

McAfee Firewall Enterprise

Army Information Assurance Approved Products List (IA APL) Solutions



McAfee Firewall Enterprise Security Features

Firewall

- Packet, stateful, and full application filtering
- Multiple delivery options, including multifirewall appliances (one appliance managing up to 32 virtual firewalls) and a virtual firewall appliance
- Network address translation (NAT)

Authentication

- Local
- Microsoft Active Directory
- LDAP (iPlanet, Open LDAP, Custom LDAP)
- RADIUS
- Microsoft Windows Domain Authentication
- Microsoft Windows NTLM Authentication
- Passport (single sign-on)
- Strong authentication (SafeWord, SecurID)

High availability (HA)

- Active/active
- Active/passive
- Stateful session failover
- Remote IP monitoring

Global Threat Intelligence

- TrustedSource global reputation service
- Geo-location filtering

Encrypted application filtering

- SSH
- SFTP
- SCP
- SSL/HTTPS*

* These services are purchased separately.

Today's Firewall Challenges Mandate a New Paradigm of Protection

Firewalls are a company's first line of defense against security threats and critical to every organization's network protection strategy. But threats to the enterprise are becoming more dangerous and unpredictable every day, with new application-layer attacks, Web 2.0 vulnerabilities, and signature-evading malware. Security incidents are on the rise—due in large part to archaic firewall protection technologies that cannot defend against these new threat vectors. At the same time, firewall administrators struggle to manage and troubleshoot numerous legacy firewall policies as administration costs continue to rise.

Exploding cost of management

Managing multiple aging firewalls is a time- and resource-intensive task, to say the least. Uncoordinated changes to applications and networks cause outages that often take hours or even days to troubleshoot. Administrators lack visibility into user behavior and struggle to efficiently respond to changing business needs. This is to say nothing of more frequent mandates to demonstrate compliance with audit and regulatory requirements—another tedious task that is made more costly and laborious if you lack useful reporting tools.

To proactively defend against the ever-changing threat landscape, you need to simply and confidently implement the firewall changes your business requires. In other words, you need a new firewall solution—McAfee® Firewall Enterprise.

Archaic protection technology fails against latest threats

The old technology of rules and signatures is no longer enough. New threats are combining into blended attacks that simultaneously exploit a variety of vulnerabilities. Worse yet, they're coming from both outside and inside the network and even through encrypted protocols. Keeping this threat environment at bay has never been more challenging, as networks and connectivity keep growing and threats evolve at rapid-fire speed. Without visibility into emerging threats, administrators spend too much time and effort just trying to keep up.

McAfee Firewall Enterprise Overview

With McAfee Firewall Enterprise and its related products, administrators can immediately begin to put firewall rules in the proper business context and take advantage of centralized firewall management, reporting, and user-friendly rule creation capabilities. Additionally, Firewall Enterprise offers unprecedented levels of threat protection. Advanced capabilities such as reputation-based global threat intelligence, configurable application-level protection, encrypted traffic inspection, anti-virus, content filtering, and intrusion prevention systems (IPS) block attacks before they occur.

Streamline Firewall Management and Regulatory Compliance While Improving the Agility of Your Business

McAfee Firewall Profiler, a separate appliance in the McAfee Firewall Enterprise line up, specifically targets some of the most time-consuming tasks in current firewall administration—investigating and resolving firewall outages. By pinpointing in real time how firewall rules correlate to business users and

McAfee Firewall Enterprise Security Features Continued

Intrusion prevention system (IPS)

- More than 10,000 signatures
- Automatic signature updates
- Custom signatures
- Preconfigured signature groups

Anti-virus and anti-spyware

- Protects against spyware, Trojans, and worms
- Heuristics
- Automatic signature updates

