

NS SERIES

powered by
Microsoft® Internet Security & Acceleration Server



Protecting Microsoft® Exchange Server with NS Series Security Appliances

PROBLEM: Microsoft Exchange Server provides organizations with access to email, calendars, tasks and contacts from any Internet-connected location. Yet, securing this messaging system has become increasingly difficult. The inability of traditional security technologies to inspect encrypted content (SSL) or proprietary Exchange protocols provides an express lane for email-borne attacks which bypass enterprise security defenses. Attack vectors are also changing – those targeting specific software vulnerabilities have complicated the task of ensuring confidentiality, integrity and availability of vital information and computing resources. And it's not getting easier. Research firm Gartner states that 70 percent of all web attacks target the application layer. Blaster, Sasser and Nachi are recent examples of RPC worm variants that successfully targeted the Exchange application. To ensure that your Exchange service is providing the messaging infrastructure necessary to support a mobile workforce demands a new approach to security – defense-in-depth. While traditional firewalls provide critical protection for the corporate network's connection to the Internet, they do little to stop SMTP/POP3 exploits and email-borne attacks. To attain an in-depth defensive security posture, the strategy must be enhanced with Exchange-specific, application layer filtering.

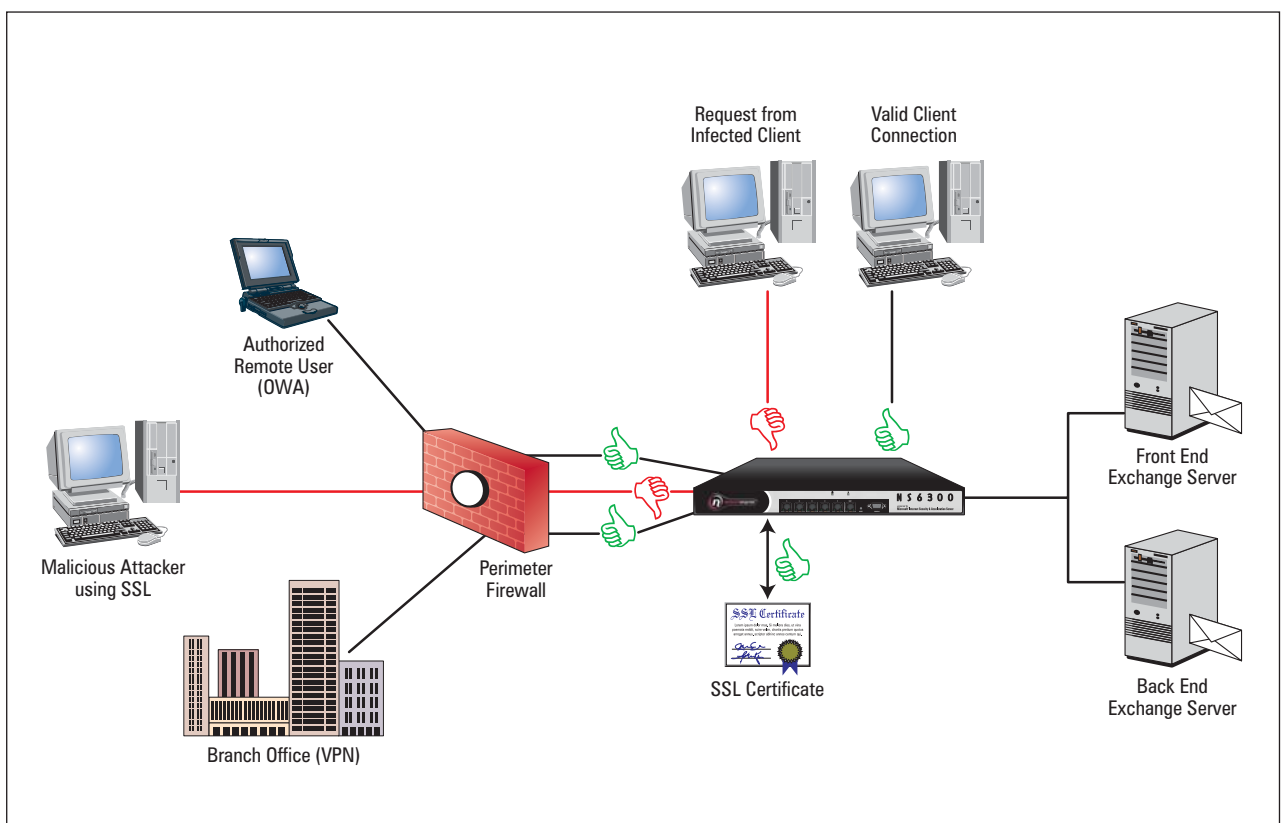
SOLUTION: The NS Series is a multi-layered security appliance that delivers comprehensive application layer filtering in addition to stateful packet filters. The product is powered by Microsoft Internet Security and Acceleration (ISA) Server 2004 and operates on a Network Engines hardened version of Windows Server 2003. To achieve best-practice defense-in-depth, the NS Security Appliance should be placed behind a high-speed packet filtering firewall in a high-speed Internet connection environment. This is especially important on networks with multi-gigabit connections. Packet-filtering firewalls reduce the total amount of traffic each back-end NS Series Appliance must process. The reduction in overhead allows the NS Security Appliance to operate at peak performance, providing the deep application layer inspection required to secure Exchange infrastructures.

