

PROTECTION FOR CRITICAL MICROSOFT® BUSINESS APPLICATIONS

SECURE
MANAGE
DEPLOY



NS SERIES SECURITY APPLIANCES AT A GLANCE

SIZED FOR SMALL OFFICES UP TO THE LARGEST ENTERPRISES, all NS Series appliances provide the same core security functions in a compact 1U rackmount chassis.



	1:1 Automatic Failover	Backup and Recovery Features	Secure Remote Management	Secure Automated Updates	Dual Drives	Dual Power	Hot-swappable Drives and Power	MOM Integration	Secure Application Manager	WebSense Web Security Suite™	Exchange Mailbox Clients	Target Market	
	✓	✓	✓	✓			✓	✓				500	Small Business or Branch Office
	✓	✓	✓	✓			✓	✓				500	Small to Medium Office
	✓	✓	✓	✓			✓	✓	✓			1,000	Medium Business to Small Enterprise
	✓	✓	✓	✓	✓		✓	✓	✓			1,500	Small to Medium Enterprise
	✓	✓	✓	✓	✓	✓	✓	✓	✓			4,000	Medium to Large Enterprise

NETWORK ENGINES: *THE APPLIANCE COMPANY*



Network Engines builds more than 10,000 appliances every quarter for world-class customers who demand superior quality, performance and functionality from security and storage solutions. The company's award-winning security appliance family, the NS Series™, delivers advanced application-layer protection necessary to defeat modern Internet threats.

Network Engines developed the NS Series appliances in partnership with Microsoft® to leverage the power of Microsoft Internet Security and Acceleration (ISA) Server 2004. The company's unique appliance technology – NEWS™ – enables seamless deployment of mission-critical protection for Microsoft applications including Exchange, OWA/OMA, SharePoint®, IIS, and Windows® XP clients for organizations of every size.

CHALLENGE: CORE APPLICATION SERVERS ARE UNPROTECTED

Today's application-layer threats breeze through simple perimeter firewalls to infect core applications.

These assets are also vulnerable to self-propagating malicious code which can traverse unprotected LANs behind the firewall after being downloaded from seemingly innocent Web sites.

APPROACH: DEFENSE-IN-DEPTH

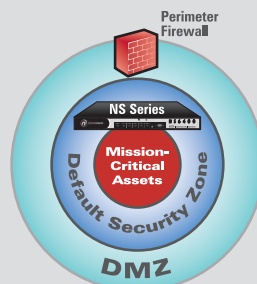
To defeat these threats, organizations need specific protection arranged in layers surrounding critical assets.

Known as defense-in-depth, this best-practice strategy enables enterprises to build effective security systems that safeguard business communication pathways and give valuable data the protection it requires – while enabling authorized users to access it from wherever their business takes them.

