Forcepoint

Decritivo

NGFW Security Management Center

Administração em painel único para visibilidade máxima na rede

Principais benefícios

- Administração centralizada em painel único de até 6.000 NGFWs físicos ou virtuais da Forcepoint em ambientes distribuídos
- Flexibilidade e escalabilidade para implementação em grandes redes corporativas
- Opção de alta disponibilidade para requisitos de tempo de funcionamento rigorosos
- Políticas Inteligentes e automação eficiente do fluxo de trabalho para implementação e manutenção rápidas e precisas do Forcepoint NGFW
- Contexto, conscientização e visibilidade de usuários e endpoints em toda a rede, desde o data center e a borda, até as filiais e a nuvem
- Escolha entre opções de implementação de software ou appliance

O Forcepoint NGFW Security Management Center (SMC) fornece administração unificada e centralizada de todos os modelos de Forcepoint Next Generation Firewalls—físicos, virtuais ou de nuvem—em ambientes corporativos grandes e geograficamente distribuídos.

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 disponibilidade

As empresas atuais têm tolerância zero para disrupção, e precisam de acesso 24h aos recursos críticos. Com a opção de alta disponibilidade do Forcepoint SMC, as organizações mantêm acesso contínuo aos recursos de registro para resiliência em análise e resposta de incidentes.

Cliente de administração de segurança

Não importa qual seja a localização geográfica, os administradores podem acessar o Forcepoint SMC com segurança usando o Management Client. Esse cliente fornece uma interface gráfica de usuário potente para configuração, monitoramento, registros, alertas, relatórios, atualizações e upgrades para Forcepoint Next Generation Firewalls. O cliente Forcepoint SMC fornece aos administradores uma visão holística da rede e ações aprofundadas e contextuais para administração rápida e eficaz de todo o seu ambiente de segurança.

Especificações do SMC para NGFWs da Forcepoint

SERVIDOR DE ADMINISTRAÇÃO	
Número de dispositivos administrados	Licenciados: 1 a 6.000 nós com um servidor de administração
Número de administradores	Ilimitado
Número de elementos	Ilimitado
Número de políticas	Ilimitado
Número de servidores de registro	Ilimitado
Número de servidores do portal web	Ilimitado
Autenticação de administrador	Banco de dados local, RADIUS. TACACS+, Client Certificate e Microsoft Active Directory (LDAP)
Conexões de dispositivo	Criptografia TLS
SERVIDOR DE REGISTRO	
Número de dispositivos suportados	Ilimitado
Registros em log por segundo	O sistema de registros de alto desempenho pode receber até 500.000 registros por segundo
Conexões de dispositivo	Criptografia TLS 1.2 e autenticação usando chaves e certificados X.509v3
Tamanho de armazenamento de registros	Ilimitado
Número de encaminhamento de registros por servidor de registro	Ilimitado
GERAL	
Cliente de Administração	Interface de usuário HTML5
SMC Application Programming Interface (SMC API)	API documentada que habilita integração fácil com produtos e serviços de terceiros Usa arquitetura REST em que os dados podem ser codificados em XML ou JSON
Administradores simultâneos	Vários administradores podem fazer alterações ao mesmo tempo e elementos críticos, como políticas, ficam bloqueados para edição
Painéis de controle na tela inicial	Painéis de controle personalizáveis na tela inicial para NGFWs, VPNs, usuários e outros elementos
Monitoramento de usuários	Além das correlações e verificações relacionadas ao comportamento de usuários, fornece informações de status de segurança de endpoints e estatísticas de aplicativos de endpoints

