McAfee Next Generation Firewall

McAfee® Next Generation Firewall changes how network security is delivered. McAfee Next Generation Firewall complements network edge solutions with a high-performance, advanced next-generation firewall (NGFW) solution that is versatile and adaptable. It adds control, visibility, and protection—including advanced anti-evasion techniques—where you need it most, including remote sites and branches, data centers, and the network edge.

Key Advantages

- One adaptive, affordable solution for all environments.
- One unified software-based design for all network security controls.
- One integrated central management center.
- One solution that provides the industry's most powerful anti-evasion capabilities.
- One solution that scales with your business.
- One solution that deploys three ways: hardware appliance, virtual appliance, and software.

Most legacy firewalls force enterprises to choose between critical features and then bolt on new security components as separate, individually managed boxes. Some NGFWs offer impressive features without the performance and availability required for reliable protection and control during demanding operations.

McAfee Next Generation Firewall has been built from the ground up to deliver application control, intrusion prevention system (IPS), and virtual private network (VPN) functionality—as well as innovative evasion prevention capabilities in an efficient, extensible, and highly scalable design.

Offering more than just deep packet inspection, McAfee Next Generation Firewall includes powerful anti-evasion technologies that decode and normalize network traffic for inspection on all protocol layers, making traffic evasion-free and exploits detectable. Vulnerability-based fingerprints block exploits in the normalized data stream.

One Unified Software Core

McAfee Next Generation Firewall is available as a physical appliance, software solution, or virtual appliance. All options are based on a unified software core and receive new features and updates automatically. The solution has been designed from the ground up to offer significant performance advantages and ease of use compared with traditional multifunction products.

One Management Center

With the McAfee Security Management Center, administrators have the ability to manage and/or monitor all security devices and relevant information across the network. This is done by enabling policy management of the appliance, tracking usage at the application and user level, applying policies, and generating reports.

McAfee Security Management Center gives you the power and flexibility to place the right network security where you need it and keep your business running smoothly as needs and threats evolve.

Self-Customization

McAfee Next Generation Firewall lets administrators choose, self-configure, and change platforms, capacity, security controls, and features easily—without extra fees or new contracts. McAfee Next Generation Firewall meets the needs of multiple network security applications.

- *Firewall/VPN concentrator*—Provides a powerful and fully resilient firewall with application control, deep packet inspection, and advanced virtual private networking (VPN) capabilities.
- *NGFW-IPS mode*—Performs layer 7 application analysis and can detect sophisticated attacks, such as advanced evasion techniques (AETs) at the network edge or manage application traffic within network segments.
- *Layer 2 firewall*—Convenient when you need the network segmentation, but cannot use routing; this mode also supports filtering of non-IP legacy protocols or lower-level layer 2 protocols.
- *IPsec VPN*—Provides a highly available remote access gateway for branch and remote offices, and can be extended with antivirus, antispam, and web filtering.

Anti-Evasion Capabilities

As part of the solution, McAfee provides the industry's most advanced anti-evasion capabilities to protect against today's advanced threats. Network-based evasion techniques are used—often in combination and with multiple exploits—to bypass most current security detection devices. They help well-resourced, motivated attackers implement advanced persistent threats (APTs).

McAfee offers unique and thorough protection against the most determined attacks across all protocols and network layers. This NGFW has been successfully tested against more than 800 million AETs. Advanced anti-evasion techniques decode and normalize traffic for inspection on all protocol layers:

- Normalization removes evasions before data stream inspection.
- Vulnerability-centric fingerprints detect exploits in the normalized data streams.

Scale Protection with Business

Businesses today require full resiliency in their network security solution. To fulfill business continuity, McAfee Next Generation Firewall provides active clustering of up to 16 nodes, providing great flexibility in situations where processing-intensive security applications such as deep inspection or VPNs require more performance and protection.

Transparent session failovers and support for multiple software versions within the same cluster provide industry-leading system availability and serviceability without disruption. McAfee Multi-Link extends high availability to cover network and IPsec VPN connections. You get the confidence of military-grade security for every deployment.

Virtualize the Same Strong Security

Accredited as a VMware-ready virtual appliance, this solution is easy to deploy in your virtual infrastructure as a virtual appliance or virtual context. Each virtual appliance can run independently, even running its own software version and operating system. Yet virtual appliances are managed in the same way and with the same functionality as a physical appliance.

Virtual context capability allows a physical appliance to support many instances of the NGFW, reducing costs and increasing operational efficiencies. This multitenant capability offers a way to logically separate up to 250 security gateway configurations into separately manageable instances. This capability enables businesses such as Managed Security Services Providers (MSSPs) to offer and manage services for multiple customers using the same physical elements.

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 virtualization platforms
Supported Roles	Firewall/VPN (layer 3), IPS mode (layer 2), layer 2 firewall
Virtual Context	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
VPN	
Protocols	IKEv1, IKEv2, and IPsec with IPv4 and IPv6v6
Encryption	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES*
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

McAfee Next Generation Firewall Specifications (continued)

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
Routing	Static IPv4 and IPv6 routes, policy-based routing, static multicast routing
Dynamic Routing	IGMP proxy, RIPv2, OSPFv2, single firewalls 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)
Antivirus (Subscription Required)	
Scanned protocols	HTTP, HTTPS, POP3, IMAP, SMTP
McAfee AntiVirus	File-based, local signature database, automatic real-time updates
Antispam (Subscription Required)	
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)
General Functionality (All Roles)	
Encapsulation	Ethernet, 802.1q VLAN, PPPoA**, PPPoE**
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
Dynamic Context Detection	Protocol, application, file type (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, text file, binary file)

McAfee Next Generation Firewall Specifications (continued)

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 Security Management Center (SMC) • Current coverage of approximately 4000 protected vulnerabilities
URL Filtering (Subscription Required)	
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
Platform Certifications	
VPN Consortium	VPNC interoperability certified: basic, AES, certification, IKEv2, and IPv6
ICSA Labs	Network IPS, Network Firewall, IPv6, High Availability, USGv6
VMware	Virtual appliance VMware-ready certified
RSA	Secured by RSA, certified with RSA SecureID and RSA enVision
Arcsight	Common event log format (CEF) certified
Q1Labs	Log event enhanced format (LEEF) certified
Microsoft	IPSec VPN client certified for Windows Vista, compatible with Windows 7

* Supported encryption algorithms depend on license used.
** Firewall/VPN role only.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

61001ds_ngfw_0314_fnl_ETMG