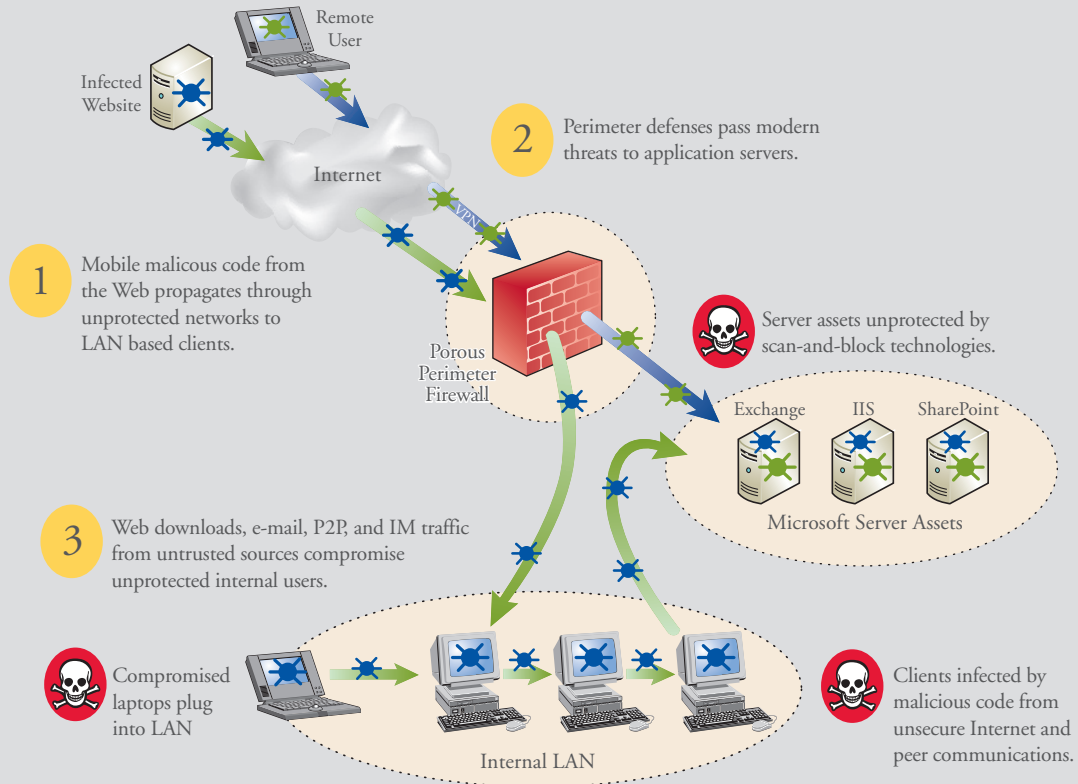
SOLUTION: NS SERIES WITH INTEGRATED WEBSense WEB SECURITY SUITE™

NS Series Security Appliances implement defense-in-depth by performing application-level deep packet inspection to ensure that only known-good traffic reaches core Microsoft application servers.

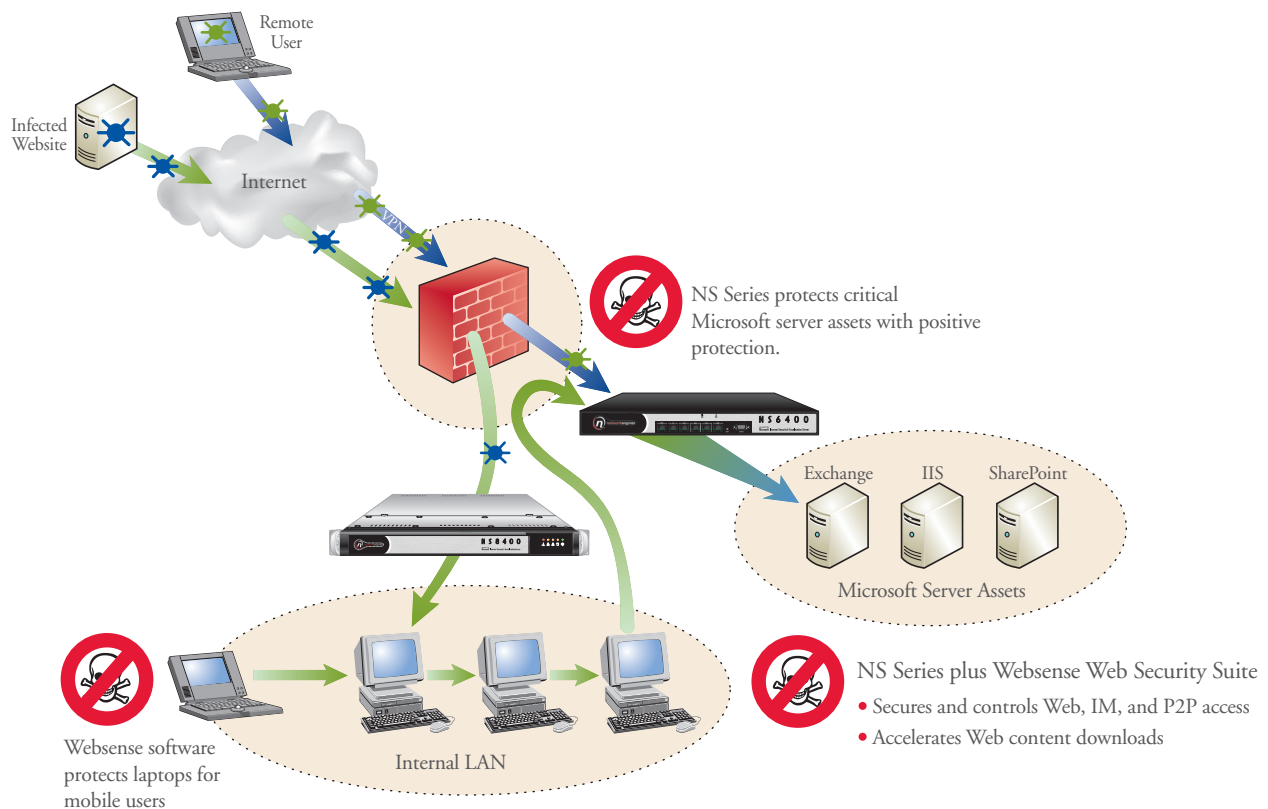
NS Series with optional Websense Web Security Suite blocks known threats including malicious code, phishing, pharming, and keylogging. NS Series with Websense also controls and secures IM, P2P, e-mail, file transfer, and other protocols.



