centralizada desde un único panel de hasta 6000 Forcepoint NGFW físicos o virtuales en entornos distribuidos
- › Flexibilidad y escalabilidad para el despliegue en redes empresariales grandes
- › Opción de alta disponibilidad para requisitos de tiempo productivo exigentes
- › Smart Políticas y automatización de flujos de trabajo eficientes para el despliegue y mantenimiento rápidos y precisos de Forcepoint NGFW
- › Contexto, reconocimiento y visibilidad de usuarios y dispositivos finales en toda la red, desde la central de datos y el borde a las sucursales y la nube
- › Elección de opciones de despliegue de software o dispositivo

El centro de gestión de seguridad Forcepoint NGFW Security Management Center (SMC) brinda una administración centralizada y unificada de todos los modelos de Forcepoint Next Generation Firewalls, ya sean físicos, virtuales o en la nube, a lo largo de entornos empresariales grandes y distribuidos geográficamente.

Com flexibilidade, escalabilidade e facilidade de uso superiores, o Forcepoint Security Management Center (SMC) torna os ambientes de segurança de rede dinâmicos mais administráveis e compatíveis com planos de crescimento de negócios agressivos. As Políticas Inteligentes permitem que os processos de negócios sejam expressos em termos naturais, e os fluxos de trabalho otimizados dinamizam as tarefas administrativas diárias para alta eficiência e baixo custo total de propriedade (TCO).

O SMC fornece visibilidade em 360 graus nas redes corporativas, obtendo informações de administração de eventos e monitoramento de status de Forcepoint NGFWs, endpoints e dispositivos de outros fornecedores para investigação interativa e também relatórios detalhados. Além disso, o Forcepoint SMC pode agregar dados de registro de NGFW de vários Forcepoint NGFW Log Servers geograficamente distribuídos para gerar relatórios consolidados, mantendo a soberania dos dados.

Alta disponibilidad

Las empresas de hoy tienen cero tolerancia a las interrupciones, y requieren acceso constante a los recursos críticos. Con la opción de alta disponibilidad de Forcepoint SMC, las organizaciones mantienen un acceso ininterrumpido a los recursos de registro para un análisis y una respuesta frente incidentes resiliente.

Cliente de gestión de seguridad

Sin importar la ubicación geográfica, los administradores pueden acceder de manera segura a Forcepoint SMC a través del cliente de gestión. Este cliente cuenta con una interfaz de usuario gráfica poderosa para configuración, monitoreo, registro, alertas, informes y actualizaciones de Forcepoint Next Generation Firewalls. El cliente de Forcepoint SMC ofrece a los administradores una vista holística de la red y acciones exhaustivas e impulsadas por el contexto para administrar de forma rápida y eficiente todo el entorno de seguridad.

Especificaciones de Forcepoint NGFW SMC

| SERVIDOR DE ADMINISTRACIÓN | |
|---|---|
| Cantidad de dispositivos administrados | Con licencia: De 1 a 6000 nodos con un servidor de administración |
| Cantidad de administradores | Ilimitada |
| Cantidad de elementos | Ilimitada |
| Cantidad de políticas | Ilimitada |
| Cantidad de servidores de registro | Ilimitada |
| Cantidad de servidores de portal web | Ilimitada |
| Autenticación de administradores | Base de datos local, RADIUS, TACACS+, certificados de clientes y Microsoft Active Directory (LDAP) |
| Conexiones de dispositivos | Cifrado TLS |
| SERVIDOR DE REGISTRO | |
| Cantidad de dispositivos admitidos | Ilimitada |
| Registros por segundo | El sistema de registro de alto desempeño puede recibir hasta 500 000 registros por segundo |
| Conexiones de dispositivos | TLS 1.2 cifrada y autenticada mediante el uso de claves y certificados X.509v3 |
| Tamaño de almacenamiento de registros | Ilimitada |
| Cantidad de reenvíos de registros por servidor de registros | Ilimitada |
| GENERAL | |
| Ciente de gestión | UI basada en HTML5 |
| Interfaz de programación de aplicaciones de SMC (SMC API) | API documentada que posibilita la integración fácil de servicios y productos de terceros. Utiliza arquitectura REST en la que los datos pueden codificarse como XML o JSON |
| Administradores simultáneos | Varios administradores pueden realizar cambios al mismo tiempo y los elementos críticos, como las políticas, se bloquean para que no puedan editarse |
| Paneles de pantalla de inicio | Paneles de pantalla de inicio personalizables para NGFW, VPN, usuarios y otros elementos |
| Monitoreo de usuarios | Además de las verificaciones y correlaciones respecto del comportamiento del usuario, brinda información sobre el estado de seguridad de dispositivos finales y estadísticas sobre aplicaciones de dispositivos finales |

