Forcepoint

Datasheet

Next Generation Firewall

Enterprise Network Security with native SD-WAN capabilities

Key Benefits

Always-on SD-WAN connectivity for enterprises

Today's businesses demand fully resilient network security solutions. Forcepoint Next-Gen Firewall (NGFW) builds in high scalability and availability at all levels.

- **Active-active, mixed clustering.** Up to 16 nodes of different models running different versions can be clustered together. This provides superior networking performance and resilience, and enables security such as deep packet inspection and VPNs.
- **Seamless policy updates and software upgrades.** Forcepoint's industry-leading availability enables policy updates (and even software upgrades) to be seamlessly pushed to a cluster without interrupting service.
- **SD-WAN network clustering.** Extends high-availability coverage to network and VPN connections. Combines nonstop security with the ability to take advantage of local broadband connections in order to complement or replace expensive leased lines like MPLS.

Forcepoint Next-Gen Firewall provides industry-leading network security with fast, flexible SD-WAN connectivity to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Forcepoint NGFW delivers consistent security, performance, and operations across physical, virtual, and cloud systems. It is designed from the ground up for high availability and scalability, along with centralized management and full 360° visibility.

Customers who switch to Forcepoint NGFW report an 86% drop in cyberattacks, 53% less burden on IT, and 70% less maintenance time.*

Keep pace with changing security needs

A unified software core enables Forcepoint to handle multiple security roles, from firewall/VPN and ZTNA Application Connector to Intrusion Prevention System (IPS) and layer 2 fire wall, in dynamic business environments. Forcepoint can be deployed in a variety of ways (e.g., physical, virtual, cloud appliances), all managed from a single console.

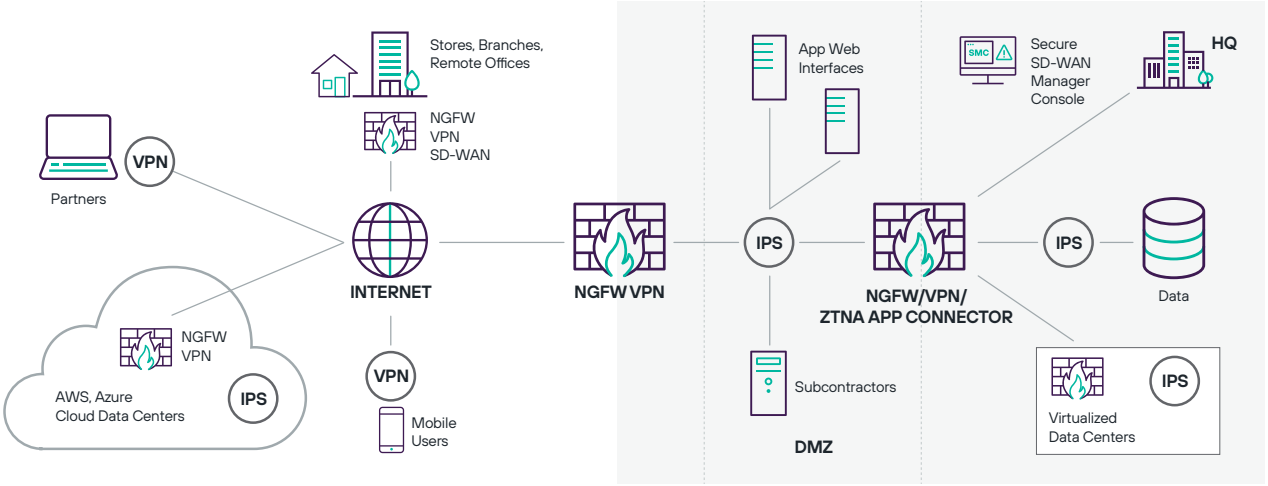
Forcepoint uniquely tailors access control and deep inspection for each connection to provide high performance and security. It combines granular application control, IPS defenses, built-in virtual private network (VPN) control, and mission-critical application proxies into an efficient, extensible, and highly scalable design. Our powerful anti-evasion technologies decode and normalize network traffic before inspection and across all protocol layers to expose and block the most advanced attack methods.

Block sophisticated data breach attacks

Large data breaches continue to plague businesses and organizations in every industry. Combat this threat with application-layer exfiltration protection. Forcepoint selectively and automatically allows or blocks network traffic originating from specific applications on PCs, laptops, servers, file shares, and other endpoint devices based on highly granular endpoint contextual data. It goes beyond typical firewalls to prevent attempted exfiltration of sensitive data from endpoints via unauthorized programs, web applications, users, and communication channels.

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

One platform with many deployment options—all managed from a single console



Unmatched protection

Attackers have become experts in penetrating enterprise networks, applications, data centers, and endpoints. Once inside,they steal intellectual property, customer information, and othersensitive data, causing irreparable damage to businesses and their respective reputations.

New attack techniques can evade detection by traditional security network devices, including many name-brand firewalls, moving beyond the simple transmission of vulnerability exploits.

