

## McAfee IntruShield Network IDS Sensor

McAfee® IntruShield™ network security products are built upon the industry's first architecture for real-time detection and prevention of network intrusions against enterprise and government networks. The innovative IntruShield architecture integrates patented signature, anomaly, and Denial of Service (DoS) analysis techniques, enabling accurate and intelligent attack detection and prevention at multi-gigabit speeds. This unprecedented harnessing of innovative technologies protects even the most demanding networks from the threat of known, first-strike (unknown), and DoS attacks.

The IntruShield product family includes the IntruShield 4000, IntruShield 2600, and IntruShield 1200—three powerful network intrusion detection and prevention sensor appliances that provide the performance and functionality required to protect high availability networks—and the IntruShield Security Management (ISM) system, a powerful, scalable security management solution.

The scalable IntruShield solution offers comprehensive protection spanning the enterprise core, the enterprise perimeter, and branch office networks. It delivers compelling price/performance for bandwidth needs ranging from a few tens of Mbps to two Gbps.

### At-a-Glance Features:

- **Intrusion Intelligence™:** Unprecedented capabilities provide detailed, accurate, and reliable information related to intrusion identification, relevancy, direction, impact, and analysis.
- **Virtual IDS:** Powerful capability to enforce multiple, highly granular, custom-intrusion policies within a single sensor.
- **Comprehensive Intrusion Detection:** Intelligent detection of known, first-strike, and DoS attacks using a combination of signature, anomaly, and DoS detection techniques.
- **Flexible Deployment:** Unprecedented flexibility of IDS deployment—including SPAN, tap, in-line, port clustering, and high availability modes—to suit any network security architecture.
- **Real-Time Intrusion Prevention:** Proactive capability to stop in-progress attacks coupled with a rich set of automated and user-initiated alerting and response actions.
- **Multi-Gigabit Performance:** Powered by purpose-built hardware that is capable of delivering multi-gigabit performance.
- **Automated Real-Time Threat Updates:** Innovative, automated process delivers real-time, enterprise-wide signature updates without requiring sensor reboots, and provides protection against newly discovered attacks while eliminating manual updates and sensor downtime.
- **Interoperability:** Works with leading firewalls, enterprise management applications, and Security Information Management (SIM) applications to offer reduced total cost of ownership.

### The IntruShield 4000

The IntruShield 4000 (I-4000) is suited for deployment at the core of the enterprise network or data centers. The I-4000's Gigabit Ethernet interfaces provide the performance and operational redundancy required to secure a high-availability network infrastructure.



- Four Gigabit Ethernet detection ports
- Two Fast Ethernet response ports
- One Fast Ethernet management port
- Optional redundant hot-swappable power supply
- Up to 2 Gbps performance

### The IntruShield 2600

The IntruShield 2600 (I-2600) offers a flexible IDS for enterprise perimeter deployment. Multiple Fast Ethernet and Gigabit Ethernet interfaces provide effective protection for multiple network segments.



- Two Gigabit Ethernet and six Fast Ethernet detection ports
- Built-in Fast Ethernet network taps
- Three Fast Ethernet response ports
- One Fast Ethernet management port
- Up to 600 Mbps performance

### The IntruShield 1200

The IntruShield 1200 (I-1200) offers a cost effective IDS deployment for mid-size or remote/branch office networks. Centralized Web-based management for enterprise-wide IDS deployment dramatically reduces operational costs.



- Two Fast Ethernet detection ports
- Built-in Fast Ethernet network taps
- One Fast Ethernet response port
- One Fast Ethernet management port
- Up to 100 Mbps performance

# McAfee IntruShield Network IDS Sensor

## Intrusion Intelligence

The IntruShield IDS introduces the industry's first Intrusion Intelligence capabilities. This unprecedented set of features delivers detailed, accurate, and reliable information related to intrusion identification, relevancy, direction, impact, and analysis. Intrusion Intelligence lays the foundation for enterprises to migrate from reactive intrusion detection to proactive intrusion prevention capabilities where attacks are stopped by intrusion prevention devices before they reach their intended targets.

