McAfee Next Generation Firewall

McAfee® Next Generation Firewall protects enterprise networks with high-performance "intelligence aware" security supported by real-time updates from the Security Connected ecosystem. This enables McAfee, a part of Intel Security, to deliver the industry's best defense against advanced evasions, along with complete next-generation firewall (NGFW) protections when and where you need it—at remote sites, branch offices, data centers, and the network edge.

Key Benefits

- The best protection for your business and digital assets.
- Adapts easily to your security needs.
- Scales effortlessly as your business grows.
- Optimizes productivity of employees and customers.
- Lowers TCO for both your security and network infrastructure.

Key Features

- Superior NGFW protection.
- "Intelligence aware" security controls.
- Advanced evasion prevention.
- Unified software core design.
- High availability options for security and network infrastructure.
- Powerful centralized management.
- Built-in SSL VPN and IPsec VPN.

McAfee Next Generation Firewall starts with a solid foundation of protections, including granular application control, an intrusion prevention system (IPS), built-in virtual private network (VPN), and deep packet inspection, all in an efficient, extensible, and highly scalable unified design. Then we add powerful anti-evasion technologies that decode and normalize network traffic—before inspection and across all protocol layers—to expose and block the most advanced attack methods.

Superior Flexibility to Keep Pace with Changing Security Needs

A unified software core enables McAfee Next Generation Firewall to easily change security roles, from NGFW to IPS to layer 2 firewall, in dynamic business environments. The unified software core also serves to optimize the data plane, providing a significant performance advantage regardless of security role or number of active security features. For even more flexibility, McAfee Next Generation Firewall can be deployed in a wide variety of formats—as a physical appliance, software solution, virtual appliance, or as virtual contexts on a physical appliance.

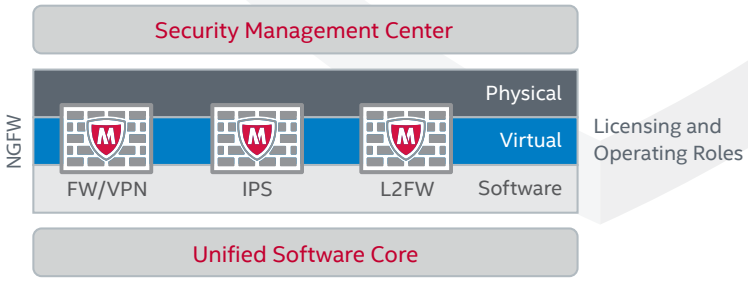

Figure 1. McAfee Next Generation Firewall adapts to multiple roles and installations.

intel Security

High Scalability and Availability to Secure Business-Critical Applications

Today's businesses demand fully resilient network security solutions. McAfee Next Generation Firewall delivers high scalability and availability in three powerful ways:

- **Native active clustering:** Up to 16 nodes can be clustered together, providing superior performance and resiliency when running demanding security applications, such as deep packet inspection and VPNs.
- **Transparent session failover:** Provides industry-leading availability and serviceability of security systems. McAfee Next Generation Firewall even supports transparent failover for multiple software and hardware versions within the same cluster.
- **McAfee Multi-Link:** Extends high availability coverage to network and IPsec VPN connections. Provides the confidence of non-stop security along with high performance for every deployment.

Unmatched Protection to Keep Your Business in Business

It's no secret. Every day attackers get better at penetrating enterprise networks, applications, data centers, and endpoints. Once inside, they can steal intellectual property, customer information, and other sensitive data, causing irreparable damage to your business and global reputation.

Unknown to many security administrators, determined attackers can use advanced evasion techniques (AETs) to bypass most of today's security devices. AETs deliver advanced persistent threats (APTs) through advanced techniques such as masking and obfuscation. Once inside your network, threats are reassembled. Here they can hide, execute, and propagate unchallenged.

McAfee Next Generation Firewall uses a variety of techniques on network traffic to identify applications and users at a granular level. Security policies can then be applied based on strict business rules. Then McAfee Next Generation Firewall performs specialized deep packet inspection, including advanced techniques such as full stack normalization and horizontal data stream-based inspection. These techniques normalize traffic flows, enabling McAfee to expose AETs and traffic anomalies that other NGFWs miss. Only after traffic has been fully normalized can it be properly inspected across all protocols and layers for threats and malware. And only McAfee Next Generation Firewall has been successfully tested against more than 800 million AETs.

