Forcepoint

产品资料

Next Generation Firewall

具备原生 SD-WAN 功能的企业网络安全

主要优点

面向企业的持续 SD-WAN 连接

当今企业需要完全具备弹性的网络安全解决方案。Forcepoint Next-Gen Firewall (NGFW) 在所有级别均具备高可扩展能力和可用性。

- **主动-主动混合集群。**最多可将 16 个运行不同版本的不同模型节点聚集在一起。这可提供卓越联网性能高和弹性，并实现诸如深度数据包检测和 VPN 等安全功能。
- **无缝策略更新和软件升级。** Forcepoint 行业领先的可用性，能够实现策略更新（甚至软件升级）无缝推送到集群，而不会中断服务。
- **SD-WAN 网络集群。** 将高可用性覆盖范围扩展到网络和 VPN 连接。将不间断安全与利用本地宽带连接的能力相结合，以补充或取代昂贵的租赁线路，如 MPLS。

Forcepoint Next-Gen Firewall 可采用快速灵活的 SD-WAN 连接提供行业领先的网络安全，以便在多样化、不断演变的企业网络中连接并保护人员及其数据。Forcepoint NGFW 在物理、虚拟和云系统中提供一致的安全、绩效和运营。它从头开始设计，可实现高可用性和可扩展性，以及集中管理和全方位 360° 可见性。

切换到 Forcepoint NGFW 的客户报告网络攻击下降 86%，减少 IT 负担 53%，维护时间减少 70%。*

跟上不断变化的安全需求

Forcepoint 采用统一软件核，能够在动态业务环境中处理多个安全角色，从防火墙/VPN 和ZTNA 应用连接器到入侵防御 系统 (IPS) 和二层防火墙。Forcepoint 可以各种方式部署（例如物理、虚拟、云设备），所有部署都通过单一控制台进行管理。

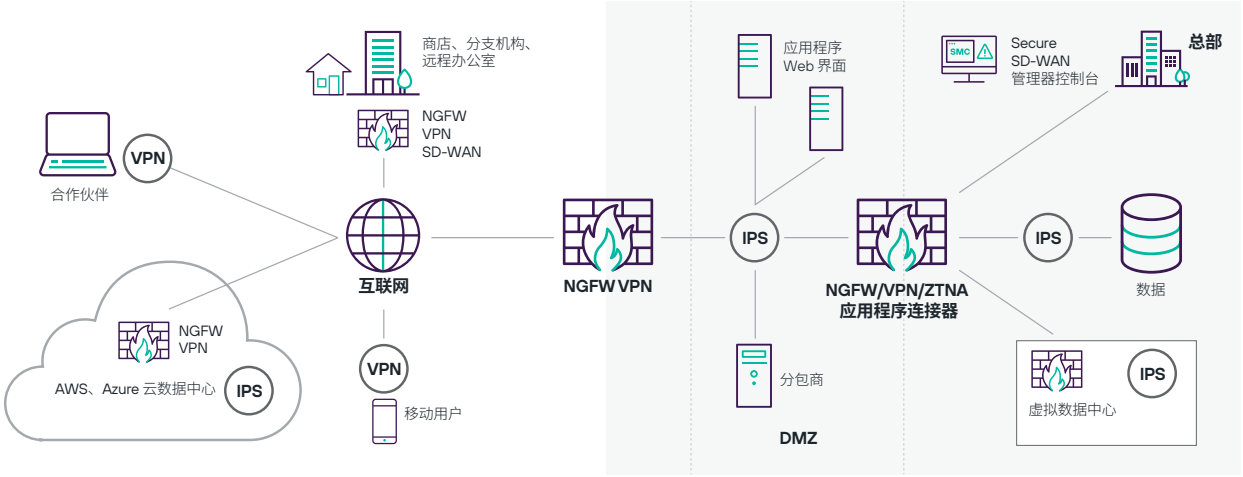
Forcepoint 为每个连接定制访问控制和深度检测，以提供高性能和安全性。它将细粒度应用控制、IPS防御、内置虚拟专用网络 (VPN) 控制和关键任务应用代理结合成高效、可扩展且高度可扩展的设计。我们强大的反逃避技术在检查之前对所有网络流量进行解码并标准化，以揭露并阻止最先进的攻击方法。

拦截复杂的数据外泄攻击

大规模数据泄露继续困扰各个行业的企业和组织。可应用层数据泄露保护应对这一威胁。Forcepoint 根据高度精细的端点上下文数据，有选择性地和自动地允许或阻止来自个人计算机、笔记本电脑、服务器、文件共享和其他端点设备上的特定应用程序的网络流量。它超越了典型的防火墙，防止敏感数据通过未经授权的程序、Web 应用程序、用户和通信渠道从端点泄露。

* "量化切换到 Forcepoint NGFW 的运营和安全结果"，R. Ayoub & M. Marden，IDC Research，2017 年 5 月。

提供多种部署选项的平台 - 所有部署都通过单一控制台进行管理



无与伦比的防护性能

攻击者已成为渗透企业网络、应用程序、数据中心和端点的专家。一旦进入内部，他们就会窃取知识产权、客户信息和其他敏感数据，对企业及其各自的声誉造成不可弥补的损害。

新的攻击技术可以规避传统安全网络设备的检测，包括许多名牌防火墙，已不再是简单的漏洞利用传输。规避在多个层面上工作，以伪装漏洞和恶意软件，使其在传统的基于签名的数据包检查中不可见。即使已阻止多年的攻击也可以通过规避进行重新包装，以损害内部系统。

Forcepoint 采用不同的方法。我们的行业领先安全引擎专为网络防御的所有三个阶段设计：击败规避、检测漏洞利用以及阻止恶意软件。它可以透明地部署在现有防火墙后面，在不中断的情况下增加保护，也可以作为功能齐全的企业防火墙，实现一体化的安全。