Intrusion Intelligence consists of a unique collection of features to analyze key characteristics of an intrusion. The features include:

- **Intrusion Identification:** Identify a broad range of attacks with high confidence. Innovative features including Protocol Discovery and Protocol Tunneling to detect "hidden" attacks designed to evade an IDS.
- **Intelligent Alert Viewer:** Visual representation and analysis of intrusion events. User-selected, color-coded tracking of suspicious activity by attack, source or destination using innovative intrusion watch-lists. Powerful drill-down capabilities to pinpoint relevant events with just a couple of clicks.
- **Intrusion Direction:** Detection and granular prevention of both inbound and outbound attacks leveraging Policy by Traffic Direction. Accurate prevention of outbound attacks protects enterprises from unforeseen legal liabilities.
- **Intrusion Relevancy:** Granular security policy alerts and selectively blocks only relevant attacks, reducing false positives.
- **Intrusion Impact:** Unique Attack Verification feature determines if an attack was successful and assesses its impact by examining post-attack activities. Empowers security analysts to focus their time and resources on relevant events.

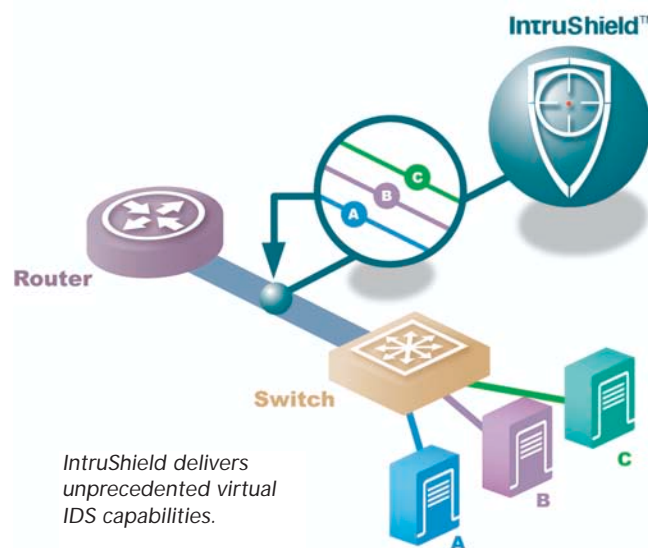
- **Intrusion Forensics:** Intelligent forensic analysis capabilities. Capture and analyze in-progress as well as post-attack activities by granular packet and session logging.
- **Intrusion Reporting:** Rich reporting offers macroscopic and detailed views of an enterprise's security posture. Formats include executive summary reports, detailed security incident reports, configuration reports and trend reports. Powerful and flexible User Defined Reports complement rich set of pre-defined reports. Reports can be generated on-demand or at a pre-determined schedule. Scheduled reports can be distributed automatically via e-mail.
- **Intrusion Incident Management:** Hundreds of IntruShield events related to a single intrusion collapsed into a single intrusion incident through powerful event correlation. Intuitive workflow capabilities to manage incidents among security analysts. Event correlation boosts alert and data management efficiencies by up to a hundred-fold.