| | |
|--|--|
| 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 |
| Umbral 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 |

ADMINISTRACIÓN DE POLÍTICAS

| | |
|--|--|
| Motor NGFW virtual | Comparta un mismo contexto maestro entre distintos dominios administrativos de SMC; hasta 250 contextos virtuales, cada uno con sus propias políticas y tablas de enrutamiento |
| Administración de políticas jerárquicas | Las plantillas de políticas, subpolíticas, alias y secciones de comentarios de reglas mantienen la política organizada y entendible |
| Identificación de aplicaciones | <ul style="list-style-type: none"> → Restrinja el acceso según las aplicaciones de dispositivos finales o redes → Restrinja el acceso desde/a aplicaciones según la carga → Permita lista/bloquee lista por nombre de aplicación y versión desde el agente de contexto de dispositivo final de Forcepoint |
| Administración de cambios | Requiera la revisión y aprobación de un segundo administrador antes de desplegar los cambios |
| Filtrado de URL | Restrinja el acceso por categorías de URL |
| Nombres de dominio | Restrinja el acceso dinámicamente utilizando nombres de dominio que puedan traducirse en direcciones IP |
| Identificación de usuarios | Haga coincidir reglas basadas en usuarios mediante la identificación de usuarios transparente o la aplicación de métodos de autenticación fuertes |
| Zonas | Las interfaces físicas se pueden etiquetar con zonas y hacer referencia a ellas en las políticas |
| Protección geográfica | Restrinja el acceso por países o regiones geográficas |
| Políticas de inspección | Control granular para la inspección profunda de paquetes y formas fáciles de desactivar falsos positivos |
| Políticas de calidad de servicio (QoS) | Configuración de políticas basada en la clase de QoS |
| Filtrado de archivos basado en políticas | Defina de qué manera se inspeccionan los archivos con la reputación de archivos de McAfee Global Threat Intelligence, Anti-Malware Scan y McAfee Advanced Threat Defense |
| Traducción de direcciones de red (NAT) | <ul style="list-style-type: none"> → NAT predeterminada → NAT basada en elementos → Políticas de NAT |
| Herramienta de validación de políticas | Ayuda al administrador a encontrar errores en la configuración antes de la activación de las políticas |
| Instantáneas de políticas | Permite la exploración y comparación del historial de configuración de Forcepoint Next Generation Firewall |
| Restauración de políticas | Se puede recuperar la versión anterior de una política y cargarla al firewall de última generación |
| Herramienta de optimización de uso de reglas | Permita que los administradores vean cuántas veces se produjo una coincidencia de cada regla dentro de un período determinado |
| Herramienta de búsqueda de reglas | Herramienta integrada para buscar reglas en las políticas |
| Nombres de reglas | Capacidad de crear nombres de reglas que estén visibles en registros, estadísticas e informes |
| Cargas de políticas a prueba de errores | El sistema restaura automáticamente la versión anterior de la política si la nueva versión falla |

