McAfee Network Security Platform

Optimize network protection with next-generation intrusion prevention

McAfee, the global leader in network intrusion prevention systems (IPS) delivers unprecedented levels of security while offering flexible deployment options that help you optimize network investments. Only McAfee® Network Security Platform provides category-best security effectiveness, scalable in-line performance, and next generation IPS controls that take the guesswork out of security management. Unify network security management across physical and virtual environments, streamline security operations, and protect your business from the latest malware, zero-day attacks, botnets, denial-of-service (DoS) attempts and advanced targeted attacks.

Key Advantages

Fast, accurate threat prevention
- Stateful traffic inspection
- Predictive threat intelligence via McAfee GTI
- Malware, zero-day, DoS/DDoS, botnets

Performance and availability
- Over 10 Gbps throughput
- Industry-leading reliability
- Fail-over and fail-open

Network-wide visibility
- Next-generation application visibility
- Behavior-based bot detection
- Flow-based network behavior analysis

Centralized security management
- Scalable network security management
- McAfee ePO software integration
- Host IPS/virus/spyware event visibility

Operational simplicity
- Dynamic smart blocking
- Multithreat correlation
- Integrated vulnerability scanning

Inspection of virtual environments
- Inspect inter-VM traffic
- Quarantine malicious VMs
- One console for physical and virtual

Industry-Leading Protection

Let McAfee do the heavy lifting when it comes to network security. McAfee Network Security Platform boasts better out-of-the-box security effectiveness than most network IPS solutions achieve after significant tuning. With tens of thousands of sensors deployed worldwide, McAfee Network Security Platform is the industry's most proven Network IPS. Its provides coverage against malware, zero-day threats, denial-of-service attacks, and botnets.

Multigigabit performance

Get the best of both worlds—security and high performance. McAfee Network Security Platform combines a single-pass, protocol-based inspection architecture with purpose-built, carrier-class hardware to achieve real-world inspection of more than 10 Gbps in a single device. Its ultra-efficient architecture preserves performance regardless of security settings, while other IPS solutions can experience up to 50 percent reduction in throughput with "security over performance" policies.

Predictive threat intelligence

Dramatically improve your security effectiveness with predictive threat intelligence. McAfee Network Security Platform incorporates McAfee Global Threat Intelligence™ (McAfee GTI™) to dynamically affect in-line prevention of traditional and emerging attacks. McAfee GTI assesses the reputation of network communications based on the reputation of billions of unique file, IP, URL, protocol, and geo-location data from around the globe.

Application awareness and control

Make informed decisions about the applications and protocols on your network. McAfee Network Security Platform is the first and only IPS solution to combine advanced threat prevention and application awareness into a single security decision engine. We correlate threat activity with application usage, including layer 7 visibility of more than 1,100 applications and protocols, to allow you to make more informed decisions about which applications you allow on your network.

Unmatched network visibility

See further into your network than ever before. Get a clear understanding of system, application, and user behavior with network anomaly detection. McAfee Network Security Platform dramatically expands the purview of traditional network IPS to easily identify bots and other malicious activity throughout the network by analyzing flow data from switches and routers anywhere in the enterprise.

Context-aware security

Get aggressive with network security without increasing the risk of false positives. McAfee correlates data across several sources—McAfee GTI, vulnerability scans, application behavior, and system

McAfee Network Security Platform helps you:

Protect your business
- Prevent attacks while reducing downtime
- Protect your data and infrastructure
- Meet compliance initiatives

Protect your systems
- Proactive protection for unpatched systems
- Proactive protection for zero-day attacks
- Context-aware intrusion prevention

Protect your network
- Application visibility and control
- Adaptive rate limiting
- Host-specific connection limiting

Protect your security investment
- Native 10-gigabit Ethernet
- Network-grade hardware
- Industry-leading useful life

behavior—to confidently identify network attacks and, in many cases, automatically prevent malicious activity. For example, a low confidence "alert-only" event can be dynamically upgraded to a high-confidence "block" event based on real-time correlation of a signature-based attack definition and the reputation of the threat's source IP.

Built-in access control

Add optional network access control (NAC) software, and turn McAfee Network Security Platform into a NAC device that offers both pre- and post-admission control and identity based-access control, along with host quarantine and enforceable access policies.

Integrated security management

Make the most of your security investment through integrated security and risk management. Network Security Platform integrates with McAfee® ePolicy Orchestrator® (McAfee ePO™) software to give your organization a consolidated view of risk and compliance across the entire enterprise, including up-to-the-minute assessments of at-risk infrastructure based on system vulnerabilities, network defenses, and endpoint security levels.

