Forcepoint FlexEdge Secure SD-WAN

Always-on SD-WAN connectivity for enterprises

Today's businesses demand fully resilient network security solutions. FlexEdge Secure SD-WAN 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.

FlexEdge Secure SD-WAN combines fast, flexible networking (SD-WAN and LAN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. FlexEdge Secure SD-WAN provides consistent security, performance, and operations across physical, virtual, and cloud systems. It's designed from the ground up for high availability and scalability, as well as centralized management with full 360° visibility.

Keep pace with changing security needs

A unified software core enables FlexEdge Secure SD-WAN to handle multiple security roles, from firewall/VPN to IPS to layer 2 firewall, in dynamic business environments. FlexEdge Secure SD-WANs 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 to each connection to provide high performance and security. It combines granular application control, intrusion prevention system (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. Now you can fight back with application-layer exfiltration protection. FlexEdge Secure SD-WANs electively and automatically whitelist or blacklist 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 network security to prevent attempted exfiltration of sensitive data from endpoints via unauthorized programs, web applications, users, and communications channels.

Forcepoint FlexEdge SD-WAN 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

NETWORK SECURITY FEATURES	
Deep Packet Inspection	Multi-Layer Traffic Normalization/Full-Steam 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 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, NAT64, ICMPv6, DNSv6, NAT
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
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

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 available both as cloud and on-premises service

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

Forcepoint