TYPICAL PERIMETER-ONLY DEFENSE



DEFENSE-IN-DEPTH WITH THE NS SERIES



PROACTIVE DEFENSE FOR CRITICAL MICROSOFT APPLICATIONS

THE MOST VALUABLE INFRASTRUCTURE ASSETS OF ANY ORGANIZATION ARE ITS MESSAGING, COLLABORATION, AND WEB SYSTEMS. NS SERIES APPLIANCES PROVIDE THE MOST COMPREHENSIVE PROTECTION FOR THESE VITAL SYSTEMS:

POSITIVE DEFENSE FOR EXCHANGE SERVERS

By combining negative defenses which block known threats with positive defenses that permit only authenticated users to initiate communications and other actions that exhibit “known good” behavior and attributes, the universe of methods available for compromise is substantially reduced. NS Series appliances installed in front of Exchange servers protects them from internal and external attacks while enabling anywhere access to Exchange using a variety of secured protocols:

- Secure publishing for Microsoft Outlook® Web Access (OWA)
- Forms-based authentication enforces valid credentials for OWA
- SSL and VPN termination and proxy services perform application-layer inspection of encrypted content
- RPC proxy service ensures that only valid RPC connections propagate to Exchange servers

COMPREHENSIVE WEB PROTECTION

With the optional Websense Web Security Suite, NS Series appliances provide an integrated Web security solution that protects organizations from both internal and external threats:

- Able to block more than 1 million categorized executables
- Allows/disallows protocols including P2P, IM, streaming media, and remote access
- Enables/disables access to more than 10 million categorized sites
- Real-time updates quickly block newly discovered threats

SECURE, MANAGE, DEPLOY: THE NS SERIES APPLIANCE ADVANTAGE

NS SERIES SECURITY APPLIANCES ENABLE ORGANIZATIONS TO SECURE ACCESS TO ESSENTIAL SERVER APPLICATIONS BY PROVIDING A MANAGEMENT ENVIRONMENT THAT EASES IMPLEMENTATION IN MANY IMPORTANT WAYS:

- Automated updates reduce the cost and simplify maintenance by eliminating the need for each customer to scan for updates, determine their applicability, and perform the testing required to ensure proper integration
- Configuration management streamlines backup and restore operations
- Remote management console enables secure administration from any location via RDP over HTTPS
- 1:1 failover, dual ISP failover, and return-to-factory-default settings provide system resiliency and fault tolerance
- Secure Application Manager provides tight integration of Websense Web Security Suite
- Alert management notifies support staff of problems via SMTP
- MOM agent enables staff to monitor NS Series operation using Microsoft Operations Manager

It costs less to deploy Microsoft ISA on NS Series appliances than on general-purpose servers. Tight integration with Websense provides comprehensive defense-in-depth protection with unparalleled ease of deployment and management.



Network Engines, Inc.
25 Dan Road, Canton, MA 02021 USA
Appliance Sales: +1 877-638-9323 • Fax: +1 781-770-2000

email: NSsales@networkengines.com
www.networkengines.com