## Virtual IDS

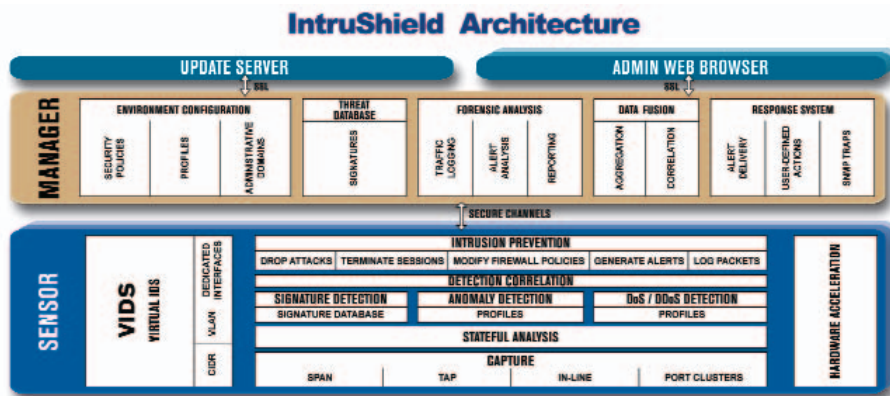
IntruShield sensors support the innovative and powerful concept of a Virtual IDS (VIDS™). Virtual IDS provides the capability to segment an IntruShield sensor into a large number of virtual sensors that can be completely customized with a granular security policy—including individualized attack selection and associated response actions. A VIDS can be defined based on a block of IP addresses, one or multiple VLAN tags, or by specific port(s) on a sensor.

This capability allows security professionals to implement and enforce a heterogeneous set of security policies with a single IntruShield sensor, thus better serving differing security needs within an organization. VIDS further reduces the total number of devices required for a network-wide IDS deployment and reduces total cost of ownership.

Virtual IDS also reduces the number of irrelevant alerts: if the user defines the target environment very specifically—applicable protocols, OS, applications of interest—then IntruShield raises only alerts relevant to the environment, thus reducing the number of false alarms to process.



# McAfee IntruShield Network IDS Sensor



## Comprehensive Intrusion Detection

No single technique or technology is a panacea, guaranteeing protection against all known, first-strike (unknown), and DoS attacks. To robustly protect against the complete spectrum of threats and vulnerabilities, IntruShield sensors tightly integrate signature and anomaly detection techniques and DoS detection—in a single purpose-built platform. Combining these three forms of protection significantly improves detection rates. Deep Packet Analysis, described earlier, significantly improves the quality of the data gathered, thus improving accuracy of detection. IntruShield sensors perform thorough traffic inspection and protocol analysis by gathering detailed information on communication state, protocol, and application. This is used for highly accurate attack detection and real-time intrusion prevention.

### Signature Detection

Sensors offer powerful signature detection capabilities to accurately guard against known attacks.

- **Stateful Signature Detection Engine:** IntruShield sensors employ a patented stateful signature detection engine. This enables context-sensitive signature detection, leveraging state

information within data packets, utilizing multiple token matches and detecting attack signatures that span packet boundaries or are in an out-of-order packet stream.

- **Signature Specification Language:** IntruShield sensors utilize a proprietary, high-level Signature Specification Language. The IntruShield architecture decouples signatures from the sensor software, enabling quality signatures to be made available with a quicker turnaround.
- **Real-Time Signature Updates:** IntruShield sensors benefit from an innovative Real-Time Signature Update process, where new signatures are automatically pulled by the IntruShield Manager software at the customer site. Based on policy configuration, these signatures can be pushed from the IntruShield Manager to sensors automatically in real-time. IntruShield sensors dynamically utilize the latest signatures without requiring reset or reboot for uninterrupted attack protection.
- **User-Defined Signatures:** Sensors also leverage custom signatures that users can easily create through IntruShield Manager's intuitive graphical user interface.

### Anomaly Detection

Sensors' anomaly detection functionality can identify sophisticated first-strike and unknown attacks, improving attack detection rates.

- **Statistical, Protocol, Application Anomalies:** Sensors offer comprehensive anomaly detection by employing statistical, protocol, and application anomaly detection techniques.
- **Buffer Overflow Detection:** More than half of new exploits today are buffer overflow attacks. IntruShield's anomaly detection techniques are effective in protecting against this major threat source.

### Denial of Service (DoS) Detection

Sensors offer unprecedented accuracy and granularity for DoS detection and deliver the response actions needed to thwart these attacks.

