Forcepoint 下一代防火墙 (NGFW)

企业 SD-WAN 与最安全的网络保护措施相结合

Forcepoint NGFW 将快速、灵活的网络（SD-WAN 和 LAN）与业界领先的安全保护措施相结合，可通过各种不断发展的企业网络连接和保护员工及其使用的数据。Forcepoint NGFW 在物理、虚拟和云系统中皆具有一致的安全性、性能和操作。产品设计从根本上保证了高可用性和可扩展性，还提供 360° 全面可视性的集中式管理。

让企业始终畅享 SD-WAN 连接

如今，企业需要弹性极高的网络安全解决方案。Forcepoint NGFW 可在各个级别实现高可扩展性和可用性：

- **主动-主动、混合集群。**最多可将 16 个型号和版本各不相同的节点集中在一起。可实现卓越的网络性能和弹性，并实现深度数据包检测和 VPN 等安全性能。
- **无缝策略更新和软件升级。**Forcepoint 在可用性方面保持业界领先，可在不中断服务的情况下，将策略更新（甚至软件升级）无缝推送到集群。
- **SD-WAN 网络集群。**让网络连接和 VPN 连接也实现高可用性。将全天候安全保护与利用本地宽带连接的能力结合，以补充或取代昂贵的租用线路（如 MPLS）。

根据切换到 Forcepoint NGFW 的客户反馈，网络攻击减少了 86%，IT 负担减轻了 53%，维护时间缩短了 70%。*

跟上不断变化的安全需求

Forcepoint NGFW 采用统一软核结构，因此能够在瞬息万变的商业环境中胜任多种安全角色（包括防火墙/VPN、IPS 和第 2 层防火墙）。Forcepoint NGFW 可通过多种方式（例如物理、虚拟、云设备）部署，所有部署都从单一控制台进行管理。

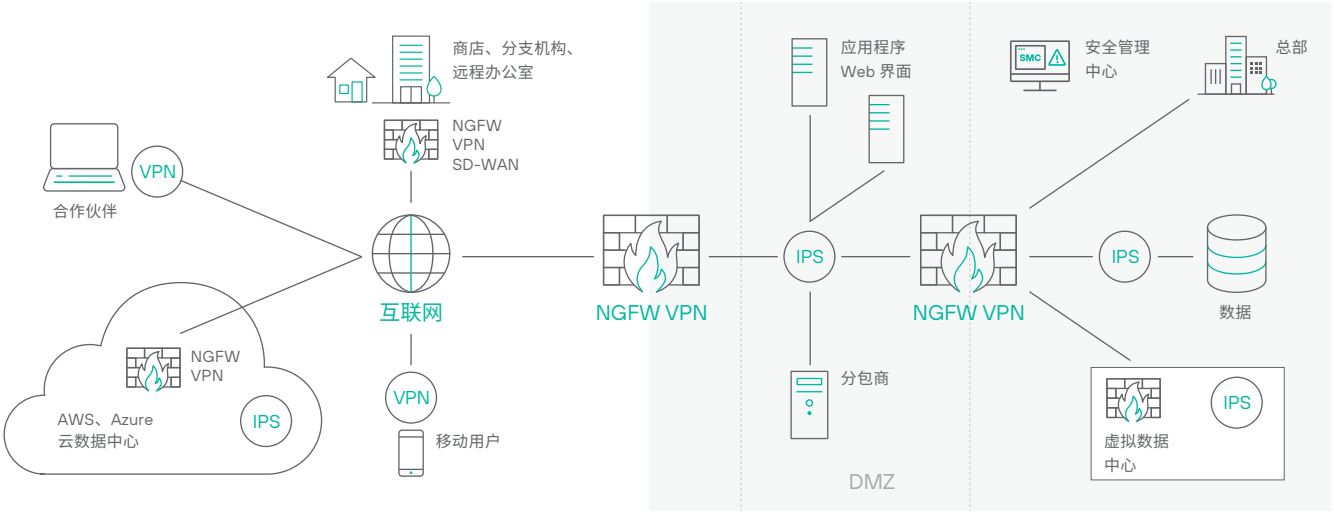
Forcepoint 针对每个连接定制唯一的访问控制和深度检测，从而提供高性能和安全性。它将细粒度应用程序控制、入侵防御系统 (IPS)、内置虚拟专用网 (VPN) 控制和任务关键型应用程序代理整合到一个高效、灵活、高度可扩展的设计中。我们强大的防规避技术能够在检测之前解码并规范化各个协议层的网络流量，从而发现并拦截最先进的攻击方法。