| CONFIGURACIÓN | |
|---|---|
| Enrutamiento | Configuración de enrutamiento de arrastrar y soltar para los firewalls y widgets específicos a fin de agregar rutas y rutas predeterminadas |
| Enrutamiento dinámico | Configuración avanzada de BGP y OSPF a través de una interfaz de usuario gráfica intuitiva |
| Antispoofing automática | La configuración antispoofing se crea automáticamente según el enrutamiento |
| VPN de sitio a sitio | <ul style="list-style-type: none"> → VPN IPsec basada en políticas → Túneles (GRE) y VPN IPsec basados en rutas |
| VPN de acceso remoto | <ul style="list-style-type: none"> → Cliente de VPN IPsec (iOS y Windows) → Cliente de VPN SSL (Android, Mac y Windows) → Portal de VPN SSL sin clientes |
| Administración de agente de contexto de dispositivo final | Amplíe la visibilidad y el control de acceso a las aplicaciones que se ejecutan en los dispositivos finales |
| Asistente de creación de elementos de firewall | Cree cientos de elementos de firewall a través de un asistente de creación de firewall |
| Autenticación de usuarios basada en navegadores | Configure y personalice un servicio de autenticación basado en navegadores para los usuarios |
| ESTADO, ESTADÍSTICAS E INFORMES | |
| Monitor de estado del sistema | Información de estado en tiempo real sobre dispositivos de red y sus conexiones |
| Monitor de estado de los dispositivos | Vista gráfica del estado del hardware de los dispositivos |
| Diagramas de redes | Visualice configuraciones, topologías y estado de conectividad |
| Monitoreo de la sesión | Vistas dedicadas para monitorear conexiones, asociaciones de seguridad (SA) de VPN, usuarios autenticados, alertas activas y rutas dinámicas y estáticas |
| Descripciones generales | Personalice paneles de estadísticas de redes y usuarios para un monitoreo en tiempo real |
| Geolocalizaciones | Muestre la información del país de todas las direcciones IP con la ayuda de banderas de países y estadísticas de geolocalización. Muestra de dónde vienen los ataques a la red |
| Generación de informes | Personalice y programe informes que brinden información detallada sobre las estadísticas de la red |
| Portal web | Acceso de solo lectura para ver políticas y registros y programar informes |

| ADMINISTRACIÓN DE TERCEROS | |
|--|---|
| Monitoreo de dispositivos | Permita que el administrador monitoree y vea los cambios de estado en la disponibilidad de dispositivos de terceros |
| Inserción de registros de los dispositivos | Análisis y recepción de registros en formato syslog de dispositivos de terceros y soporte listo para implementar para los formatos CEF, LEEF, CLF y WELF |
| Recepción de NetFlow/IPFIX | Capacidad de recibir, enviar y consolidar datos en formatos NetFlow v9 e IPFIX |
| Estadísticas de los dispositivos | Estadísticas e informes gráficos basados en datos de registro de terceros y contadores de protocolo simple de administración de redes (SNMP) |
| Cantidad de dispositivos admitidos | 200 por servidor de registro |
| Licencias | Cada dispositivo de terceros consume 0.2 del conteo de dispositivos con licencia del servidor de administración |
| REGISTROS | |
| Navegador | Vista granular para diferentes tipos de registros además de navegación de registros común para ver todos los datos de registro |
| Filtrado de arrastrar y soltar | Filtrado de registros interactivo: arrastre y suelte cualquier celda de datos de registro en el Panel de consultas |
| Estadísticas | Cree contadores basados en registros incorporados y estadísticas a pedido para generar informes, monitorear y alertar |
| Visualizaciones | Encuentre las anomalías en el tráfico registrado en visualizaciones de registro que pueden filtrarse |
| Analizador de registros | Combine libremente en la amplia cantidad de datos de registro filtrados por cualquiera de las columnas |
| Archivado | Duplique o archive los registros en directorios por tipo de datos de registro, hora o filtros |
| Respaldos | Programador de copias de respaldo integrado para datos de registro y configuración del servidor de registro |
| Exportaciones | Exportaciones de registros, CSV, XML y LEEF; los registros también pueden ser informes instantáneos |
| Envío | Redireccionamiento en tiempo real de registros en syslog; formatos CEF, LEEF, XML, CSV, IPFIX, NetFlow y McAfee Enterprise Security Manager; configuración para filtrado, tipo de datos, y selección de campos de registro disponible |
| Contextos de datos | Accesos directos para navegar por distintos tipos de registros con conjuntos de columnas contextuales que son personalizables |
| Alta disponibilidad | Soporte para la asignación de servidores de registro primario y de respaldo para cada fuente de registro |

