

NS SERIES

powered by
Microsoft Internet Security & Acceleration Server



Enabling Secure Mobility with Exchange and NS Series Security Appliances

PROBLEM: Today's businesses operate in an increasingly mobile environment. A multitude of portable devices used by employees, partners and customers are used to increase productivity, competitiveness and customer satisfaction. This need to satisfy employee demand for around-the-clock network access is motivating enterprises to implement mobility solutions. In fact, in this business climate the definition of "mobility" has taken on new meaning – access to enterprise information and network resources anytime, anywhere.

Providing unfettered freedom for users to access the enterprise network, wherever and whenever a user needs access, requires new security strategies to accommodate the various network connections used to communicate. Increasing productivity without compromising the security of the network continues to be an important goal for enterprise customers. While users demand mobility, business executives and network managers must address the complex network challenges associated with deploying a highly secure, mobile network solution.

THE NS SERIES SOLUTION: Microsoft Exchange Server 2003 supports a variety of connectivity options, including Outlook Web Access, Outlook Mobile Access, Exchange Active Sync and Exchange RPC (MAPI) over the Web (HTTP). Although Exchange can provide the immediate access to information that the mobile workforce requires, OWA, OMA and RPC expose Exchange servers to the perils of a connected world. The challenge for administrators is to permit access from authorized users while protecting Exchange from being used as an attack vector.

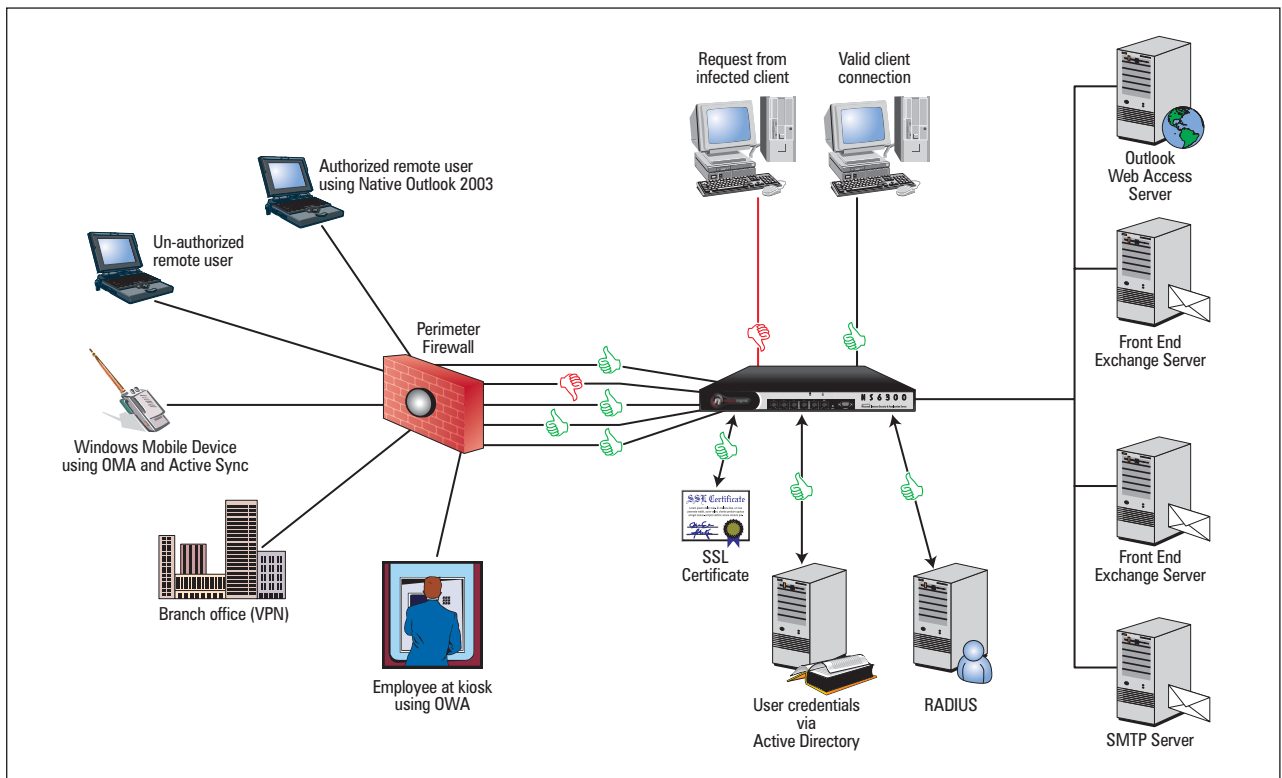
The NS Series, powered by Microsoft Internet Security & Acceleration Server 2004, delivers comprehensive application layer filtering specifically designed to protect Exchange Server. The NS Series secures the Exchange architecture with a comprehensive approach for the provisioning of Web-based access via OWA/OMA and native Outlook support using RPC (MAPI) over secure SSL connections. In addition, integration with Active Directory and support for forms-based authentication ensures that only authorized users are accessing the network. The NS Security Appliance enables Exchange to deliver full-function secure mobility services to a broad range of remote client devices while enforcing the strictest security policies in the industry.