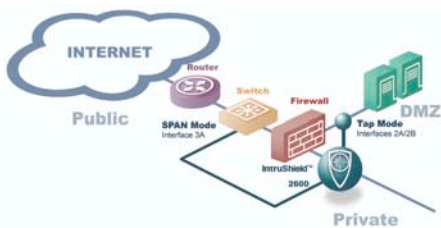
- **Self-Learning Profiles and Threshold-based Detection:** Sensors offer threshold-based detection as well as self-learning, profile-based DoS detection that uses a patented algorithm to separate even low volumes of attack traffic from large volumes of legitimate traffic.
- **Highly Granular DoS Detection:** Sensors deliver unparalleled granularity in DoS detection using profile-based techniques. A DoS profile contains pre-defined thresholds as well as self-learning parameters used to detect DoS attacks. A profile can be created for a range of IP addresses or even an individual host, and the IntruShield architecture supports several hundred profiles per sensor. Any deviation from normal traffic behavior flags a DoS condition. If a single host/subnet downstream to a Gigabit network link comes under attack—with even a couple of Mbps of traffic—a sensor's granular DoS detection can spot the attack.

# McAfee IntruShield Network IDS Sensor

## Flexible Deployment

IntruShield sensors enable large-scale IDS deployment across high-availability networks.

- **Three Modes of Operation:** Three flexible deployment modes enable sensors to be integrated within a wide range of network architectures.



*IntruShield can be deployed in SPAN, Tap, and In-line Modes.*

- **SPAN/Hub Monitoring:** The sensor can monitor hubs or the SPAN ports of multiple switches. The sensor can inject several response actions, such as TCP resets to terminate malicious connections through the monitoring port itself.
- **Tap Mode:** Full-duplex monitoring allows a complete direction-sensitive view of network traffic, enabling stateful analysis of traffic. This is leveraged for accurate detection and activating indirect prevention, such as firewall reconfiguration. Dedicated response ports enable indirect response actions, such as initiating TCP resets to terminate malicious connections.
- **In-Line Mode:** Sensors sit in the data path with active traffic passing through them, mediating the flow of traffic and dropping malicious packets—based on granular policy—before they reach their intended targets. Wire-speed performance and highly reliable operation prevent IntruShield sensors from becoming bottlenecks.

Fast ethernet network taps are built into the I-2600 for ease of installation and monitoring. Users can switch between tap and in-line mode for these ports using the IntruShield

Manager application—without any physical rewiring. Gigabit ethernet ports on the I-4000 and I-2600 employ external network taps. Mode selection is on a per port basis.

- **Port Clustering:** Port Clustering, or “interface grouping,” enables traffic monitored by multiple ports on a single system to be aggregated into one traffic stream for stateful intrusion analysis.
- **High Availability with Stateful Failover:** Sensors support high-availability IDS deployments using stateful sensor fail-over between two sensors, avoiding a single point of failure.