此外，Forcepoint 可提供加密流量的快速解密，包括 HTTPS 网络连接，结合精细化隐私控制，在瞬息万变的世界中确保您的业务和用户安全。它甚至可以限制特定端点应用程序的访问权限，以锁定设备或防止使用易受攻击的软件。

业务成果

- → 加快部署分支机构、云或数据中心
- → 减少停机时间
- → 无干扰，更安全
- → 减少泄露
- → 在 IT 团队准备部署新补丁的同时，减少新漏洞的风险
- → 降低网络基础设施和安全的 TCO

主要特点

- → 企业规模的 SD-WAN 连接
- → SASE/SSE 集成，实现网络、云、私人应用程序安全
- → 具备反规避防御功能的内置 IPS
- → 设备和网络的高可用性集群
- → 零停机自动更新
- → 策略驱动的集中式管理
- → 可操作、交互式 360°可视性
- → 适用于关键任务应用程序的 Sidewinder 安全代理
- → 用户和端点上下文信息
- → 通过精细化隐私控制实现高效解密
- → 允许/阻止客户端应用程序和版本
- → 应用程序运行状况监控
- → CASB 与 Web Security 集成
- → 防恶意软件沙盒
- → 统一软件，适用于实体、AWS, Azure, 、VMware 部署
- → 在 IT 团队准备部署新补丁的同时，减少新漏洞的风险
- → 降低网络基础设施和安全的 TCO

Forcepoint NGFW 规格

平台	
物理设备	有多种硬件设备方案，包括在分支机构和数据中心部署
云基础设施	Amazon Web Services、Microsoft Azure、谷歌、Oracle、IBM
虚拟设备	x86 64 位架构系统；VMware ESXi、VMware NSX、Microsoft Hyper-V、KVM 和 Nutanix AHV
端点	Endpoint Context Agent (ECA)、VPN 客户端
虚拟情景	高达 250
集中式管理	企业级集中管理系统，具有日志分析、监控和报告功能。有关详细信息，请参阅 Forcepoint 安全管理中心产品资料。

防火墙功能	
深度数据包检测	多层流量标准化/全流深度检测、反逃避防御、动态上下文检测、特定于协议的流量处理/检查、SSL/TLS 流量的粒度解密（包括 TLS 1.2 和 1.3）、漏洞利用检测、自定义指纹识别、侦察、反僵尸网络、关联、流量记录、DoS/DDoS 保护、阻止方法、自动更新
用户身份识别	内部用户数据库、原生的 LDAP、Microsoft Active Directory、RADIUS、TACACS+、Microsoft Exchange、客户端证书
高可用性	› 主用-主用/主用-备用防火墙集群包含多达 16 个节点 › SD-WAN › 有状态失效备援（包括 VPN 连接） › 服务器负载均衡 › 链路聚合 (802.3ad) › 链路故障检测
IP 地址分配	› IPv4 静态、DHCP、PPPoA、PPPoE、IPv6 静态、SLAAC、DHCPv6 › 服务：适用于 IPv4 的 DHCP 服务器和适用于 IPv4 和 IPv6 的 DHCP 中继
路由	› 静态 IPv4 和 IPv6 路由、基于策略的路由、静态组播路由 › 动态路由：RIPv2、RIPng、OSPFv2、OSPFv3、BGP、MP-BGP、BFD、PIM-SM、PIM-SSM、IGMP 代理 › 应用程序感知路由
IPv6	双栈 IPv4/IPv6、NAT64、ICMPv6、DNSv6、NAT、完整 NGFW 功能
代理重定向	HTTP、https、FTP、SMTP 协议重定向到 Forcepoint 或第三方内容检查服务 (CIS) 本地和云
地域防护	动态更新的来源和目的地国家/地区或大洲
IP 地址列表	预定义 IP 类别或使用自定义或导入的 IP 地址列表
网址过滤（单独订阅）	自定义或导入的 URL 列表；支持 QUIC 和 HTTP/3
端点应用程序名称和版本	端点应用程序名称和版本
网络应用程序	7400+ 网络和云应用程序
Sidewinder Security Proxies	TCP、UDP、HTTP、HTTPS、SSH、FTP、TFTP、SFTP、DNS

›

SASE 集成	
网络流量转发	GRE 和 IPsec 隧道到 Security Service Edge (SSE) 平台，如 Forcepoint ONE
ZTNA 应用程序连接器	支持内部数据中心中的私人应用程序连接到 Forcepoint ONE 的 Zero Trust

SD-WAN	
协议	Ipsec 和 TLS
站点到站点 VPN	› 基于策略和路由的 VPN › 中心辐射型拓扑、全网状拓扑、半网状拓扑、混合型拓扑 › 动态选择多个 ISP 链路 › 负载共享、主用/备用、链路聚合 › 实时监控和报告 ISP 链路质量（延迟、抖动、丢包）
远程访问	› 适用于 Microsoft Windows、Android 和 Mac OS 的 Forcepoint VPN 客户端 › 任何标准 IPsec 客户端 › 高可用性、自动失效备援 › 客户端安全检查 › TLS VPN 门户访问

高级恶意软件检测和文件控制	
协议	FTP、HTTP、HTTPS、POP3、IMAP、SMTP
文件筛选	基于策略的文件筛选，具有高效的筛选流程。支持 19 个文件类别中的 200 多种文件类型
文件信誉	基于云的高速恶意软件信誉检查和拦截
反病毒	本地防病毒扫描引擎*
零日沙盒	Forcepoint 高级恶意软件检测和保护，既可作为云端服务也可作为本地服务

* 本地反恶意软件扫描不适用于 110/115 设备。