McAfee Network Security Platform

A uniquely intelligent approach to network security

Key Advantages

Unparalleled Advanced Threat prevention

- Signature-less, advanced malware analysis.
- Inline Browser and JavaScript emulation.
- Advanced botnet and malware callback detection.
- Behavior-based analysis and DDoS protection.
- Outbound SSL Decryption.
- Integration with McAfee Advanced Threat Defense and McAfee Cloud Threat Detection.

Unified Defense Architecture

- Real-time threat sharing with McAfee Threat Intelligence Exchange (TIE).
- Endpoint context via ePolicy Orchestrator® (McAfee ePO™).
- Endpoint process correlation via Endpoint Intelligence Agent.
- Data Sharing and Quarantine with McAfee Enterprise Security Manager (SIEM).
- Host Risk Analysis via McAfee Vulnerability Manager.
- Predictive malware detection via McAfee GTI.

McAfee® Network Security Platform is a uniquely intelligent security solution that discovers and blocks sophisticated threats in the network. Using advanced detection and emulation techniques, it moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy. This next-generation hardware platform scales to speeds of more than 40 Gbps with a single device to meet the needs of demanding networks. Our Unified Defense Architecture approach to security management streamlines security operations by combining real-time McAfee Global Threat Intelligence (McAfee GTI) feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.

Protection Against Today's Stealthy Threats

Your network faces advanced, stealthy attacks that can evade traditional detection methods, leaving your network exposed to crippling breaches and downtime. Unfortunately, most organizations lack the financial and operational resources to implement and manage the combination of tools and technologies required to provide adequate defense.

McAfee Network Security Platform is an integrated network security platform that combines intelligent threat prevention with intuitive security management to improve detection accuracy and streamline security operations. It provides industry-leading coverage against advanced threats, malware callbacks, zero-day threats, and denial-of-service attacks. Built from the ground up for integration with McAfee's Unified Defense Architecture, McAfee's Network Security Platform leverages security data from across the organization and help plug the security gaps often missed by other pieced-together security solutions.

Unparalleled threat prevention

McAfee Network Security Platform is based on a next-generation inspection architecture designed to perform deep inspection of network traffic while maintaining line-rate speeds. It uses a combination of advanced inspection technologies—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis to detect and prevent both known and zero-day attacks on the network.

intel Security

Key Advantages continued

Performance and availability

- Next Generation Architecture.
- Up to 40 Gbps throughput.
- Unrivaled SSL inspection performance.
- Industry-leading reliability.
- Active-active and active-passive availability.

Intelligent security management

- Intelligent alert correlation and prioritization.
- Robust malware investigation dashboards.
- Preconfigured investigation workflows.
- Scalable web-based management.

Visibility and control

- Application identification.
- User identification.
- Device identification.

Comprehensive malware defense

No single malware detection technology can prevent all attacks, which is why McAfee Network Security Platform layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc on your network. It combines file reputation from McAfee GTI, deep file analysis with JavaScript inspection, and an advanced anti-malware engine to detect custom malware and other stealthy attacks.

Unified Defense Architecture

Getting your hands on the data you need has never been easier. McAfee offers real-time integration with McAfee ePO software and McAfee Enterprise Security Manager for real-time correlation of network events across all relevant sources. Through integration with McAfee ePO software and McAfee Enterprise Security Manager, McAfee Network Security Platform gets an accurate view of threats as they relate to devices and users and which ones present the greatest risk to the organization. The solution incorporates device details, user information, endpoint security posture, vulnerability assessments, and other rich information to help organizations understand threat severity and business risk factors.

Performance and scalability

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 40 Gbps in a single device. Its ultra-efficient architecture preserves performance regardless of security settings, while other intrusion prevention system (IPS) solutions can experience up to 50% reduction in throughput with security-over-performance policies.

Visibility 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 1,500 applications and protocols, to allow you to make more informed decisions about which applications you allow on your network. In addition to application identification, McAfee Network Security Platform provides user and device visibility. It prioritizes risky hosts and users, including active botnets, through the identification of anomalous network behavior.