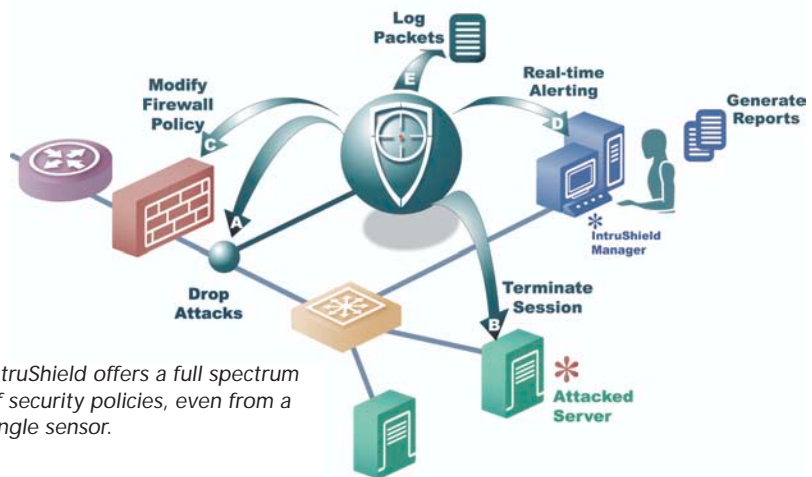
## Real-Time Intrusion Prevention

No security solution is complete unless it can actually stop attacks. Accurate detection is the foundation for the rich set of real-time intrusion prevention options available with IntruShield sensors. These attack response options enable IntruShield sensors to be integrated into network environments with a full spectrum of security policies, ranging from real-time notification to complete blocking of attacks in progress. Upon detecting an attack, IntruShield sensors can:

- A. Drop or block a single packet or a single session between the attack source and destination in real-time, with very high granularity. This can thwart an attack in progress all the

way down to a single flow transmitting to a single server within a server farm without affecting any other traffic when the IntruShield sensor is operating in in-line mode.

- B. Initiate TCP resets or ICMP unreachable messages through response ports to the victim, attacker, or both when the sensor is operating in tap or SPAN mode. TCP resets can be sent for SYN Flood-type DoS attacks.
- C. Reconfigure firewalls to block offending traffic.
- D. Trigger a real-time notification or alert to the IntruShield Manager. With e-mail, pager, and script alerts, network security professionals can be notified, based on a configured severity level or per user-selected attacks. Script-based alerts enable the configuration of robust notification processes, which can inform specific groups and individuals of incoming attacks. Forensic logging enhances packet/session logging to capture additional data following an attack (e.g., all subsequent communication between the attacker and victim) as forensic evidence and/or to assess the impact of a successful attack.
- E. Capture and log packets prior or subsequent to the attack for detailed attack analysis. Post-attack logging of packets/sessions between intruder and victim allow accurate analysis of attack impact.



*IntruShield offers a full spectrum of security policies, even from a single sensor.*

# McAfee IntruShield Network IDS Sensor

Integrated detection and prevention in a single product enable the flexibility to migrate from intrusion detection to intrusion prevention at a user-selected pace, while preserving end-user investment in the technology.

## Multi-Gigabit Performance

IntruShield sensors are powered by programmable security-focused hardware. Intrusion detection and prevention is an extremely compute-intensive application, requiring eight to ten times the processing power of a firewall. Specialized silicon is used to speed up almost every function with orders of magnitude improvements in repetitive tasks such as protocol analysis, statistical analysis, string matching, and virtualization. As a result, IntruShield sensors can support thousands of signatures at wire-speed traffic rates without any packet loss, while protecting

against known, unknown, and DoS attacks. IntruShield delivers compelling price/performance for bandwidth needs ranging from few tens of Mbps to 2 Gbps.

