Forcepoint Next Generation Firewall (NGFW)

SD-WAN corporativa com o nº 1 em segurança de redes

O Forcepoint NGFW reúne conexão de rede rápida e flexível (SD-WAN e LAN) com segurança líder do setor para conectar e proteger pessoas e dados em redes corporativas diversas e em evolução. O Forcepoint NGFW oferece segurança, desempenho e operações consistentes em sistemas físicos, virtuais e em nuvem. Foi projetado do zero para alta disponibilidade e escalabilidade, e administração centralizada com visibilidade total de 360°.

Conectividade SD-WAN sempre ativa para empresas

As empresas atuais exigem soluções de segurança de rede totalmente resilientes. O Forcepoint NGFW integra alta escalabilidade e disponibilidade em todos os níveis:

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

Os clientes que migram para o Forcepoint NGFW relatam redução 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 o Forcepoint NGFW administre várias funções de segurança, incluindo firewall/VPN, IPS e firewall de camada 2, em ambientes de negócios dinâmicos. Os Forcepoint NGFWs podem ser implementados de várias formas (por exemplo, dispositivos físicos, virtuais, em nuvem), todos administrados a partir de um única console.

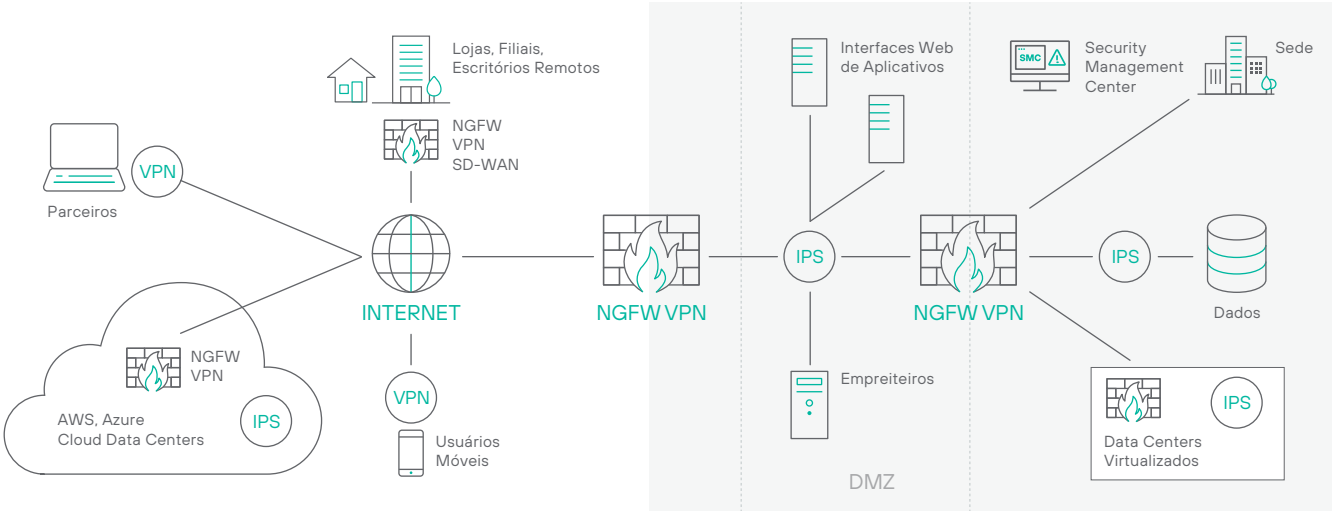
A Forcepoint adapta de forma exclusiva o controle de acesso e a inspeção profunda a cada conexão para fornecer alto desempenho e segurança. Associa controle granular de aplicativos, defesas de sistema de prevenção de intrusões (IPS), controle de rede privada virtual (VPN) integrado e proxies de aplicativos de missão crítica em um design eficiente, extensível e altamente escalável. Nossas potentes tecnologias antievasão 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

Grandes violações de dados continuam a atormentar empresas e organizações em todos os setores. Agora você pode revidar com a proteção contra exfiltração da camada de aplicativo. Os Forcepoint NGFWs criam listas de aprovação e rejeição automáticas e seletivas para tráfego de rede originado de aplicativos específicos em computadores de mesa, notebooks, servidores, compartilhamentos de arquivos e outros dispositivos de endpoint com base em dados contextuais de endpoint altamente granulares. Vai além dos firewalls típicos e previne tentativas de exfiltração de dados confidenciais de endpoints por meio de programas, aplicativos da Web, usuários e canais de comunicação não autorizados.