Key Benefits

NS Series Security Appliances, powered by ISA Server 2004, secure and simplify access to Microsoft Exchange Server from remote locations. These features include:

- Forms-based authentication to increase the security of Microsoft Outlook® Web Access (OWA)
- Secure RPC publishing to provide remote employees with full Outlook client access
- Powerful mail-server publishing wizards eliminate configuration mistakes
- Reduction of unwanted email with the SMTP Message Screener
- SMTP and POP3 filters to protect against mail server attacks.

APPLICATION BRIEF



Protecting Exchange: The NS Series Security Appliance secures an Exchange installation by providing deep application layer inspection and user credential authentication.

KEY FEATURES

Forms-Based Authentication for Increased OWA Security

When remote users attempt to log on to Microsoft Exchange Server 2003 through a Web browser, the Outlook Web Access server generates a log-on form. After the user completes the form, the OWA server checks the user's credentials and allows or denies the log-on request. However, while the authentication process is taking place, the unauthenticated user has a direct connection to the OWA server. Even if authentication is denied, an attacker can take advantage of the connection to gain access to server and Web site content. For this reason, it is important to prevent users from accessing an OWA server until after they have been authenticated.

NS Series Security Appliances solve this problem by generating the OWA logon form. Instead of requiring the remote user to connect to the OWA server to access the form, the embedded ISA Server 2004 firewall generates the form and then forwards credentials to the OWA server. When the OWA server successfully authenticates the user, the ISA Server 2004 firewall grants access to the OWA site, enabling the user to access email and other Exchange Server information. In this way, forms-based authentication prevents unauthenticated users from accessing an OWA server.

Secure RPC Publishing for Full Outlook Client Access

Corporations standardizing on the full Outlook MAPI client give users access to the complete range of services available from Exchange Server, enabling significantly increased productivity. In the past, however, users at remote locations who needed to access Exchange mailboxes were unable to benefit from the full set of Exchange and Outlook features. Because there was no way to securely connect from a remote location to the full suite of services using the full Outlook MAPI client, remote users had to use an alternative email client, leading to reduced productivity and diminished satisfaction with the overall Exchange experience.

NS Series Security Appliances solve this problem by using an RPC filter to perform application-layer inspection of RPC connections moving through the firewall. The embedded ISA 2004 firewall forwards only legitimate RPC connections to Exchange Server, dropping all other RPC connections, such as those generated by prevalent Internet worms. With this capability, corporate users working outside of the office can continue using the familiar email client and benefit from the entire array of Exchange Server services. Whether in the corporate office or a continent away, users can open laptops, start Outlook and discover that it works no matter where they are.

Powerful Mail-Server-Publishing Wizards

Publishing Exchange Server mail services allows users on the Internet to connect to these services. However, because any Internet-accessible resource is a potential target for attack, it is critical that these services be published securely. The problem is that configuring a firewall to securely publish Exchange services to Internet-based users can be complicated—and misconfigured publishing rules can lead to unexpected results.

NS Series Security Appliances address this issue by providing intuitive yet powerful mail-server-publishing wizards that take the guesswork out of publishing Exchange to the Internet. Three mail publishing wizards are available:

1. Outlook Web Access
2. Secure SMTP/POP3/IMAP4
3. Mail server-to-server publishing wizard

Each wizard allows the firewall administrator to quickly and securely publish Exchange services to the Internet. The administrator can review firewall access policies created by the wizards and if desired, change them before implementing.

Reduction of Unwanted email with the SMTP Message Screener

NS Series Security Appliances include an SMTP Message Screener that blocks spam by evaluating the following characteristics of incoming and outgoing email: where it is going (destination), where it is coming from (source), whether it contains administrator-defined keywords or character strings in the subject or body, the name, file type, and size of any attachments.

If the above characteristics match patterns identified as spam, ISA Server can be configured to immediately delete the message, forward it to an email security administrator for further action, or hold it in a special folder on the ISA Server machine. Message Screener can also be configured to block mail containing attachments known to contain viruses or other malicious software.

SMTP and POP3 Filters to Protect Mail Servers

Internet-based attackers can use buffer overflow attacks to compromise the SMTP and POP3 mail services in Exchange. The intelligent, application-layer filtering in ISA Server 2004 helps prevent intruders from disabling or taking control of SMTP and POP3 services by blocking buffer overflow attacks against these services. The SMTP and POP3 application-layer filters in ISA Server 2004 inspect all incoming SMTP and POP3 communications and block any command sequences that could potentially disrupt the SMTP and POP3 services.

For more information, contact:

InTechnology

InTechnology (Security Solutions)

1320 Arlington Business Park, Theale, Reading, Berkshire RG7 4SU

Phone +44 (0) 870 366 8511 • Fax +44 (0) 870 366 8522

email: security@intechnology.co.uk • training@intechnology.co.uk

www.intechnology.co.uk