Knowledge Is Power

Point security solutions restrict knowledge sharing, weakening their ability to recognize and block threats. The Security Connected threat ecosystem enables rapid sharing of extensive real-time threat information, empowering organizations to defeat cybercrime with the latest global and local threat knowledge. Security Connected enables McAfee Next Generation Firewall to leverage threat information from a wide variety of third party sources, as well as other McAfee security solutions including:

- **ePolicy Orchestrator® (McAfee ePO™) software:** Allows McAfee Next Generation Firewall to obtain contextual information from users and their host systems, providing valuable insights into endpoint security postures. This information can also be used to simplify workflows when troubleshooting or investigating threats or problems.
- **McAfee Enterprise Security Manager:** Ensures continuous monitoring and alerting of compliance status, providing real-time situational awareness while improving security posture and reducing event response times.

- **McAfee Advanced Threat Defense:** Delivers superior protection against zero-day threats through dynamic sandboxing of malware and static inspection of suspect code. McAfee Advanced Threat Defense integration also allows McAfee Next Generation Firewall to offload inspection of suspect files for rapid threat feedback without impacting network performance.
- **McAfee Global Threat Information:** Provides McAfee Next Generation Firewall with superior reputation intelligence to protect against globally active advanced threats and malware.

Security Connected, along with the flexibility of McAfee Next Generation Firewall, enables dynamic enterprises to quickly and easily deploy multilayered security solutions when and where they are needed.

Powerful Centralized Management for Lower TCO

In order to contain costs and optimize resources, today's businesses need operational and workflow efficiency when managing their NGFWs. McAfee Security Management Center provides centralized management and visibility of any role or features used on McAfee Next Generation Firewall. From a central location, McAfee Security Management Center gains deep insight into applications, user traffic, and shared content. A simple graphical user interface enables easy configuration, management, and monitoring of the entire system, lowering operational expenses so you can keep your business running smoothly as threats and related security needs evolve.

McAfee Next Generation Firewall Specifications

Supported Platforms	
Appliances	Multiple hardware appliances with firewall throughput of 5 Gbit/s to 120 Gbit/s. See the appliance comparison data sheets for more details.
Software Appliance	X86-based systems
Virtual Appliance	VMware ESX and KVM support
Supported Roles	Firewall/VPN (layer 3), IPS mode (layer 2), layer 2 firewall
Virtual Contexts	Virtualization to separate logical contexts (FW, IPS, or L2FW) with separate interfaces, addressing, routing, and policies
Firewall/VPN-Specific Functionality	
General	Stateful and stateless packet filtering, circuit-level firewall with TCP proxy protocol agent
Firewall Protocol Agents	FTP, H.323, HTTP, HTTPS, IMAP4, MGCP, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH, RTSP, SCCP, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP
User Authentication	• Internal user database, LDAP • Microsoft Active Directory, RADIUS, TACACS+
High Availability	• Active-active/active-standby firewall clustering up to 16 nodes • Stateful failover (including VPN connections) • VRRP • Server load balancing • Link aggregation (802.3ad) • Link failure detection
ISP Multihoming	• McAfee Multi-Link: high availability and load balancing between multiple ISPs, including VPN connections, McAfee Multi-Link VPN link aggregation, QoS-based link selection
IP Address Assignment	• FW clusters: static, IPv4, IPv6 • FW single nodes: static, DHCP, PPPoA, PPPoE, IPv4, static IPv6 • Services: DHCP Server and DHCP relay for IPv4
Address Translation	• IPv4, IPv6 • Static NAT, source NAT with port address translation (PAT), destination NAT with PAT

McAfee Next Generation Firewall Specifications continued

Routing	Static IPv4 and IPv6 routes, policy-based routing, static multicast routing
Dynamic Routing	IGMP proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM
IPv6	Dual stack IPv4/IPv6, ICMPv6, DNSv6
SIP	Allows RTP media streams dynamically, NAT traversal, deep inspection, interoperability with RFC3261-compliant SIP devices
CIS Redirection	HTTP, FTP, SMTP protocols redirection to content inspection server (CIS)
IPsec VPN	
Protocols	IKEv1, IKEv2, and IPsec with IPv4 and IPv6
Encryption	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES[1]
Message Digest Algorithms	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Diffie-Hellman	DH group 1, 2, 5, 14, 19, 20, 21
Authentication	RSA, DSS, ECDSA signatures with X.509 certificates, pre-shared keys, hybrid, XAUTH, EAP
Other	• IPCOMP deflate compression • NAT-T • Dead peer detection • MOBIKE
Site-to-Site VPN	• Policy-based VPN, route-based VPN (GRE, IP-IP, SIT) • Hub and spoke, full mesh, partial mesh topologies • McAfee Multi-Link fuzzy-logic-based dynamic link selection • McAfee Multi-Link modes: load sharing, active/standby, link aggregation
Client-to-Gateway VPN	• IPsec VPN client for Microsoft Windows • Automatic configuration updates from gateway • Automatic failover with McAfee Multi-Link • Client security checks • Secure domain logon
SSL VPN	
Client-Based Access	• Supported platforms: Android 4.0, Mac 10.7[2] and Windows Vista SP2[3] (and newer versions)
Portal-Based Access	• OWA and Intranet access via SSL VPN portal through a browser
Antispam	
Scanned Protocols	SMTP
Engine	Scoring-based spam detection
Filtering Methods	• Customizable email envelope/header/content matching • Local anti-spoofing and relay • Honeypot filtering • SPF/MX record matching • DNS-based blacklists
IPS Mode And Layer 2 Firewall-Specific Functionality	
General	• Stateless packet filtering for Ethernet protocols (Dix/IEEE) • Stateful packet filtering for IP protocols • Logical Interface matching for VLANs and physical interfaces • VLAN re-tagging • MAC address filtering
High Availability	• Layer 2 firewall clustering (active-passive) • IDS clustering (active-active/active-passive) • IPS serial clustering (active-active) • Fail-open interface support (IPS mode) • Dynamic inspection overload handling (IPS mode)