The following capabilities are offered on all McAfee Network Security Platform appliances:

Advanced intrusion prevention

- Stateful traffic inspection (IP defragmentation and TCP stream reassembly)
- Anomaly detection
- Signature-based detection (McAfee-defined, user-defined, open source)
- Reputation-based detection (McAfee GTI)
- Heuristic bot detection
- Multi-attack correlation
- Layer 7 protocol detection
- Host quarantine
- Advanced evasion protection

Denial-of-service (DoS) and distributed denial-of-service (DDoS) prevention

- Threshold and heuristic-based detection
- Connection limiting
- Self-learning profile-based detection

Network visibility

- Application visibility
- System information
- Vulnerability correlation
- Host IPS alerts
- Inspection of virtual environments
- Packet capture for forensics analysis integration
- Flow-based behavior analysis (via NTBA)

Granular control

- Application and sub-application control
- Geo-location based ACL rules
- Connection limiting
- Host quarantine (via IPS or NAC)
- Identity-based access control
- System health-based access control

McAfee GTI

- File reputation
- IP reputation
- Application and protocol reputation
- Geo-location

High availability options

- Complete stateful fail-over
- External fail-open (active and passive)
- Built-in fail-open (for copper ports only)

Protocol Tunneling Support

- IPv6
- V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels
- MPLS
- GRE
- Q-in-Q Double VLAN

McAfee Network Security Manager

- Always-on management
- Dozens of predefined IPS security policy templates
- Up to 1,000 "virtual IPS" policies (on specified models)
- Integrated user authentication (Radius, LDAP, and TACACS)
- Automated failover and fail-back
- Disaster recovery of critical configuration data
- Hierarchical management for centralized policy control

Integrated Solutions

- McAfee ePolicy Orchestrator software
- McAfee Network Threat Behavior Analysis
- McAfee Network Access Control (software add-on)
- McAfee Network Threat Response
- McAfee Vulnerability Manager
- Third-party forensics

McAfee

Network Security Platform Specifications

	10 Gigabit Ethernet Connectivity							
								
Sensor Hardware Components	**M-8000**	**M-6050**	**M-4050**	**M-3050**	**M-2950**	**M-2850/M-2750**	**M-1450**	**M-1250**
Performance								
Real-World Throughput	10 Gbps	5 Gbps	3 Gbps	1.5 Gbps	1.0Gbps	600 Mbps	200 Mbps	100 Mbps
Max Throughput (UDP 1512 Byte Packets)	Up to 20 Gbps	Up to 10 Gbps	Up to 4 Gbps	Up to 2.5 Gbps	Up to 1 Gbps	Up to 1 Gbps	Up to 300 Mbps	Up to 150 Mbps
Maximum Concurrent Connections	4,000,000	2,000,000	1,500,000	750,000	750,000	750,000 / 250,000	80,000	40,000
New Connections per Second	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000
Throughput with SSL Decryption (based on 10% SSL traffic)	8.8 Gbps	4.4 Gbps	2.7 Gbps	1.3 Gbps	900 Mbps	550 Mbps	N/A	N/A
Maximum SSL Flow Count	400,000	200,000	150,000	75,000	25,000	25,000	N/A	N/A
SSL Keys Imported	64	64	64	64	64	64	N/A	N/A
Profiles								
Number of Virtual IPS Systems	1,000	1,000	1,000	1,000	100	100	32	16
Maximum DoS Profiles	5,000	5,000	5,000	5,000	5,000	300	120	100
ACL Rules	1,000	1,000	1,000	1,000	1,000	400	100	50
Ports								
Gigabit Ethernet—Fixed Copper Ports	—	—	—	—	8	8 / –	8	8
Gigabit Ethernet—SFP Ports	16	8	8	8	12	12 / 20	—	—
10-Gigabit Ethernet	12	8	4	4	—	—	—	—
Dedicated Response Ports (GigE)	1	1	1	1	1	1	1	1
Dedicated Management Ports (GigE)	1	1	1	1	1	1	1	1
Ports with Built-in Fail-Open Capabilities	—	—	—	—	8	8 / –	8	8
Control Ports for External Fail-Open k=Kits	14	8	6	6	6	6 / 10	—	—
Physical								
Dimensions	2x 2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D) each	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 15.88(W) x 3.3(H) x 24.5(D)	2RU Rack mountable 15.88(W) x 3.3(H) x 24.5(D)	1RU Rack mountable 17.37 (W) x 1.65(H) x 13.5 (D)	1RU Rack mountable 17.37 (W) x 1.65(H) x 13.5(D)
Weight	94 lbs. (2x47)	47 lbs.	47 lbs.	47 lbs.	40 lbs.	40 lbs.	12 lbs.	12 lbs.
Power consumption	900w (2x450w)	450w	450w	450w	450w	450w	120w	120w
DC power available	Optional	Optional	Optional	Optional	Optional	Optional	No	No
Power	100–240VAC (50/60Hz)							
Temperature	0° to 35° C (operating) –40° to 70° C (non-operating)				0° to 40° C (operating) –40° to 70° C (non-operating)			
Relative humidity (non-condensing)	Operational: 10% to 90% Non-operational: 5% to 95%							
Altitude	0 to 10,000 feet							
Safety certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040 CB license and report covering all national country deviations.							
EMI certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)							

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

37801ds_nsp_1011_fnl_ETMG