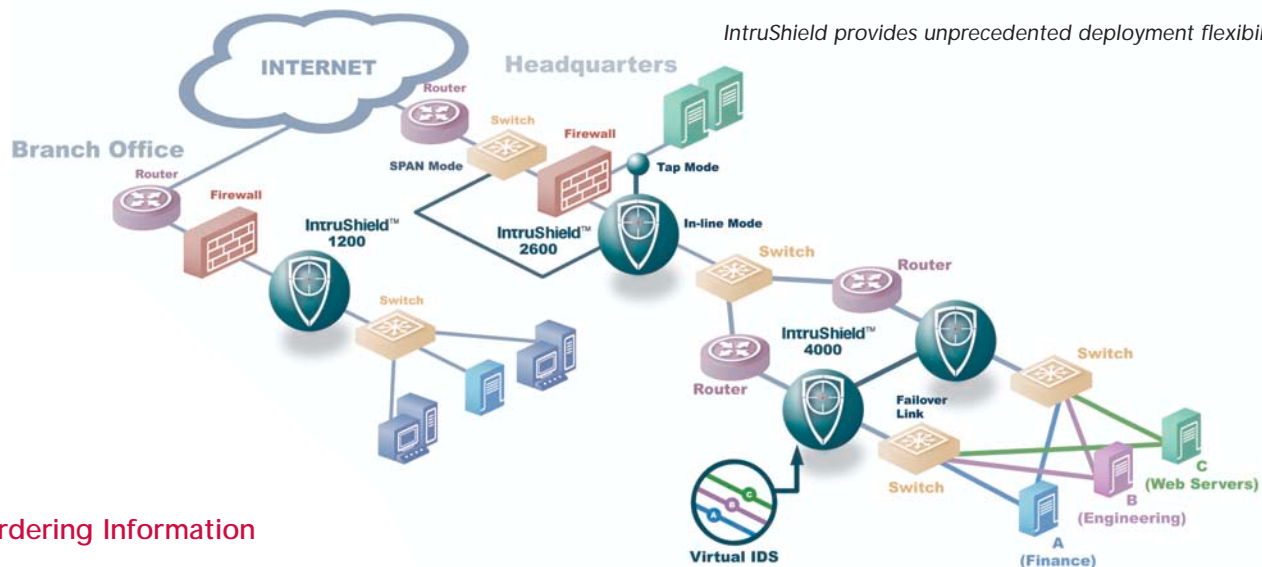
## Interoperability

The IntruShield IDS system provides interoperability with leading firewalls, enterprise management applications and Security Information Management (SIM) applications offering a reduced total cost of ownership.

## Enterprise Deployment

Besides delivering innovative features, the IntruShield solution offers unparalleled scalability for enterprise-wide IDS deployment spanning enterprise core, enterprise perimeter and branch office networks. The IntruShield system can be deployed across a wide range of network security architectures.

The IntruShield 4000's multi-gigabit performance makes it suitable for deployment at logical traffic aggregation points at the core of the enterprise network or in data centers. By deploying sensors in front of the server farm, users can leverage IntruShield's Virtual IDS capability to monitor each aggregation point with multiple customized security policies. Furthermore, the sensor's high-availability deployment option—using stateful failover between two sensors—provides operational redundancy, preventing any single point of failure, and offers uninterrupted IDS protection. The IntruShield 2600, with its Fast and Gigabit Ethernet interfaces, offers a flexible solution for the perimeter of enterprise networks. The IntruShield 1200 delivers a scalable solution for mid-size and branch and remote offices of enterprise networks.



## Ordering Information

Part Number	Description
ICVS04KADEA	IntruShield 4000 Sensor Appliance
ITV-F04K-NA-100	IntruShield 4000 Sensor Appliance Failover Configuration
ICVS26KADEA	IntruShield 2600 Sensor Appliance
ITV-F26C-NA-100	IntruShield 2600 Sensor Appliance Failover Configuration
ICVS12KADEA	IntruShield 1200 Sensor Appliance
IMGCU-AD-A	IntruShield Global Manager Software
IMSCUED-A	IntruShield Manager Software
ITV-RPS4-NA-100	Redundant AC Power Supply for the IntruShield 4000 Sensor

