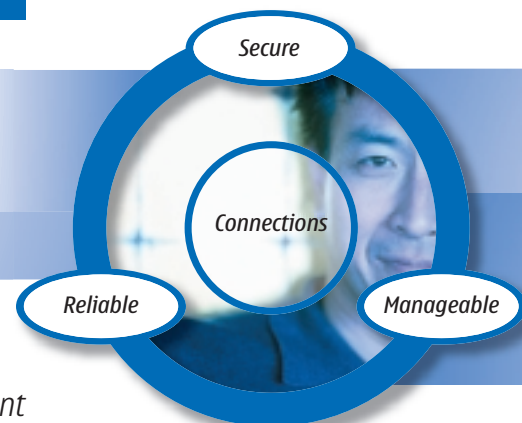# Nokia Message Protector

Secure Content Management from Nokia

Nokia Message Protector is an enterprise-class secure content management appliance for SMTP (simple mail transport protocol) traffic entering, flowing within and leaving corporate mail networks. Complementing the Nokia IP Security Platform family, Message Protector has its own hardware platform and specifically designed IPSO-SX operating system optimized for intensive corporate mail networks. Nokia Message Protector can decrease total cost of ownership for enterprise customers.

Challenges to Securing Enterprise Mail

Email remains the mission critical application for the enterprise. Protecting against security exploits is essential to ensuring the flow of communication and protecting on-line assets. More than 80% of enterprise exploits are targeted at this mission critical application. Malicious exploits are increasingly frequent and sophisticated in attacking network vulnerabilities, and threatening corporate intellectual property, IT assets, financial assets, health records and personal identity privacy and liability.

Anti virus solutions at the desktop have failed to achieve a unified barrier of protection against blended threats and hybrid worms. Desktop solutions are limited in scope, fail to prevent virus attacks and are expensive to maintain. The decentralized and distributed nature of corporate networks—headquarters, multiple regional and branch offices—means exclusive dependence on desktop architectural integrity and management efficiency is inadequate.

The scope of secure content management extends far beyond anti virus. Perimeter based appliances capable of adding a layered approach for hardware, software and security policy are required to complement desktop based virus protection. Nokia believes that a best-of-breed appliance with multiple secure content management technologies, including Internet gateway virus protection from Trend Micro, offers customers a leading content management solution.

Message Protector Unique Benefits
- Appliance
- Performance
- Trend Micro™ Partnership
- Statistical Protection™
- Secure & Automatic Updates

Nokia Message Protector

The Message Protector appliance sits between the corporate firewall and mail server(s), and functions as the externally visible gateway MTA (mail transport agent) for the corporate network (Refer to Figure 1). Easy to deploy and manage, the Nokia SC6600 appliance platform can be configured via Message Protector's Network Voyager element management tool. Nokia Statistical Protection™ technology includes multiple virus scanning engines, macro stripping, and behavioral filters that work in a layered protection approach to block exploits, reject nuisance email, and quarantine inappropriate content. Because Message Protector is a true appliance, it can provide performance leadership in security, mail processing and signature update deployment speed, as well as Nokia acclaimed First Call—Final Resolution support.

Nokia SC6600

NOKIA
CONNECTING PEOPLE

True Appliance Value

Fast and simple deployment is a principal advantage of the Message Protector appliance. Nokia IPSO-SX provides a hardened operating system environment that is optimized for high processing performance and throughput of SMTP traffic. Unlike a proxy server, Message Protector's MTA design guards the identity of corporate mail servers. Its store and forward mail characteristics works to ensure all incoming email is protected until delivery to destination mail server(s) is confirmed. Nokia Message Protector is backed by a global support infrastructure, world-class facilities and expertise to provide online registration, installation, maintenance and operational integrity. First Call-Final Resolution technical support offers customers a single point of contact for expert technical assistance and resolution on partner software as well as the Nokia platform and operating system.

Performance

Nokia Message Protector is capable of processing more than 120,000 emails per hour due to dual P4 Xeon processors and 1 GB of RAM. This superlative level of performance is delivered by an application and purpose-built system design providing dedicated protection for SMTP messaging to ensure that corporate mail servers won't experience disruption in email flow, even when the Message Protector is confronting a malicious code attack. To protect against mail message loss or corruption, RAID-1 disk mirroring commits incoming email to disk until receipt is confirmed by the destination mail server(s).