Evasions work at multiple levels to camouflage exploits and malware, making them invisible to traditional signature-based packet inspection. Even attacks that have been blocked for years can be repackaged with evasions to compromise internal systems.

Forcepoint takes a different approach. Our industry leading security engine is engineered for all three stages of network defense: to defeat evasions, detect exploits of vulnerabilities, and stop malware. It can be deployed transparently behind existing firewalls to add protection without disruption, or as a full-featured Enterprise Firewall for all-in-one security.

In addition, Forcepoint provides fast decryption of encrypted traffic, including HTTPS web connections, combined with granular privacy controls that keep your business and users safe in a rapidly changing world. It can even limit access from specific endpoint applications to lock down devices or prevent the use of vulnerable software.

Business outcomes

- → Faster rollout of branches, clouds or data centers
- → Less downtime
- → Greater security without disruption
- → Fewer breaches
- → Less exposure to new vulnerabilities while IT teams prepare to deploy new patches
- → Lower TCO for network infrastructure and security

Key features

- → SD-WAN connectivity at enterprise scale
- → SASE/SSE Integration for web, cloud, private app security
- → Built-in IPS with anti-evasion defenses
- → High-availability clustering of devices and networks
- → Automated, zero-downtime updates
- → Policy-driven centralized management
- → Actionable, interactive 360° visibility
- → Sidewinder security proxies for mission-critical applications
- → User and endpoint context
- → High-performance decryption with granular privacy controls
- → Allow/block by client application and version
- → Application health monitoring
- → CASB and Web Security integration
- → Anti-malware sandboxing
- → Unified software for physical, AWS, Azure, VMware deployments
- → Less exposure to new vulnerabilities while IT teams prepare to deploy new patches
- → Lower TCO for network infrastructure and security

Forcepoint NGFW specifications

PLATFORMS	
Physical Appliance	Multiple hardware appliance options, ranging from branch office to data center installations
Cloud Infrastructure	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Virtual Appliance	x86 64-bit based systems; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM, and Nutanix AHV
Endpoint	Endpoint Context Agent (ECA), VPN Client
Virtual Contexts	Up to 250
Centralized Management	Enterprise-level centralized management system with log analysis, monitoring, and reporting capabilities. See the Forcepoint Security Management Center datasheet for details.

FIREWALL FEATURES	
Deep Packet Inspection	Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti-Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates
User Identification	Internal user database, Native LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Client Certificates
High Availability	› Active-active/active-standby firewall clustering up to 16 nodes › SD-WAN › Stateful failover (including VPN connections) › Server load balancing › Link aggregation (802.3ad) › Link failure detection
IP Address Assignment	› IPv4 static, DHCP, PPPoA, PPPoE, IPv6 static, SLAAC, DHCPv6 › Services: DHCP Server for IPv4 and DHCP relay for IPv4 and IPv6
Routing	› Static IPv4 and IPv6 routes, policy-based routing, static multicast routing › Dynamic routing: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD,PIM-SM, PIM-SSM, IGMP proxy › Application-aware routing
IPv6	Dual-stack IPv4/IPv6, NAT44, NAT64, NAT66, ICMPv6, DNSv6, NAT, Full NGFW features
Proxy Redirection	HTTP, HTTPS, FTP, SMTP protocols redirection to Forcepoint or third-party Content Inspection Service (CIS) on-premise and cloud
Geo-Protection	Dynamically updated source/destination country or continent
IP Address List	Predefined IP categories or using custom or imported IP address lists
URL Filtering (Separate Subscription)	Custom or imported URL lists; supports QUIC and HTTP/3
Endpoint Applications	Application name and version
Network Applications	7400+ network and cloud applications
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

SASE INTEGRATION	
Web Traffic Forwarding	GRE and IPsec tunneling to Security Service Edge (SSE) platforms such as Forcepoint ONE
ZTNA Application Connector	Enables private applications in internal datacenters to connect to Forcepoint ONE's Zero Trust

SD-WAN	
Protocols	IPsec and TLS
Site-to-Site VPN	› Policy- and route-based VPN › Hub and spoke, full mesh, partial mesh, Hybrid topologies › Dynamic selection of multiple ISP Links › Load sharing, active/standby, link aggregation › Live monitoring and reporting on ISPs link quality (Delay, jitter, packet loss)
Remote Access	› Forcepoint VPN client for Microsoft Windows, Android, and Mac OS › Any standard IPsec client › High availability with automatic failover › Client security checks › Access to TLS VPN portal

ADVANCED MALWARE DETECTION AND FILE CONTROL	
Protocols	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
File Filtering	Policy-based file filtering with efficient down selection process. Over 200 supported file types in 19 file categories
File Reputation	High-speed cloud-based malware reputation checking and blocking
Anti-Virus	Local antivirus scan engine*
Zero-Day Sandboxing	Forcepoint Advanced Malware Detection and Protection available both as cloud and on-premises service

* Local anti-malware scan is not available with 110/115 appliances.