# McAfee IntruShield Network IDS Sensor

## IntruShield Sensor Specifications

Sensor Software Components		I-4000	I-2600	I-1200
Stateful Traffic Inspection	IP Defragmentation & TCP Stream Reassembly	Yes	Yes	Yes
	Detailed Protocol Analysis	Yes	Yes	Yes
	Asymmetric Traffic Monitoring	Yes	Yes	Yes
	Protocol Normalization	Yes	Yes	Yes
	Unicode Detection	Yes	Yes	Yes
	Whisker De-obfuscation	Yes	Yes	Yes
	Forensic Data Collection	Yes	Yes	Yes
	Protocol Tunneling	Yes	Yes	Yes
	Protocol Discovery	Yes	Yes	Yes
	Signature Detection	User-defined Signatures	Yes	Yes
Real-Time Signature Updates		Yes	Yes	Yes
Anomaly Detection	Statistical Anomaly	Yes	Yes	Yes
	Protocol Anomaly	Yes	Yes	Yes
	Application Anomaly	Yes	Yes	Yes
DoS Detection	Threshold-based Detection	Yes	Yes	Yes
	Self-learning Profile-based Detection	Yes	Yes	Yes
	DoS Profiles	5,000	300	100
Intrusion Prevention	Stop Attacks in Progress in Real-Time	Yes	Yes	Yes
	Drop Attack Packets/Sessions	Yes	Yes	Yes
	Drop DoS Packets	Yes	Yes	Yes
	Reconfigure Firewall	Yes	Yes	No
	Initiate TCP Reset, ICMP Unreachable	Yes	Yes	Yes
	Packet Logging	Yes	Yes	Yes
	Automated Prevention	Yes	Yes	Yes
	User-initiated Prevention	Yes	Yes	Yes
	High Availability	Stateful Fail-over	Yes	Yes (for Fast Ethernet Ports)
Network Notification on Fail-over		Yes	Yes	-
Management	Command Line Interface (Console)	Yes	Yes	Yes
	Manager Communication	Secure Channels	Secure Channels	Secure Channels

Sensor Hardware Components		I-4000	I-2600	I-1200	
Performance	Throughput	Up to 2 Gbps	Up to 600 Mbps	Up to 100 Mbps	
	Concurrent Session State Maintenance	1,000,000	250,000	40,000	
Ports	Gigabit Ethernet Detection Ports	4	2	-	
	Fast Ethernet Detection Ports	-	6	2	
	Dedicated Fast Ethernet Response Ports	2	3	1	
	Dedicated Fast Ethernet Management Port	Yes	Yes	Yes	
	Console and Aux Ports	Yes	Yes	Yes	
	Built-in Network Taps	No	Yes (for Fast Ethernet Ports)	Yes	
	Fail-open	Yes	Yes	Yes	
	Fail-close	Yes	Yes	Yes	
	Mode of operation	SPAN Port Monitoring	Yes	Yes	Yes
		Tap Mode	Yes	Yes	Yes
In-line Mode		Yes	Yes	Yes	
Port Clustering		Yes	Yes	Yes	
No. of Virtual IDS (VIDS) Systems		1,000	100	16	
Traffic Monitoring on Active-Active Links		Yes	Yes	Yes	
Traffic Monitoring on Active-Passive Links		Yes	Yes	Yes	
Monitoring of Asymmetric Traffic Routing		Yes	Yes	Yes	
High Availability		Redundant Power	Yes (Optional)	No	No
	Device Failure Detection	Yes	Yes	Yes	
	Link Failure Detection	Yes	Yes	Yes	
Physical	Dimensions	2 RU rack-mountable	1 RU rack-mountable	1 RU rack-mountable	
		17.44 (W) x 3.44 (H) x 23.00 (D)	17.32 (W) x 1.69 (H) x 17.64 (D)	17.32 (W) x 1.65 (H) x 10.5 (D)	
	Weight	38 lbs.	20 lbs.	7 lbs.	
	Power	100-240VAC (50/60 Hz)	100-240VAC (50/60 Hz)	100-240VAC (50/60 Hz)	
	Power Consumption	350W	250W	100W	
	Temperature	0 to 40 C (Operating) -40 to 70 C (Non-operating)	Same for All Models	Same for All Models	
	Relative Humidity (non-condensing)	Operational: 10% to 90% Non-operational: 5% to 95%	Same for All Models	Same for All Models	
	Altitude	0 - 10,000 feet	Same for All Models	Same for All Models	
	Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040	Same for All Models	Same for All Models	
	EMI Certification	CB license and report covering all national country deviations. FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	Same for All Models	Same for All Models	



3965 Freedom Circle | Santa Clara, CA 95054 | 800.764.3337 main

networkassociates.com



YOUR NETWORK. OUR BUSINESS.™