Trend Micro™ Partnership

Nokia is combining its global leadership in appliance-based IP network security systems, with Trend Micro's leadership in network anti virus technology to provide enterprise mail networks with a Message Protector appliance at the Internet gateway. In addition to setting new standards for rapid response to exploits and consulting services for outbreak prevention, Trend Micro has established market leadership with more than 41%[1] anti virus market share at the Internet gateway. Without doubt, Trend Micro represents a best-of-breed technology partnership designed to offer fast and comprehensive protection at the Internet gateway against virus outbreaks. Nokia and Trend Micro have already established momentum with collaboration on content security innovations that makes Message Protector the first in a line of messaging protocol content solutions.

[1] IDC, Antivirus Software 2002: A Segmentation of the Market, 2002
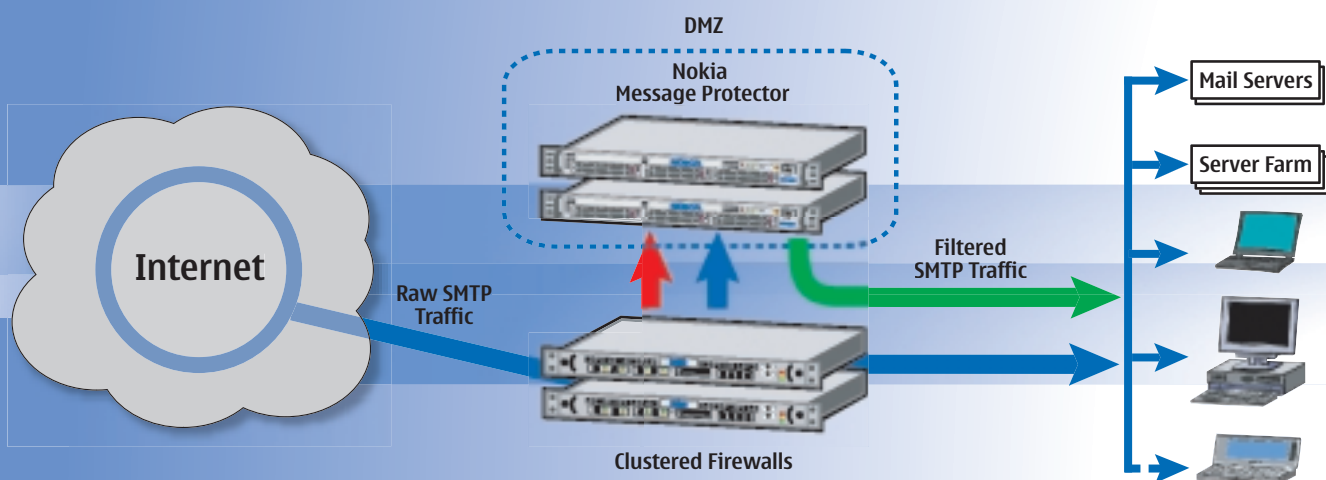
Figure 1: Nokia Message Protector in the Network

DMZ

Nokia Message Protector

Mail Servers

Server Farm

Internet

Raw SMTP Traffic

Filtered SMTP Traffic

Clustered Firewalls

Figure 2: Message Protector Statistical Protection

HERO[3]	
Hardened Point of Contact	
SPAM Rejection	
Intermediary Implementation	
Unencapsulation & Decompression	
	Fast Rejection
	Format Conformance
	Content Type Analysis
Anti-Virus Scanning	
Content Management	

[3] Heuristic Exploit Rejection Object™ (HERO)

Statistical Protection

The scope of secure content management extends beyond anti-virus protection. To address this, Message Protector orchestrates multiple technologies all directed specifically at controlling SMTP traffic entering, flowing within and leaving an enterprise mail network. Nokia Statistical Protection technology offers the highest degree of speed and security performance. In addition to element management and hardware integration, Message Protector's layered application protection approach includes in-depth, defensive characteristics such as multiple virus scanning technologies, con-

tent management, SPAM protection, intelligent exploit rejection and signature generation, with secure and automatic updates for minimal latency in deployment of the latest exploit prevention technology. Figure 2 illustrates Message Protector Statistical Protection.