* "Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub e M. Marden, IDC Research, maio de 2017.

Plataforma única com muitas opções de implementação – tudo administrado a partir de uma console centralizada



Proteção incomparável

Os atacantes tornaram-se especialistas em invadir redes corporativas, aplicativos, data centers e endpoints. Depois que entram, roubam propriedade intelectual, informações de clientes e outros dados confidenciais, causando danos irreparáveis às empresas e às respectivas reputações.

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

As evasões funcionam em vários níveis para camuflar exploits e malwares, tornando-os invisíveis para a inspeção tradicional de pacotes baseada em assinaturas. Com as evasões, até mesmo ataques antigos que foram bloqueados por anos podem ser reformulados para comprometer sistemas internos.

O Forcepoint NGFW usa uma abordagem diferente. Nosso mecanismo de segurança líder do setor foi projetado para os três estágios de defesa de redes: derrotar evasões, detectar explorações de vulnerabilidades e bloquear malwares. Pode ser implementado de forma transparente por trás de firewalls existentes para adicionar proteção sem interrupção ou como parte de nosso NGFW completo para segurança "tudo em um".

Além disso, o Forcepoint NGFW fornece descriptografia rápida de tráfego criptografado, incluindo conexões HTTPS, combinada com controles de privacidade granulares que mantêm a sua empresa e os usuários seguros em um mundo que muda muito rápido. Pode até limitar o acesso de aplicativos de endpoint específicos para bloquear dispositivos ou impedir o uso de softwares vulneráveis.

Resultados de negócios

- → 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 implementar novos patches
- → TCO mais baixo para infraestrutura de rede e segurança

Principais recursos

- → Conectividade SD-WAN em escala corporativa
- → IPS integrado com defesas antievasão
- → Clustering de alta disponibilidade para dispositivos e redes
- → Atualizações automáticas sem tempo de parada
- → Administração centralizada orientada por políticas
- → Visibilidade acionável e interativa em 360°
- → Proxies de segurança Sidewinder para aplicativos de missão crítica
- → Contexto de usuário e endpoint centrado nas pessoas
- → Descriptografia de alto desempenho com controles de privacidade granulares
- → Listas de aprovações e rejeições por aplicativo cliente e versão
- → Integração de CASB e Web Security
- → Sandboxing antimalware
- → Software unificado para implementações físicas, AWS, Azure, VMware

Especificações do Forcepoint Next Generation Firewall (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 gerenciamento centralizado de nível empresarial com recursos de análise de registros, 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 de várias camadas, inspeção profunda a todo vapor, defesa antievasão, detecção de contexto dinâmico, manipulação/inspeção de tráfego específico de protocolo, descriptografia granular de tráfego SSL/TLS (TLS 1.2 e 1.3), detecção de exploits de vulnerabilidades, impressão digital personalizada, reconhecimento, antibotnets, correlação, registro de tráfego, proteção contra DoS/DDoS, métodos de bloqueio, atualizações automáticas
Identificação de usuários	Banco de dados de usuários internos, LDAP nativo, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Certificados de clientes
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 relay 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, proxy IGMP › Roteamento com reconhecimento de aplicativo
IPv6	Pilha dupla IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, recursos completos de NGFW
Redirecionamento de proxy	Redirecionamento de protocolos HTTP, HTTPS, FTP, SMTP para Forcepoint ou Serviço de Inspeção de Conteúdo (CIS) de terceiros no local e na nuvem
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 URLs (Assinatura separada)	Listas de URLs personalizadas ou importadas
Aplicativos de endpoint	Nome e versão do aplicativo
Aplicativos de rede	Mais de 7.400 aplicativos de rede e nuvem
Segurança Sidewinder Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

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 para baixo 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 com base na nuvem
Antivírus	Mecanismo de verificação antivírus local*
Sandboxing de dia zero	Forcepoint Advanced Malware Detection disponível como serviço na nuvem e local

*A verificação antimalware local não está disponível em appliances 110/115.