Intelligent security management

Make the most of your security investment through intelligent network security management. McAfee Network Security Manager offers scalable web-based management from two to several hundred network security appliances. It offers intuitive progressive disclosure workflows that guide administrators to relevant alerts as well as easy-to-use security dashboards that automatically prioritize events based on alert severity and relevancy. McAfee Network Security Platform integrates with 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.

McAfee Network Security Platform Helps You:

Close security holes.

- Block malicious network activity.
- Prevent stealthy attacks.
- Detect advanced malware.

Reduce management headache.

- Automatically prioritize events.
- Streamline investigative workflows.
- Eliminate unnecessary tuning.

Adapt to the network.

- 1 GigE, 10 GigE, 40 GigE connectivity.
- Scale to 40 Gbps.
- Active-active and active-passive availability.

Additional Features

Advanced threat prevention

- McAfee Gateway Anti Malware (GAM) Emulation engine.
- PDF Javascript emulation engine.
- Adobe Flash behavioral analysis engine.
- Advanced evasion protection.
- Mobile threat reputation and cloud analysis.
- Outbound SSL decryption (NS-series).

Botnet and malware callback protection

- DNS/DGA Fast flux callback detection.
- DNS Sinkholing.
- Heuristic bot detection.
- Multiple attack correlation.
- Command and control database.

Advanced intrusion prevention

- IP defragmentation and TCP stream reassembly.
- McAfee, user-defined, and open-source signatures.
- Host quarantine and rate limiting.
- Inspection of virtual environments.
- Integration with McAfee Advanced Threat Defense.

DoS and DDoS prevention

- Threshold and heuristic-based detection.
- Host-based connection limiting.
- Self-learning, profile-based detection.

McAfee GTI

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

High availability

- Active-active and active-passive with stateful failover.
- External fail-open (active).
- Built-in fail-open.

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

- Tiered management (up to 1,000 sensors).
- User authentication (Radius and LDAP).
- Automated failover and fail-back.
- Disaster recovery of critical configuration data.
- Centralized, hierarchical policy management.
- Ability to connect with McAfee Integration with McAfee Cloud Threat Detection to submit unknown files.
- Memory dashboard detailing memory utilization by device.