拦截复杂的数据泄露攻击

大型数据泄露仍然困扰着各行各业的企业和组织。现在，应用层外泄防护解决方案可以对抗这种情况。Forcepoint NGFW 可以根据非常细粒度的端点情景数据，有选择性地将来自个人电脑、笔记本电脑、服务器、文件共享设备及其他端点设备上特定应用程序的网络流量自动列入白名单或黑名单。该解决方案超越了典型的防火墙，可防止攻击者试图通过未经授权的程序、Web 应用程序、用户和通信渠道窃取端点设备中的敏感数据。

* “量化切换到 Forcepoint NGFW 的操作和安全结果 (Quantifying the Operational and Security Results of Switching to Forcepoint NGFW)”，R. Ayoub & M. Marden，IDC Research，2017 年 5 月。

一个平台，多种部署选项 - 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

现在的攻击者精通各种攻破企业网络、应用程序、数据中心和端点的手段。一旦攻破防线，攻击者就可以窃取知识产权、客户信息及其他敏感数据，导致企业的业务及其信誉都蒙受无法弥补的损失。

新的攻击手段可以规避传统网络安全设备（其中不乏许多知名的防火墙产品）的检测，不再局限于单纯利用漏洞进行传输。

规避技术可在多个层级对漏洞和恶意软件进行伪装，导致基于签名的传统数据包检测无法识别它们。通过规避技术，即使是多年前就会被拦截的旧攻击也可通过重新包装入侵内部系统。

Forcepoint NGFW 却不一样。我们业界领先的安全引擎专为网络防御的全部三个阶段而设计：挫败规避企图，检测容易被利用的漏洞，以及阻止恶意软件的入侵。它可以透明部署在现有防火墙后面，强化保护的同时不会有任何负面影响；或者作为全功能 NGFW，打造多合一的安全屏障。

此外，Forcepoint NGFW 可快速解密加密流量，包括 HTTPS Web 连接，结合细粒度隐私控制，在瞬息万变的环境中确保您的企业和用户安全。其甚至可以限制对特定端点应用程序的访问，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时，减少遭遇新漏洞的风险
- → 降低网络基础设施及安全措施的总体拥有成本 (TCO)

主要特点

- → 企业规模的 SD-WAN 连接
- → 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
- → 适用于任务关键型应用程序的 Sidewinder 安全代理
- → 以人为中心的用户和端点环境
- → 具有细粒度隐私控制的高性能解密
- → 按客户应用程序和版本列入白名单/黑名单
- → CASB 与 Web Security 集成
- → 防恶意软件沙盒
- → 适用于物理、AWS、Azure、VMware 部署的统一软件

Forcepoint 下一代防火墙 (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
虚拟设备	x86 64 位系统：VMware ESXi、VMware NSX、Microsoft Hyper-V 和 KVM
终端	Endpoint Context Agent (ECA)、VPN 客户端
虚拟情景	最多 250 个
集中式管理	企业级集中式管理系统，具备日志分析、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	多层流量规范化/全流式深度检测、反规避防御、动态情景检测、特定协议流量处理/检查、SSL/TLS 流量细粒度解密、漏洞攻击检测、自定义指纹识别、侦察、防僵尸网络、相关性、流量记录、DoS/DDoS 保护、拦截方法、自动更新
用户身份识别	内部用户数据库、本地 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 服务器以及适用于 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、v6、DNSv6、NAT、全功能 NGFW
代理重定向	HTTP、HTTPS、FTP、SMTP 协议重定向到本地和云端的 Forcepoint 或第三方内容检测服务 (CIS)
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
URL 过滤（单独订购）	自定义或导入的 URL 列表
端点应用程序	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 安全代理	TCP、UDP、HTTP、HTTPS、SSH、FTP、TFTP、SFTP、DNS

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 › 任意标准 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
文件过滤	基于策略的文件过滤，具有高效的下拉选择流程。 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
防病毒保护	本地防病毒扫描引擎*
零日沙盒化	Forcepoint 高级恶意软件检测可同时作为云端和本地服务提供

* 110/115 设备不具备本地防恶意软件扫描功能。

[Forcepoint-NGFW-Datasheet-ZH-CN] 26Jun2020