Web filtering

- McAfee SmartFilter®
- Block Java, Active-X, JavaScript, SOAP

Anti-spam

- TrustedSource global reputation service

SVPN

- ICSA IPsec certified
- IKEv1 and IKEv2
- DES, 3DES, AES-128, and AES-256 encryption
- SHA-1 and MD5 authentication
- Diffie-Hellmann groups 1, 2, and 5
- Policy-restricted tunnels
- NAT-T
- Xauth

Application visibility and control

- VoIP (SIP)
- SQL (Oracle, MS-SQL)
- Multimedia (H.323)
- SSH
- SMTP
- Citrix
- FTP
- HTTP
- HTTPS*
- IM/P2P
- Others

McAfee SecureOS® operating system

- McAfee Type Enforcement® technology
- Preconfigured operating system (OS) security policy
- OS compartmentalization
- Network stack separation

applications, Firewall Profiler enables administrators to see the impact of creating or changing a specific firewall rule set. Hours and days of rule creation and troubleshooting work become a mere matter of clicks. As a result, operational costs decrease and firewall administrators can implement new applications faster and respond more quickly to business needs.

McAfee Firewall Enterprise administrative console simplifies policy creation

Reliable security must also be easy to configure. Firewall Enterprise's administrative console is a user-friendly interface that lets your administrators create rules and selectively apply defenses such as application filters, IPS signatures, and URL filtering from a single screen. New software feature updates are delivered automatically via the Internet, reducing maintenance effort. Simply determine the schedule with a single mouse click. Additionally, Firewall Enterprise has an unequalled U.S. Computer Emergency Readiness Team (CERT) advisory record. You are never interrupted by emergency security patches, and your staff can stay focused on more strategic projects.

The McAfee Firewall Enterprise product line includes additional tools for simplifying management: McAfee Firewall Reporter and McAfee Firewall Enterprise Control Center.

McAfee Firewall Reporter

Included at no additional cost, Firewall Reporter turns audit streams into actionable information. This award-winning security event management (SEM) tool delivers central monitoring and correlated alerting and reporting. Easily generate more than 800 graphical reports to depict network traffic and help meet all major regulatory requirements, including:

- Sarbanes-Oxley (SOX)
- Payment Card Industry Security Standards (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

McAfee Firewall Enterprise Control Center

Sold separately, Firewall Enterprise Control Center offers centralized firewall policy management for multiple Firewall Enterprise appliances. Maximize operational efficiency, simplify policy control, optimize rules, streamline software updates, and demonstrate regulatory compliance. You can even compare policy configurations on all of your Control Center-managed devices to ensure consistency across your network. Robust configuration management features let you centrally track, trace, and validate all policy changes. Furthermore, Control Center now integrates with the McAfee ePolicy Orchestrator® (ePO™) management console, providing McAfee ePO™ software with visibility to firewall health data and reports.

Gain Real-Time Global Threat Visibility While Eliminating Unwanted Traffic

Firewall Enterprise virtually eliminates exposure to unknown attackers thanks, in part, to two exclusive technologies: McAfee TrustedSource™, the industry's first global reputation system for Internet senders, and geo-location filtering, which provides geographic visibility and policy management based on the traffic's country of origin.

Global Threat Intelligence

McAfee TrustedSource has set a new standard for proactive detection. Backed by McAfee Labs™, the world's most comprehensive threat research organization, this in-the-cloud service dissects traffic not against signatures but on the historical behavior of Internet-based hosts and devices. TrustedSource rejects connections with known bad senders, infected web pages, blended threats, and hosts that have been turned into malware-distributing zombies, effectively blocking these attacks at your perimeter.

By blocking these attacks, TrustedSource also blocks over 70 percent of unwanted traffic at the network edge. This reduces traffic volume on downstream network servers, saving you bandwidth and processing time.



The McAfee SecureOS Operating System Delivers the Most Hardened Appliance

At its core, McAfee Firewall Enterprise runs on the high-speed, high-assurance McAfee SecureOS operating system with patented McAfee Type Enforcement technology that enables an unparalleled level of platform security. SecureOS has an unmatched CERT advisory record and is deployed in the world's most demanding networks.