Network Security Platform Specifications

	Next Generation Hardware		
			
Sensor Hardware Components	**NS9300**	**NS9200**	**NS9100**
Performance			
Aggregate Performance	40 Gbps	20 Gbps	10 Gbps
Maximum Throughput (UDP 1512 Byte Packets)	Up to 70 Gbps	Up to 35 Gbps	Up to 30 Gbps
Maximum Concurrent Connections	32,000,000	16,000,000	13,000,000
Connections per Second	1,000,000	575,000	450,000
HTTP Connections per Second	750,000	375,000	260,000
Throughput with SSL Decryption (based on 10% SSL traffic)	40 Gbps	20 Gbps	10 Gbps
Maximum SSL Flow Count	3,200,000	1,600,000	1,200,000
SSL Keys Imported	1,024	1,024	1,024
Typical Latency	Less than 100 µs	Less than 100 µs	Less than 100 µs
Number of Virtual IPS Systems	1,000	1,000	1,000
Maximum DoS Profiles	5,000	5,000	5,000
ACL Rules	20,000	20,000	20,000
Ports			
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	16	8	8
Fixed 10 GigE/1 GigE (SFP+) Ports	—	—	—
Fixed 40-Gigabit Ethernet	—	2	2
Network I/O Slots	4	2	2
Network I/O Modules (eight options)	4-port 10 GigE/1 GigE SR Optical 50 micron with fail open, 4-port 10 GigE/1 GigE SR Optical 62.5 micron with fail open, 4-port (QSFP+) 40 GigE, 2-port (QSFP+) 40 GigE, 8-port (SFP+/SFP) 10 GigE/1 GigE, 6-port (RJ45) 1 GigE (with internal fail-open), 4-port (RJ45) 10 GigE/1 GigE (with internal fail-open), or 4-port 10 GigE/1 GigE LR Optical with fail open	4-port 10 GigE/1 GigE SR Optical 50 micron with fail open, 4-port 10 GigE/1 GigE SR Optical 62.5 micron with fail open, 4-port (QSFP+) 40 GigE, 2-port (QSFP+) 40 GigE, 8-port (SFP+/SFP) 10 GigE/1 GigE, or 6-port (RJ45) 1 GigE (with internal fail-open)	4-port 10 GigE/1 GigE SR Optical 50 micron with fail open, 4-port 10 GigE/1 GigE SR Optical 62.5 micron with fail open, 4-port (QSFP+) 40 GigE, 2-port (QSFP+) 40 GigE, 8-port (SFP+/SFP) 10 GigE/1 GigE, or 6-port (RJ45) 1 GigE (with internal fail-open)
10 Gigabit Ethernet	Up to 32	Up to 16	Up to 16
40-Gigabit Ethernet	Up to 16	Up to 10	Up to 10
Dedicated Response Ports (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Dedicated Management Ports (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Dedicated Storage Ports (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Physical			
Dimensions	2 x 2RU Rack Mountable 17.24" (W) x 6.88" (H) x 28.76" (D)	2RU Rack Mountable 17.24" (W) x 3.44" (H) x 28.76" (D)	2RU Rack Mountable 17.24" (W) x 3.44" (H) x 28.76" (D)
Weight	134 lbs.	67 lbs.	67 lbs.
Storage	600 GB (2 x Dual Solid State 300 GB in RAID 1 configuration)	Dual Solid State 300 GB in RAID 1 configuration	Dual Solid State 300 GB in RAID 1 configuration
Maximum Power Consumption	2260w	1130w	1130w
DC Power Available	Optional	Optional	Optional
Redundant Power Supply	Included	Included	Optional
Power	100-240 VAC (50 / 60Hz)		
Temperature	0° to 35° 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, 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)		

Network Security Platform Specifications continued



Sensor Hardware Components	NS7300	NS7200	NS7100
Performance			
Aggregate Performance	5 Gbps	3 Gbps	1.5 Gbps
Maximum Throughput (UDP 1512 byte packets)	Up to 15 Gbps	Up to 10 Gbps	Up to 5 Gbps
Maximum Concurrent Connections	10,000,000	5,000,000	3,000,000
Connections per Second	225,000	200,000	135,000
HTTP Connections per Second	135,000	128,000	115,000
Throughput with SSL Decryption (based on 10% SSL traffic)	5 Gbps	3 Gbps	1.5 Gbps
Maximum SSL Flow Count	500,000	400,000	250,000
SSL Keys Imported	1,024	1,024	1,024
Typical Latency	Less than 100 µs	Less than 100 µs	Less than 100 µs
Number of Virtual IPS Systems	1,000	1,000	1,000
Maximum DoS Profiles	5,000	5,000	5,000
ACL Rules	5,000	3,000	3,000
Ports			
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	8	8	8
Fixed 10 GigE/1 GigE (SFP+) Ports (external passive fail-open kit support)	2	2	2
Fixed 40-Gigabit Ethernet	—	—	—
Network I/O Slots	2	2	2
Network I/O Modules (six options)	4-port 10 GigE/1 GigE SR Optical 50 micron with fail open, 4-port 10 GigE/1 GigE SR Optical 62.5 micron with fail open, 4-port 10 GigE/1 GigE LR Optical with fail open, 8-port (SFP+/SFP) 10 GigE/1 GigE, 6-port (RJ45) 1 GigE with internal fail open, or 4-port (RJ45) 10 GigE/1 GigE (with internal fail-open)		
10 Gigabit Ethernet	Up to 18	Up to 18	Up to 18
40-Gigabit Ethernet	—	—	—
Dedicated Response Ports (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Dedicated Management Ports (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Dedicated Storage Ports (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Physical			
Dimensions	1RU Rack Mountable 17.5" (W) x 1.69" (H) x 28.9" (D)	1RU Rack Mountable 17.5" (W) x 1.69" (H) x 28.9" (D)	1RU Rack Mountable 17.5" (W) x 1.69" (H) x 28.9" (D)
Weight	31 lbs.	31 lbs.	29 lbs.
Storage	Solid State 160 GB	Solid State 160 GB	Solid State 160 GB
Maximum Power Consumption	350W	350W	250W
DC Power Available	Optional	Optional	Optional
Redundant Power Supply	Optional	Optional	Optional
Power	100-240 VAC (50 / 60Hz)		
Temperature	0° to 35° 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, 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)		