Alta disponibilidade	Até quatro servidores de administração em standby
Upgrades	Upgrades e pacotes de atualizações dinâmicas podem ser baixados automaticamente
Backups	Ferramenta integrada de backup para fazer backups de todo o sistema, incluindo todas as configurações de firewalls da próxima geração
Navegação	Navegação intuitiva semelhante a navegador, com histórico de navegação, guias e marcadores
Ferramentas de pesquisa do Spotlight	Ferramentas de pesquisa de elementos e referências eficientes, com ações rápidas sensíveis ao contexto
Filtragem rápida	Filtragem de digitação antecipada conveniente em listas de elementos, tabelas e células de política
Suporte para várias seleções	Execute ações e confirme alterações em centenas de elementos simultaneamente
Ferramentas de limpeza do sistema	Permitem que o administrador encontre facilmente quais elementos e regras não são usados
ADMINISTRAÇÃO	
Encaminhamentos de alertas	Permite que o administrador encaminhe alertas do sistema usando e-mail, SMS, trap SNMP e scripts personalizados
Limiares de alertas	Limiares de alertas fáceis para estatísticas de visão geral
Registros de auditoria	Todas as mudanças no sistema são registradas em registros de auditoria
Relatórios do sistema	Relatórios de auditoria de inventário e conformidade sobre contas e atividades dos administradores
Provisionamento com toque zero	Instalação com base na nuvem (ou pen drive) com envio de política inicial por psuh
Tarefas automáticas	Administração automatizada de dados de registro, arquivamento e retenção, backups, atualizações e tarefas de atualização de políticas
Domínios administrativos	Permite a divisão do ambiente em domínios de configuração isolados
Importação/exportação	Exportação e importação de XML e CSV sempre, em vez de apenas entre instalações
Upgrades remotos	Upgrade remoto à prova de falhas com um clique para os NGFWs administrados
Controle de acesso do administrador com base em função	Funções personalizadas podem ser definidas e combinadas, além de funções predefinidas (por exemplo, Proprietário, Visualizador, Operador, Editor, Superusuário) para controlar as permissões de forma flexível e precisa
Administração de licenças	Atualizações automáticas de licenças online e relatórios de status do contrato de manutenção
Administração de certificados	Visão consolidada de todos os certificados e credenciais
Ferramentas de solução de problemas	Recursos abrangentes de diagnóstico remoto: ferramenta de captura de tráfego integrada, download de instantâneo de configuração do firewall de próxima geração e visualizações de monitoramento de sessão
Administração de casos de incidentes	Ferramentas integradas para administração colaborativa de incidentes de rede

ADMINISTRAÇÃO DE POLÍTICAS	
Mecanismo de NGFW virtual	Compartilhe o mesmo contexto mestre em vários domínios administrativos do SMC; até 250 contextos virtuais, cada um com suas próprias políticas e tabelas de roteamento
Administração de políticas hierárquicas	Modelos de políticas, subpolíticas, aliases e seções de comentários de regras mantêm a política organizada e compreensível
Identificação de aplicativos	→ Restringir o acesso com base em aplicativos de rede e/ou endpoint → Restringir o acesso de/para aplicativos por payload → Listas de permissões/bloqueios por nome do aplicativo e versão do Forcepoint Endpoint Context Agent
Administração de mudanças	Exigir revisão e aprovação por um segundo administrador antes que as alterações sejam implementadas
Filtragem de URLs	Restringir o acesso por categorias de URLs
Nomes de domínio	Restringir o acesso dinamicamente usando nomes de domínio que podem ser convertidos em endereços IP
Identificação de usuários	Corresponder a regras baseadas no usuário por meio de identificação transparente de usuários ou aplicação de métodos de autenticação fortes
Zonas	As interfaces físicas podem ser marcadas com zonas e referidas nas políticas
Geoproteção	Restringir o acesso por países ou regiões geográficas
Políticas de inspeção	Controle granular para inspeção profunda de pacotes e maneiras fáceis de desativar falsos positivos
Políticas de Qualidade do Serviço (QoS)	Configuração de política de QoS baseada em classe
Filtragem de arquivos com base em políticas	Definir como os arquivos são inspecionados usando reputação de arquivos Global Threat Intelligence, Anti-Malware Scan e McAfee Advanced Threat Defense da McAfee
Tradução de Endereço de Rede (NAT)	→ NAT padrão → NAT com base em elementos → Políticas NAT
Ferramenta de validação de políticas	Ajuda o administrador a encontrar erros de configuração antes da ativação da política
Instantâneos da política	Permite exploração e comparação do histórico de configuração do Forcepoint Next Generation Firewall
Restauração de políticas	Uma versão anterior da política pode ser recuperada e carregada no firewall de próxima geração
Ferramenta de otimização do uso de regras	Permite que os administradores vejam quantas vezes cada regra foi correspondida em um período de tempo especificado
Ferramenta de pesquisa de regras	Ferramenta integrada para pesquisar regras em políticas
Nomes de regras	Capacidade para criar nomes de regras que são visíveis em registros, estatísticas e relatórios
Carregamentos de políticas à prova de falhas	O sistema restaura automaticamente a versão anterior da política se a nova versão falhar