McAfee Next Generation Firewall Specifications continued

General Functionality (All Roles)	
Encapsulation	Ethernet, 802.1q VLAN, PPPoA[4], PPPoE[5]
Access Control	• IPv4 and IPv6 tunneled IP IP-in-IP • IPV6 encapsulation GRE
Advanced Access Control	• Interface zones • Time • TLS information • Domain names • User information • Applications
Traffic Management and QoS	• Policy-based traffic shaping • Guaranteed/maximum/bandwidth prioritization • Differentiated services code point (DSCP) matching/marking • Policy-based concurrent session limiting • Policy-based TCP MSS rewrite
Inspection	
Anti-Botnet	• Decryption-based detection • Message length sequence analysis
Advanced Anti-Malware	Down-selection using file filtering, reputation, McAfee Advanced Threat Defense, and McAfee antivirus options
File Reputation	• Policy-based file filtering • File categories: archive, executable, media file, Microsoft Office document • File types: Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, Riff, RTF, ZIP • Classification from McAfee Global Threat Intelligence cloud service
Advanced Threat Defense	• File redirection to McAfee Advanced Threat Defense
Antivirus	• McAfee antivirus: file-based, local signature database, automatic real-time updates • Scanned protocols: FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Dynamic Context Detection	Protocol, application, file type (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, text file, binary file)
Protocol Normalization	Full protocol normalization for Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS (SSL/TLS), GRE, IP-in-IP, IPv6 encapsulation
Protocol-Specific Inspection	DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP
Protocol-Independent Fingerprinting	Any TCP/UDP protocol
Evasion and Anomaly Detection	• Multilayer traffic normalization • Vulnerability-based fingerprints • Fully upgradable software-based inspection engine • Evasion and anomaly logging
Custom Fingerprinting	• Protocol-independent fingerprint matching • Regular expression-based fingerprint language • Snort signature converter • Custom application fingerprinting
TLS Inspection	• HTTPS client and server stream decryption and inspection • TLS certificate validity checks • Certificate domain name-based exemption list
Correlation	Local correlation, log server correlation
DoS/DDoS Protection	• SYN/UDP flood detection • Concurrent connection limiting, interface-based log compression • Protection against slow HTTP request methods
Reconnaissance	TCP/UDP/ICMP scan, stealth, and slow scan detection in IPv4 and IPv6
Blocking Methods	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, redirect
Traffic Recording	Automatic traffic recordings/excerpts from misuse situations
Updates	• Automatic dynamic updates through McAfee Security Management Center • Current coverage of approximately 4,000 protected vulnerabilities

McAfee Next Generation Firewall Specifications continued

URL Filtering	
Protocols	HTTP, HTTPS
Engine	Webroot category-based URL filtering, blacklist/whitelist
Database	• More than 280 million top-level domains and sub-pages (billions of URLs) • Support for more than 43 languages, 82 categories
Management and Monitoring	
Centralized Management	Enterprise-level centralized management, logging and reporting system. See the McAfee Security Management Center data sheet for more details.
SNMP Monitoring	SNMPv1, SNMPv2c, and SNMPv3
Traffic Capturing	Console tcpdump, remote capture through SMC
High Security Management Communication	256-bit security strength in engine—management communication
Security Certifications	Common Criteria EAL4+, FIPS 140-2 crypto certificate, CSPN by ANSSI (First Level Security Certification)

[1] Supported encryption algorithms depend on license used.
[2] Available soon.
[3] Ibid.
[4] Firewall/VPN role only.
[5] Ibid.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com