Forcepoint

Datasheet

Next Generation Firewall

Segurança de Rede corporativa com recursos nativos de SD-WAN

Principais benefícios

Conectividade SD-WAN sempre ativa para empresas

As empresas atuais exigem soluções de segurança de rede totalmente resilientes.O Forcepoint Next-Gen Firewall (NGFW) incorpora alta escalabilidade e disponibilidade em todos os níveis.

- **Clustering ativo-ativo e misto.** Até 16 nós de diferentes modelos com versões diferentes podem ser agrupados. Isso fornece desempenho e resiliência de rede superiores e habilita recursos de segurança, como inspeção profunda de pacotes e VPNs.
- **Atualizações contínuas de políticas e software.** A disponibilidade líder de mercado da Forcepoint permite que as atualizações de políticas (e até mesmo atualizações de software) sejam enviadas perfeitamente para um cluster sem interromper o serviço.
- **Cluster de rede SD-WAN.** Estende a cobertura de alta disponibilidade para conexões de rede e VPN. Combina segurança ininterrupta com a capacidade de aproveitar as conexões de banda larga locais para complementar ou substituir linhas alugadas caras, como MPLS.

O Forcepoint Next-Gen Firewall fornece segurança de rede líder do setor com conectividade SD-WAN rápida e flexível para conectar e proteger as pessoas e os dados que usam em redes corporativas diversas e em evolução. O Forcepoint NGFW oferece segurança, desempenho e operações consistentes em sistemas físicos, virtuais e de nuvem. Foi projetado desde o zero para alta disponibilidade e escalabilidade, juntamente com administração centralizada e visibilidade total em 360°.

Clientes que mudam para o Forcepoint NGFW Clientes que mudam para o Forcepoint NFGW relatam uma queda de 86% nos ataques cibernéticos, 53% menos carga de TI e 70% menos tempo de manutenção.*

Acompanhe as mudanças nas necessidades de segurança

Um núcleo de software unificado permite que a Forcepoint lide com várias funções de segurança, desde firewall/VPN e conector de aplicativos ZTNA até sistema de prevenção de invasões (IPS) e firewall de camada 2, em ambientes dinâmicos de negócios. A Forcepoint pode ser implementada de várias maneiras (por exemplo, dispositivos físicos, virtuais e de nuvem), todas gerenciadas a partir de um único console.

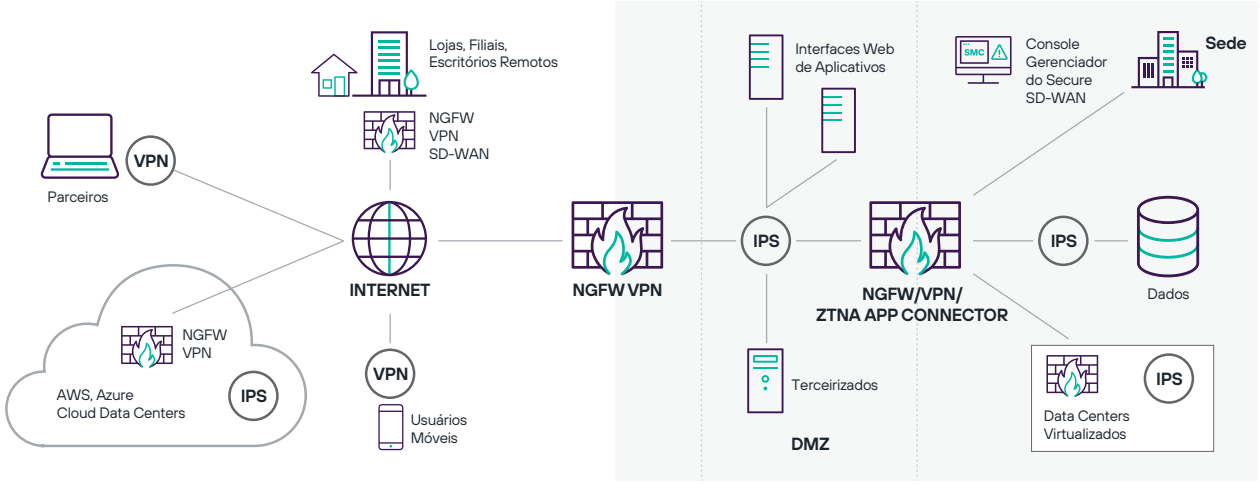
A Forcepoint adapta de forma exclusiva o controle de acesso e a inspeção profunda para cada conexão para fornecer alto desempenho e segurança. Ela combina controle granular de aplicativos, defesas IPS, controle de rede virtual privada (VPN) integrada e proxies de aplicativos de missão crítica em um design eficiente, extensível e altamente escalável. Nossas poderosas tecnologias anti-evasão decodificam e normalizam o tráfego de rede antes da inspeção e em todas as camadas de protocolo para expor e bloquear os métodos de ataque mais avançados.