Hardened Point of Contact

Message Protector complements the software strengths of the Nokia IP Security Platform series with the inclusion of specially architected, hardened IPSO-SX operating system, based on Linux. This rigorous design combines the advantage of IPSO's optimized reliability and security performance with intensive processing requirements dedicated for an SMTP gateway appliance.

SPAM Rejection

Message Protector controls mail traffic with configuration options to create "white" and "black" privilege lists based on known host names, IP addresses, and net blocks.

- White list: Allow free mail relays from specified addresses.
- Black list: Checks source IP against block list and denies open relays to block nuisance mail.

Intermediary Implementation

- Message Protector's unique MTA store and forward feature retains a copy of incoming mail on RAID-1 mirrored-disk to guarantee delivery and receipt of mail, in the event of power failure.

- Serving as a gateway MTA, denial of service (DoS) protection works to exponentially time out on multiple connections directed by an individual source.

Unencapsulation and Decompression

Message Protector unencapsulation and decompression engines take archive attachments from mail and break them into discrete files for accurate scanning and file extension validation.

Heuristic Exploit Rejection Object (HERO)

Message Protector's patent pending technologies protect corporate mail servers with HERO characteristics for intelligent and effective exploit rejection. This behavioral filtering technology is active in both Message Protector appliance and its back-end update service platforms.

- Fast Rejection: Heuristic-driven, rule-based filtering looks for malicious mail and stops new and derived exploits. This front-end layer accelerates detection and rejection and quarantine of repetitive exploits, for timely defense against security threats.
- Format Conformance: Helps prevent mail server crashes from malicious or inadvertent malformed messages by verifying email format—header, body, attachment—for null mime boundary and date buffer overflow.
- Content Type Analysis: For added protection against malicious mail attachments, discrete file extensions are validated against the internal file architecture and scanned to validate file identity.

Anti-Virus Scanning

Message Protector is a culmination of the Nokia commitment to secure content management. Multiple virus scanning technologies work in a statistical approach to bring leading innovation in virus outbreak prevention to SMTP messaging.

Content Management

Message Protector's content management capability is focused on controlling what enters and leaves the enterprise mail network. Macro stripping capabilities quickly and efficiently break mail messages down into their component parts for fast and accurate scanning of file names and file extensions. A scanning engine records signatures from rejected messages to generate a signature rejection database.

Secure Automatic Updates

The Nokia objective is to help customers eliminate the significant costs of virus outbreaks, and achieve rapid containment of threats, thus preventing propagation. Nokia Message Protector adds value by minimizing the latency between the availability of new signature updates and deployment throughout the enterprise mail network. This is accomplished via three features that differentiate the Nokia Message Protector:

• All updates to the appliance are signed by Message Protector's back-end service infrastructure.
• All updates are pulled down to the Message Protector over a secure communication channel.
• Message Protector's back-end service infrastructure is capable of providing upgrades to the Message Protector application in addition to updating signatures.

Since Nokia controls the hardware and software configuration for the Message Protector appliance, systematic testing of signature updates is fast and complete. Because Message Protector pulls down signed updates over a secure communication path, there is no need for a customer to validate updates for authenticity or compatibility. Deployment is immediate and automatic.

Nokia SC6600 at a Glance

• 1 RU chassis
• Dual high speed P4 Xeon processors
• Standard with 1GB RAM
• Dual 36 GB, "hot swap" SCSI drives in a hardware RAID-1 configuration
• Console port for access

Nokia SC6600

1- Integrated 10/100 Ethernet

1- Integrated 10/100/1000 Ethernet

Dual P4 Intel Xeon processors

Dual SCSI RAID-1 array with dual drives

Width: 16.8 in. / 42.8 cm

Height: 1.7 in. / 4.4 cm

Depth: 25.6 in. / 65 cm

Weight: 24.5 lbs. / 11 kg

Power Requirements:
   100-240V (auto switching)
   50/60 Hz, 400W, 8A MAX

Americas
Tel: 1 877 997 9199
Email: ipsecurity.na@nokia.com

Asia Pacific
Tel: +65 6588 3364
Email: ipsecurity.apac@nokia.com

Europe, Middle East and Africa
France +33 170 708 166
UK +44 161 601 8908
Email: ipsecurity.emea@nokia.com

NOKIA
CONNECTING PEOPLE