CONFIGURAÇÃO	
Roteamento	Configuração de roteamento com arrastar e soltar para firewalls e widgets específicos para adicionar rotas e rotas padrão
Roteamento dinâmico	Configuração avançada de OSPF e BGP por meio de interface gráfica de usuário intuitiva
Antispoofing automático	A configuração antispoofing é criada automaticamente com base no roteamento
VPNs site a site	→ VPN IPsec baseada em políticas → VPN IPsec baseada em rotas e tunelamento (GRE)
VPNs de acesso remoto	→ Cliente de VPN IPsec (iOS e Windows) → Cliente de VPN SSL (Android, Mac e Windows) → Portal de VPN SSL sem cliente
Gerenciamento do agente de contexto de endpoint	Estenda o controle de acesso e a visibilidade para os aplicativos executados nos endpoints
Assistente de criação de elemento de firewall	Crie centenas de elementos de firewall com um assistente de criação de firewalls
Autenticação de usuário baseada em navegador	Configure e personalize um serviço de autenticação fácil baseado em navegador para usuários
STATUS, ESTATÍSTICAS E RELATÓRIOS	
Monitoramento de status do sistema	Informações de status em tempo real sobre dispositivos de rede e suas conexões
Monitoramento de status de appliances	Exibição gráfica do status de hardware dos appliances
Diagramas de rede	Visualize configurações, topologias e conectividade de status
Monitoramento de sessão	Exibições dedicadas para monitorar conexões, associações de segurança VPN (SAs), usuários autenticados, alertas ativos e rotas dinâmicas e estáticas
Visões gerais	Personalize painéis de estatísticas de usuários e redes para monitoramento em tempo real
Geolocalizações	Mostre as informações do país para todos os endereços IP com a ajuda de bandeiras de países e estatísticas de geolocalização. Mostre a origem dos ataques de rede
Relatórios	Personalize relatórios de agendamento eletrônico que fornecem informações detalhadas sobre estatísticas de rede
Portal web	Acesso somente leitura para ver políticas, registros e relatórios programados