Administración centralizada de entornos múltiples del cliente

Los proveedores de servicios administrados de seguridad (MSSP) necesitan reducir los altos costos administrativos asociados con la administración de servidores múltiples en dominios múltiples. La Forcepoint Administrative Domain License permite administrar múltiples entornos del cliente mediante un solo servidor de administración. Las configuraciones pueden volver a utilizarse y compartirse con distintos dominios para una distribución de cambios rápida y eficiente. La arquitectura

única de la solución Forcepoint Administrative Domain License simplifica los entornos empresariales y de MSSP, haciendo que sea más fácil mantenerlos. El control de acceso basado en el rol (RBAC) garantiza la definición precisa de las responsabilidades del administrador y las limitaciones del acceso a dominios.

Los clientes basados en dominios pueden acceder fácilmente a informes, configuraciones de políticas y registros a través de un portal web ligero y seguro.

Especificaciones de Forcepoint Administrative Domain License

| DOMINIOS | |
|--|---|
| Cantidad máxima | 1000 |
| Cantidad de administradores | Ilimitada |
| Cantidad de dispositivos administrados | 6000 |
| Cantidad de elementos | Ilimitada |
| CARACTERÍSTICAS | |
| Separación de configuraciones | Aísle los entornos administrados en distintos dominios administrativos, y asegúrese de que nunca se mezclen los elementos de red de los clientes |
| Intercambio de configuraciones | Comparta elementos como plantillas de políticas con todos los dominios |
| Control de acceso | Otorgue o limite los derechos de acceso de los administradores a la configuración y visibilidad para separar los dominios administrativos |
| Monitoreo | Monitoree el estado de todos los dominios otorgados con la ayuda de la descripción general de dominios |
| Marcado | Marque los informes en PDF con plantillas de estilos personalizados |
| Herramientas de migración | Traslade elementos entre dominios con la herramienta integrada de "mover a" |
| Importación/Exportación | Importe y exporte elementos entre distintos dominios e instalaciones de SMC |
| Motor NGFW virtual | Comparta el mismo contexto maestro entre distintos dominios de hasta 250 contextos virtuales, cada uno de los cuales puede tener sus propias políticas y tablas de enrutamiento |

Forcepoint Web Portal Server

Forcepoint Web Portal Server brinda a los clientes, administradores y gerencia de MSSP una UI web ligera para visualizar registros, informes programados, políticas actuales e historial de cambios de políticas. Los administradores de MSSP pueden configurar la cantidad de información que se muestra en el portal según las necesidades del cliente o para reducir las solicitudes de soporte.

Forcepoint Web Portal Server admite inglés, español y francés de forma nativa, con la capacidad de agregar otros idiomas.

Beneficios clave

- Acceso sin clientes, de solo lectura a registros, informes, políticas e historial de cambios de políticas
- Estado de la red en tiempo real disponible para usuarios definidos
- Soporte para dispositivos móviles