Network Security Platform Specifications continued

Sensor Hardware Components	NS5200	NS5100
Performance		
Aggregate Performance	1 Gbps	600 Mbps
Maximum Throughput (UDP 1512 byte packets)	Up to 3 Gbps	Up to 1.5 Gbps
Maximum Concurrent Connections	1,350,000	750,000
Connections per Second	45,000	40,000
HTTP Connections per Second	30,000	25,000
Throughput with SSL Decryption (based on 10% SSL traffic)	1 Gbps	600 Mbps
Maximum SSL Flow Count	75,000	40,000
SSL Keys Imported	1,024	1,024
Typical Latency	Less than 100 µs	Less than 100 µs
Number of Virtual IPS Systems	1,000	100
Maximum DoS Profiles	5,000	300
ACL Rules	2,000	2,000
Ports		
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	8	8
Fixed 1 GigE (SFP) Ports	12	12
Fixed 10 GigE/1 GigE (SFP+) Ports (external passive fail-open kit support)	2	2
Fixed 40-Gigabit Ethernet	—	—
Network I/O Slots	—	—
Network I/O Modules	—	—
10 Gigabit Ethernet	—	—
40-Gigabit Ethernet	—	—
Dedicated Response Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Dedicated Management Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Dedicated Storage Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Physical		
Dimensions	1RU Rack Mountable 17.25" (W) x 1.75" (H) x 24.625" (D)	1RU Rack Mountable 17.25" (W) x 1.75" (H) x 24.625" (D)
Weight	22 lbs.	22 lbs.
Storage	Solid State 80 GB	Solid State 80 GB
Maximum Power Consumption	225W	225W
DC Power Available	Optional	Optional
Redundant Power Supply	Optional	Optional
Power	100-240 VAC (50 / 60Hz)	
Temperature	0° to 35° 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, 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)	

Network Security Platform Specifications continued

Sensor Hardware Components	NS3200	NS3100
Performance		
Aggregate Performance	200 Mbps	100 Mbps
Maximum Throughput (UDP 1512 byte packets)	up to 1 Gbps	up to 600 Mbps
Maximum Concurrent Connections	80,000	40,000
Connections per Second	20,000	15,000
HTTP Connections per Second	15,000	12,000
Throughput with SSL Decryption (based on 10% SSL traffic)	—	—
Maximum SSL Flow Count	—	—
SSL Keys Imported	—	—
Typical Latency	Less than 100 µs	Less than 100 µs
Number of Virtual IPS Systems	32	16
Maximum DoS Profiles	128	128
ACL Rules	1,000	1,000
Ports		
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	8	8
Fixed 1 GigE (SFP) Ports	—	—
Fixed 10 GigE/1 GigE (SFP+) Ports (external passive fail-open kit support)	—	—
Fixed 40-Gigabit Ethernet	—	—
Network I/O Slots	—	—
Network I/O Modules	—	—
10 Gigabit Ethernet	—	—
40-Gigabit Ethernet	—	—
Dedicated Response Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Dedicated Management Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Dedicated Storage Ports (RJ45)	1 (1G/100M)	1 (1G/100M)
Physical		
Dimensions	1RU Rack Mountable 17.375” (W) x 1.75” (H) x 11.0” (D)	1RU Rack Mountable 17.375” (W) x 1.75” (H) x 11.0” (D)
Weight	8.1 lbs.	8.1 lbs.
Storage	Solid State 30 GB	Solid State 30 GB
Maximum Power Consumption	100W	100W
DC Power Available	—	—
Redundant Power Supply	—	—
Power	100-240 VAC (50 / 60Hz)	
Temperature	0° to 35° 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, 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. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com