ADMINISTRAÇÃO DE TERCEIROS	
Monitoramento de dispositivos	Permite que o administrador monitore e exiba as alterações de status na disponibilidade de dispositivos de terceiros
Injeção de registros de dispositivo	Análise de registro e recebimento em formato syslog para dispositivos de terceiros e suporte direto da caixa para os formatos CEF, LEEF, CLF e WELF
Recebimento NetFlow/IPFIX	Capacidade para receber, encaminhar e consolidar dados nos formatos NetFlow v9 e IPFIX
Estatísticas de dispositivos	Estatísticas gráficas e relatórios baseados em dados de registros de terceiros e contadores de protocolo de gerenciamento de rede simples (SNMP)
Número de dispositivos suportados	200 por servidor de registro
Licenciamento	Cada dispositivo de terceiros consome 0,2 da contagem de dispositivos de licença do Management Server
REGISTROS	
Navegador	Exibição granular para tipos de registro separados, além da exibição de navegação de registro comum para todos os dados de registro
Filtragem com arrastar e soltar	Filtragem de registros interativa—arraste e solte qualquer célula de dados de registro no Painel de Consulta
Estatísticas	Crie contadores integrados com base em registros e estatísticas sob demanda para relatórios, monitoramento e alertas
Visualizações	Encontre as anomalias no tráfego registrado em visualizações de registros filtráveis
Analisador de registros	Agregue livremente a grande quantidade de dados de registro filtrados por qualquer coluna
Arquivamento	Duplique ou arquive registros em diretórios por tipo de dados de registro, hora ou filtros
Backups	Agendador de backup integrado para configuração do servidor de registro e dados de registro
Exportações	CSV, XML, LEEF e exportação de registros; os registros também podem ser relatórios instantâneos
Encaminhamento	Redirecionamento de registros em tempo real no syslog; formatos CEF, LEEF, XML, CSV, IPFIX, NetFlow e McAfee Enterprise Security Manager; configuração para filtragem, tipo de dados; e seleção de campo de registro disponível
Contextos de dados	Atalhos para navegar em diferentes tipos de registros com conjuntos de colunas contextuais que são personalizáveis
Alta disponibilidade	Suporte para atribuição de servidores de registros primários e de backup para cada origem de registros

Administração centralizada de vários ambientes de cliente

Os Provedores de Serviços de Segurança Gerenciados (MSSPs) precisam reduzir os altos custos administrativos associados à administração de vários servidores em vários domínios. A Forcepoint Administrative Domain License permite que vários ambientes de clientes sejam administrados com único servidor de administração. As configurações podem ser reutilizadas e compartilhadas entre domínios para uma distribuição rápida e eficiente das mudanças. A arquitetura exclusiva da solução Forcepoint Administrative Domain License simplifica os ambientes corporativos e MSSP, tornando-os mais fáceis de manter. O controle de acesso baseado em função (RBAC) garante a definição precisa das responsabilidades do administrador e limitações de acesso ao domínio. Clientes baseados em domínio podem acessar relatórios, configurações de políticas e registros facilmente através de um portal web seguro e leve.

Especificações da Forcepoint Administrative Domain License

DOMÍNIOS	
Número máximo	1.000
Número de administradores	Ilimitado
Número de dispositivos administrados	6.000
Número de elementos	Ilimitado
RECURSOS	
Separação de configuração	Isole ambientes gerenciados em diferentes domínios administrativos, e garanta que os elementos de rede dos clientes nunca se misturem
Compartilhamento de configuração	Compartilhe elementos como modelos de política para todos os domínios
Controle de acesso	Conceda ou limite os direitos de acesso dos administradores à configuração e visibilidade com a ajuda de domínios administrativos separados
Monitoramento	Monitore o status de todos os domínios concedidos com a ajuda da visão geral do domínio
Branding	Gere relatórios em PDF com a marca da empresa com modelos de estilos personalizados
Ferramentas de migração	Mova elementos entre domínios com a ferramenta integrada "mover para"
Importação/exportação	Importe e exporte elementos entre diferentes instalações e domínios de SMC
Mecanismo de NGFW virtual	Compartilhe o mesmo contexto mestre entre limites de domínio de até 250 contextos virtuais, cada um com suas próprias políticas e tabelas de roteamento

Forcepoint Web Portal Sunucusu

O Forcepoint Web Portal Server fornece aos clientes, administradores e gestores de MSSPs uma interface web leve para visualização de registros, relatórios programados, políticas atuais e histórico de alterações de políticas. Os administradores do MSSP podem configurar a quantidade de informações exibidas no portal com base nas necessidades do cliente ou para reduzir as solicitações de suporte.

O Forcepoint Web Portal Server oferece inglês, espanhol e francês nativamente, com capacidade para adicionar novos idiomas.