Management and administration options

- Windows graphical user interface
- Local console
- Full command line
- USB disaster recovery configuration backup and restore
- Rapid troubleshooting and firewall rule impact analysis with McAfee Firewall Profiler (sold separately)

Logging, monitoring, and reporting

- On-box logging
- Scheduled log archiving and exporting
- Firewall Enterprise log software Extract format (SEF)
- Export formats (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP v1, v2c, and v3
- McAfee Firewall Reporter SEM included

Networking and routing

- Dynamic routing (RIP v1 and v2, OSPF, BGP, and PIM-SM)
- Static routes
- 802.1Q VLAN tagging
- DHCP client
- Default route failover
- QoS

Secure servers

- Secure DNS (single or split)
- Secure sendmail (single or split)

Appliances and hardware

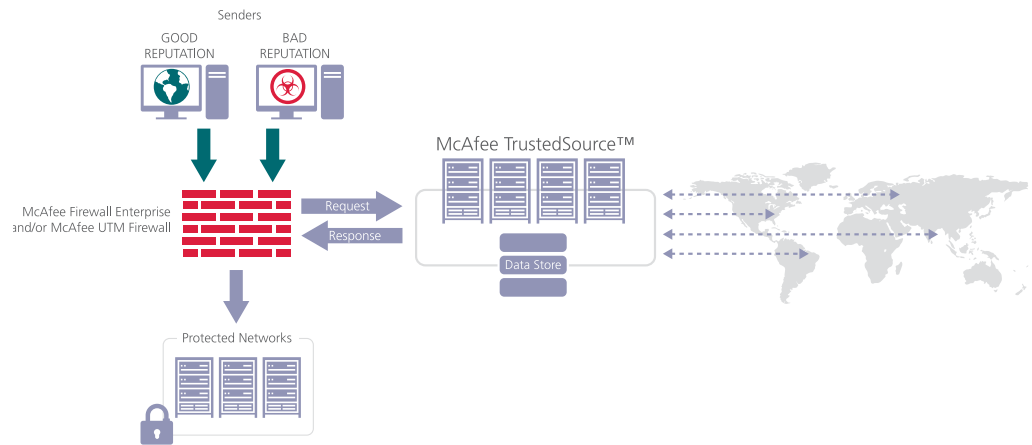
- Upgrade warranty to four-hour response for most models
- Virtualization solutions and rugged appliance options available
- Single-, dual-, and quad-core processors
- ASIC-based acceleration
- RAID HDD configurations
- Redundant power supplies

McAfee provides award-winning technical support

- 24/7 telephone-based technical support
- 24/7 technical support with web-based ticketing and knowledgebase

Geo-location

Firewall Enterprise's geo-location capability further limits global threats by allowing traffic filtering based on country code. Many organizations waste bandwidth and system resources on traffic from countries and entire continents that they don't even do business with—exposing themselves to unnecessary security risks in the process. Geo-location helps you connect only with the global traffic that's directly related to your business.



View and Control Your Applications

As cybercriminals become more organized and persistent, network security administrators need to be ever vigilant in protecting mission-critical networks, applications, and data. Applications, in particular, are a primary target of hackers—at least 80 percent of new attacks focus on application vulnerabilities. Legacy firewalls, or those that employ only stateful or deep inspection techniques, fall short of protecting your enterprise.

Firewall Enterprise includes stateful and deep inspection as part of its arsenal, but as a true application-layer firewall, Firewall Enterprise empowers you to add more advanced protection where and when you need it—without compromising performance.

Application-level controls are available for many of the most commonly used protocols, such as:

- Email (SMTP)
- Web (HTTP and HTTPS)
- Multimedia (H.323)
- Oracle and MS-SQL
- Citrix
- Voice over IP/Session Initiation Protocol (VoIP/SIP)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)

Meet PCI DSS requirements

The PCI DSS now requires companies that handle credit cards to deploy an application firewall. Firewall Enterprise helps you meet these requirements and proactively protect your customer account data.