Bloqueie ataques sofisticados de violação de dados

As grandes violações de dados continuam a atormentar empresas e organizações em todos os setores. Combata essa ameaça com proteção de exfiltração de camada de aplicação. A Forcepoint automaticamente permite ou bloqueia o tráfego de rede proveniente de aplicativos específicos em PCs, laptops, servidores, compartilhamentos de arquivos e outros dispositivos de endpoint com base em dados contextuais de endpoint altamente granulares Vai além de firewalls típicos para evitar tentativas de exfiltração de dados confidenciais de endpoints por meio de programas, aplicativos web, usuários e canais de comunicação não autorizados.

* "Quantificação dos resultados operacionais e de segurança da mudança para o Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, maio de 2017.

Plataforma única com muitas opções de implementação – tudo administrado a partir de um console centralizado



Proteção incomparável

Os invasores se tornaram especialistas em penetrar em redes, aplicativos, data centers e endpoints corporativos. Uma vez lá dentro, roubam propriedade intelectual, informações de clientes e outros dados confidenciais, causando danos irreparáveis às empresas e suas respectivas reputações.

As novas técnicas de ataque podem evitar a detecção por dispositivos de rede de segurança tradicionais, incluindo muitos firewalls de marca própria, indo além da simples transmissão de exploits de vulnerabilidade.

As evasões funcionam em vários níveis para camuflar exploits e malware, tornando-os invisíveis para a inspeção tradicional de pacotes baseada em assinatura. Mesmo os ataques que foram bloqueados há anos podem ser reembalados com evasões para comprometer os sistemas internos.

A Forcepoint adota uma abordagem diferente. Nosso mecanismo de segurança líder na indústria foi projetado para todos os três estágios da defesa de rede: derrotar evasões, detectar exploits de vulnerabilidades e impedir malware. Pode ser implementado de forma transparente atrás de firewalls existentes para adicionar proteção sem interrupções ou como um Firewall Empresarial completo para segurança tudo-em-um.

Além disso, a Forcepoint fornece descriptografia rápida de tráfego criptografado, incluindo conexões web HTTPS, combinadas com controles de privacidade granulares que mantêm sua empresa e usuários seguros em um mundo em rápida mudança. Pode até limitar o acesso de aplicativos de endpoint específicos para bloquear dispositivos ou evitar o uso de software vulnerável.

Resultados para o negócio

- → Implementação mais rápida de filiais, nuvens ou data centers
- → Menos tempo de parada
- → Mais segurança sem disrupção
- → Menos invasões
- → Menos exposição a novas vulnerabilidades enquanto as equipes de TI se preparam para implantar novos patches
- → TCO mais baixo para infraestrutura de rede e segurança

Principais funcionalidades

- → Conectividade SD-WAN em escala corporativa
- → Integração SASE/SSE para segurança de aplicativos privados na web, na nuvem e em aplicativos privados
- → IPS integrado com defesas antievasão
- → Clustering de alta disponibilidade para dispositivos e redes
- → Atualizações automáticas sem downtime
- → Administração centralizada orientada por políticas
- → Visibilidade programável e interativa em 360°
- → Proxies de segurança Sidewinder para aplicativos de missão crítica
- → Contexto de usuário e endpoint
- → Descriptografia de alto desempenho com controles de privacidade granulares
- → Permitir/bloquear por aplicativo e versão do cliente
- → Monitoramento da saúde de aplicativos
- → Integração de CASB e Web Security
- → Sandboxing antimalware
- → Software unificado para implementações físicas, AWS, Azure, e VMware
- → Menos exposição a novas vulnerabilidades enquanto as equipes de TI se preparam para implantar novos patches
- → TCO mais baixo para infraestrutura de rede e segurança

Especificações do Forcepoint NGFW

PLATAFORMAS	
Appliance físico	Várias opções de appliances de hardware, incluindo desde filiais até data centers
Infraestrutura de nuvem	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Appliance virtual	Sistemas x86 de 64 bits; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM e Nutanix AHV
Endpoint	Endpoint Context Agent (ECA), cliente VPN
Contextos virtuais	Até 250
Administração centralizada	Sistema de administração centralizada de nível empresarial com análise de logs, monitoramento e geração de relatórios. Consulte o descritivo do Forcepoint Security Management Center para obter detalhes.