Principais benefícios

- → Acesso sem cliente somente leitura para registros, relatórios, políticas e histórico de alterações em políticas
- → Status da rede em tempo real disponível para usuários definidos
- → Suporte para dispositivos móveis

Especificações do Forcepoint Web Portal Server

ESPECIFICAÇÕES	
Número máximo de usuários simultâneos	250 por servidor de portal web
Número de administradores	Ilimitado
Número de usuários do portal web	Ilimitado
Autenticação de usuários	Banco de dados do Servidor de Administração, RADIUS, TACACS+
Conexões de dispositivo	Criptografia TLS
RECURSOS	
Políticas de segurança	Exiba as configurações mais recentes dos firewalls de próxima geração em formato HTML
Relatórios	Exiba relatórios que podem ser programados para publicação no portal web em formato HTML
Navegação em registros	Navegue e filtre os registros em formato HTML
Detalhes dos registros	Monitore o status de todos os domínios concedidos com a ajuda da visão geral do domínio
Exportação de PDFs	Uma exportação de PDF permite download do relatório em formato PDF
Anúncios	Os administradores podem especificar anúncios a serem exibidos no portal da web
Comparação de políticas	Compare as diferentes versões de configuração de firewall de próxima geração para ver se a solicitação de alteração foi implementada
Localização	O portal web disponibiliza inglês, espanhol e francês, e pode ser traduzido facilmente para suporte a outros idiomas
Personalização	Personalize a aparência e o funcionamento de portais web

Forcepoint SMC Aracı

O appliance Forcepoint Security Management Center (SMC) é um dispositivo "tudo em um" dedicado para configurar, gerenciar e monitorar o Forcepoint NGFW—físico, virtual e baseado na nuvem. O Forcepoint SMC oferece facilidade de implementação para colocar em funcionamento rapidamente, combinando o servidor de gerenciamento NGFW do Forcepoint e o servidor de registros em um único pacote plug and play executado em hardware 1U otimizado.

Opções de implementação do SMC para NGFW da Forcepoint

Existem três formas de implementar o Forcepoint SMC: em seus sistemas, em seu hardware ou hypervisor, ou como um dispositivo "tudo em um"[1].

1 Uma licença de software SMC precisa ser comprada separadamente para as 3 opções de implementação. Um appliance não inclui licenças.

	OPÇÕES DE IMPLEMENTAÇÃO DO SMC PARA NGFW DA FORCEPOINT		
COMPONENTES	**SOFTWARE**	**IMAGEM ISO**	**APPLIANCE**
Software SMC	●	●	●
Sistema Operacional	Fornecido pelo cliente	●	●
Hardware/plataforma	Fornecido pelo cliente	Fornecido pelo cliente	●

Especificações do Appliance SMC

DESEMPENHO	
Firewalls administrados	2.000
Máximo de domínios	200
Registros indexados por segundo	80.000
Eventos por dia	6.912.000.000
Tamanho do registro por dia (GB)	690

Especificações do Appliance SMC

FÍSICAS	
Fator de forma	1U
Processador	2 x Intel Xeon
Memória	32 GB
Armazenamento (HDD)	Capacidade 900 GB (4 X 300 GB, RAID-5), Hot Swappable
Fonte de alimentação	2 x 550W (100V~240V) Hot Swappable
Dimensões	60,7 cm P x 43,42 cm L x 4,28 cm A
Peso	12,82 kg (12.82 kg)
Regulamentações e conformidade	FCC / ICES / EN55022 / VCCIBSMI / C-Tick / SABS / CCC / MIC Classe A e UL60950-1 / Conformidade verificada com a Diretiva RoHS

Pedidos do Forcepoint SMC

PEDIDOS	Nº DE PEÇA
Forcepoint NGFW Security Management Center (software)	SMCX
Forcepoint NGFW Security Management Center 1000 Appliance	SMCAP
Forcepoint NGFW Security Management Center de alta disponibilidade (disponível apenas para implementações de software e imagem ISO)	SMCHAX
Servidor de registros adicional do Forcepoint SMC	ALSX
Domínios do Forcepoint SMC (até 200 domínios)	ODFSMCX
Portal web do Forcepoint SMC	OWPSX