Especificaciones de Forcepoint Web Portal Server

| ESPECIFICACIONES | |
|---|--|
| Cantidad máxima de usuarios simultáneos | 250 por servidor del portal web |
| Cantidad de administradores | Ilimitada |
| Cantidad de usuarios de portal web | Ilimitada |
| Autenticación de usuarios | Base de datos del servidor de administración, RADIUS, TACACS+ |
| Conexiones de dispositivos | Cifrado TLS |
| CARACTERÍSTICAS | |
| Políticas de seguridad | Vea las más recientes configuraciones de los firewalls de última generación en formato HTML |
| Informes | Vea informes programados para publicarse en el portal web en formato HTML |
| Navegación de registros | Navegue y filtre los registros en formato HTML |
| Detalles de registros | Monitoree el estado de todos los dominios otorgados con la ayuda de la descripción general de dominios |
| Exportación a PDF | La exportación a PDF permite descargar informes en formato PDF |
| Anuncios | Los administradores pueden especificar anuncios para mostrar en el portal web |
| Comparación de políticas | Compare las diferentes versiones de configuración de los firewall de última generación para comprobar si la solicitud de cambio fue implementada |
| Localización | El portal web admite inglés, español y francés, y puede traducirse fácilmente para admitir otros idiomas |
| Personalización | Personalice la apariencia de los portales web |

Forcepoint SMC Appliance

Forcepoint Security Management Center (SMC) Appliance es un dispositivo todo en uno dedicado para configurar, administrar y monitorear los Forcepoint NGFW, ya sean físicos, virtuales o en la nube. El centro de gestión de seguridad Forcepoint SMC brinda facilidad de despliegue para que pueda estar en funcionamiento rápidamente, combinando el servidor de registro y el servidor de administración de Forcepoint NGFW en un único paquete plug-and-play que se ejecuta en hardware 1U optimizado.

Opciones de despliegue de Forcepoint NGFW SMC

Existen tres maneras de desplegar Forcepoint SMC: en sus sistemas, en su hipervisor o hardware, o como un dispositivo todo en uno¹.

¹ Se debe adquirir una licencia de software de SMC por separado para las tres opciones de despliegue. Un dispositivo por sí solo no incluye una licencia.

| OPCIONES DE DESPLIEGUE DE FORCEPOINT NGFW SMC | | | |
|---|------------------------------|------------------------------|-------------|
| COMPONENTES | SOFTWARE | IMAGEN ISO | DISPOSITIVO |
| Software de SMC | ● | ● | ● |
| Sistema operativo | Proporcionado por el cliente | ● | ● |
| Hardware/Plataforma | Proporcionado por el cliente | Proporcionado por el cliente | ● |

Especificaciones de Forcepoint SMC Appliance

| RENDIMIENTO | |
|---------------------------------|---------------|
| Firewalls administrados | 2000 |
| Cantidad máxima de dominios | 200 |
| Registros indexados por seg. | 80 000 |
| Eventos por día | 6 912 000 000 |
| Tamaño de registro por día (GB) | 690 |

Especificaciones de Forcepoint SMC Appliance

| FÍSICO | |
|---------------------------|--|
| Factor de forma | 1U |
| Procesador | 2 x Intel Xeon |
| Memoria | 32 GB |
| Almacenamiento (HDD) | Capacidad de 900 GB (4 X 300 GB, RAID-5), intercambiables en caliente |
| Fuente de alimentación | 2 x 550 W (100 V~240 V), intercambiable en caliente |
| Dimensiones | 23,9" de profundidad x 17,09" de ancho x 1,68" de alto (60,7 cm de profundidad x 43,42 cm de ancho x 4,28 cm de alto) |
| Peso | 28,26 libras (12,82 kg) |
| Normativas y cumplimiento | FCC / ICES / EN55022 / VCCI/BSMI / C-Tick / SABS / CCC / MIC Clase A y UL60950-1 / Verificado para cumplir con la Directiva RoHS |

Pedidos de Forcepoint SMC

| PEDIDOS | N.º DE PARTE |
|--|--------------|
| Forcepoint NGFW Security Management Center (software) | SMCX |
| Forcepoint NGFW Security Management Center 1000 Appliance | SMCAP |
| Forcepoint NGFW Security Management Center High Availability (solo disponible para despliegues de software e imágenes ISO) | SMCHAX |
| Forcepoint SMC Additional Log Server | ALSX |
| Forcepoint SMC Domains (hasta 200 dominios) | ODFSMCX |
| Forcepoint SMC Web Portal | OWPSX |