RECURSOS DO FIREWALL	
Inspeção profunda de pacotes	Normalização de tráfego em várias camadas/inspeção profunda de fluxo completo, defesa anti-evasão, detecção dinâmica de contexto, manuseio/inspeção de tráfego específico de protocolo, descriptografia granular do tráfego SSL/TLS (ambos TLS 1.2 e 1.3), detecção de exploits de vulnerabilidades, impressão digital personalizada, reconhecimento, anti-botnet, correlação, gravação de tráfego, proteção DoS/DDoS, métodos de bloqueio, atualizações automáticas
Identificação de usuários	Banco de dados interno de usuários, LDAP nativo, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, certificados de cliente
Alta disponibilidade	› Clustering de firewall ativo-ativo/ativo-standby até 16 nós › SD-WAN › Failover stateful (incluindo conexões de VPN) › Equilíbrio de carga de servidor › Agregação de links (802.3ad) › Detecção de falha de link
Atribuição de endereço IP	› IPv4 estático, DHCP, PPPoA, PPPoE, IPv6 estático, SLAAC, DHCPv6 › Serviços: Servidor DHCP para IPv4 e retransmissão de DHCP para IPv4 e IPv6
Roteamento	› Rotas IPv4 e IPv6 estáticas, roteamento baseado em políticas, roteamento multicast estático › Roteamento dinâmico: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy › Roteamento com reconhecimento de aplicativo
IPv6	Pilha dupla IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, recursos completos de NGFW
Redirecionamento de proxy	Protocolos HTTP, HTTPS, FTP, SMTP são redirecionados para a Forcepoint ou para o Content Inspection Service (CIS) on-premise e na nuvem de terceiros
Geoproteção	País ou continente de origem/destino atualizado dinamicamente
Lista de endereços IP	Categorias de IP predefinidas ou usando listas de endereços IP personalizadas ou importadas
Filtragem de URL (assinatura separada)	Listas de URL personalizadas ou importadas; suporta QUIC e HTTP/3
Aplicativos de Endpoint	Nome e versão do aplicativo
Aplicativos de rede	Mais de 7.400 aplicativos de rede e nuvem
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

INTEGRAÇÃO SASE	
Redirecionamento de tráfego da web	Túnel GRE e IPsec para plataformas de Security Service Edge (SSE), como o Forcepoint ONE
Conector de aplicativos ZTNA	Permite que aplicativos privados em datacenters internos se conectem ao Zero Trust do Forcepoint ONE

SD-WAN	
Protocolos	IPsec e TLS
VPN site a site	› VPN com base em políticas e rotas › Hub e spoke, malha completa, malha parcial, topologias híbridas › Seleção dinâmica de vários links de ISP › Compartilhamento de carga, ativo/standby, agregação de links › Monitoramento ao vivo e relatórios sobre a qualidade do link dos ISPs (atraso, jitter, perda de pacotes)
Acesso remoto	› Cliente VPN Forcepoint para Microsoft Windows, Android e Mac OS › Qualquer cliente IPsec padrão › Alta disponibilidade com failover automático › Verificações de segurança do cliente › Acesso ao portal VPN TLS

DETECÇÃO AVANÇADA DE MALWARE E CONTROLE DE ARQUIVOS	
Protocolos	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtragem de arquivos	Filtragem de arquivos baseada em políticas com processo de seleção eficiente. Mais de 200 tipos de arquivos compatíveis em 19 categorias de arquivos
Reputação de arquivos	Verificação e bloqueio de reputação de malware de alta velocidade baseado na nuvem
Anti-Virus	Mecanismo de verificação antivírus local*
Sandboxing Zero-Day	Forcepoint Advanced Malware Detection and Protection disponível como serviço na nuvem e on-premises

* A verificação anti-malware local não está disponível com os dispositivos 110/115.