Eliminate the Blind Spot of Encrypted Applications

Most organizations today encrypt some volume of Internet traffic—whether for communication with business partners or customers or for client-server system communications. While encryption provides valuable protection of data in transit, it can also present an opportunity for cybercriminals. Most legacy firewalls do not inspect encrypted traffic and therefore cannot screen against anti-malware or intrusion prevention signatures within such encrypted traffic. This offers hackers a wide-open tunnel to exploit your servers and applications.

Firewall Enterprise eliminates this vulnerability by decrypting, filtering, and controlling secure socket layer (SSL), secure FTP (SFTP), secure channel protocol (SCP), and secure socket layer (SSL)/HTTPS traffic. This eliminates surprise attacks on your web and application servers while still protecting the integrity and authenticity of encrypted messages.



McAfee Firewall Enterprises Product Line

The Firewall Enterprise product line includes appliances appropriate for businesses of all sizes, as well as companion products such as McAfee Firewall Profiler, McAfee Firewall Enterprise Control Center, and McAfee Firewall Reporter to streamline management activities and reduce operational costs. Ask for individual product datasheets for more information.

McAfee Firewall Enterprise IA APL-Approved Models



Hardware Specs

	1100e	2150e	4150e
Form factor	Enterprise 1U	Enterprise 2U	Enterprise 5U
Unlimited user licenses	Yes	Yes	Yes
Recommended users	Med-Large	Large	Enterprise
RAID	RAID 1	RAID 5	RAID 5
Power supply	Dual	Dual	Dual
Copper interfaces (base/max)	8/14 GB	8/20 GB	14/24 GB
Fiber interface option (max)	6	6	6
10 GB interface option (max)	N/A	2	2
SSL/HTTPS decrypting and filtering	Yes	Yes	Yes
Regulatory compliance	FCC (U.S. only) Class B, ICES (Canada) Class B, CE Mark (EN 55022 Class B, EN55024, EN61000-3-2, EN61000-3-3), VCC (Japan) Class B, BSMI (Taiwan) Class A, C-Tick (Australia/New Zealand) Class B, SABS (South Africa) Class B, CCC (China) Class B, MIC (Korea) Class B, UL 60950, CAN/CSA C22.2 No. 60950, IEC 60950		
Certifications	ICSA Labs IPsec VPN, Common Criteria EAL4+ with Application Protection Profile (the only firewall to have this level of EAL4+ certification), FIPS 140-2, Level 2		

Performance

Packet filtering throughput (TCP)	1.9 Gb/s	3.1 Gb/s	3.8 Gb/s
Stateful throughput	1.8 Gb/s	2.9 Gb/s	3.6 Gb/s
Concurrent connections	1,000,000	1,600,000	2,000,000
Application filtering throughput	1.4 Gb/s	2.2 Gb/s	2.7 Gb/s
IPsec VPN throughput	240 Mb/s	350 Mb/s	400 Mb/s

Dimensions, weight, environmental

Width	16.7 in 42.6 cm	17.5 in 44.43 cm	17.43 in 44.27 cm
Depth	30.4 in 77.2 cm	29.31 in 74.4 cm	26.55 in 67.43 cm
Height	1.67 in 4.26 cm	3.4 in 8.64 cm	8.56 in 21.77 cm
Weight	35.8 lbs 16.3 kg	57 lbs 28.85 kg	100 lbs 45.36 kg
Power supply details	Dual 670 W 110/220 V	Dual 750 W 110/220 V	Dual 930 W 110/220 V
Operating temperature	10° C – 35° C 50° F – 95° F	10° C – 35° C 50° F – 95° F	10° C – 35° C 50° F – 95° F