Key Benefits

NS Series Security Appliances, powered by ISA Server 2004, allow local and remote users to securely and easily access Microsoft® Exchange Server from any location. These features include:

- Secure remote access from a Web browser using Microsoft Outlook® Web Access (OWA)
- Native remote Outlook access using secure RPC filtering and publishing
- Access from wireless mobile devices using Outlook Mobile Access (OMA), via secure HTTP over SSL communications
- Secure access to Windows® Mobile devices using Exchange Active Sync (EAS)
- Secure use of thin email clients like Outlook Express using SMTP and POP3 filters to protect against mail server attacks
- Secure Site-to-Site or Client-to-Site access using ISA 2004 VPN Networking capability.

APPLICATION BRIEF



Secure Exchange Server Mobility: The NS Series Security Appliance enables secure, remote Exchange access from a variety of client-side devices.

KEY FEATURES

Outlook Web Access

True corporate mobile access means accessing Exchange services anywhere, anytime. Typically, however, remote users do not have full Exchange access using traditional Outlook clients such as kiosks, public computers and non-corporate home office computers. For the remote user, it is most convenient to access Exchange functionality through a standard Web browser that supports HTML and JavaScript. By contrast, the NS Series Security Appliance provides remote users with either the basic Outlook Web Access (OWA) experience for simple messaging or the rich OWA experience utilizing folder hierarchy, drag-and-drop functionality, shortcut menus, spellcheck and the creation and management of server-side rules. This flexibility ensures that all Exchange users have secure access to the rich functionality of Exchange without requiring a corporate laptop or VPN connection.

Secure Remote Native Outlook Client

E-mail users frequently require full Outlook functionality when communicating with Exchange Server. In these instances, only native Outlook will suffice. Using the NS Series Security Appliance in conjunction with ISA Server 2004's secure RPC publishing and filtering, users access Exchange Server without the need to connect through a VPN and wading through multiple logon screens. Using ISA Server's unique Forms Based Authentication, credentials are checked in a single login without allowing unauthorized users to the front end Exchange servers. Proxy of the front end Exchange server greatly enhances security, resulting in its ease of use for users and administrators and high ROI without compromise in Exchange defense.

Outlook Mobile Access

Outlook Mobile Access is designed to render select Exchange content stores to handheld mobile devices. Best security practices dictate that all mobile devices use Secure Sockets Layer encryption (SSL) to protect HTTP sessions from end to end. Using the NS Series Security Appliance for OMA provides the benefits of the HTTP Security Filter which performs stateful application layer inspection of the communications between the OMA and ActiveSync clients and Exchange Server. SSL bridging feature also prevents exploits from being hidden in an SSL tunnel - a major shortcoming for other "hardware" firewalls on the market.

Active Sync

Exchange Server ActiveSync (EAS) synchronizes Exchange data to a mobile device. This functionality works with mobile devices that run versions of Outlook. These are Microsoft Windows powered devices like the Power PC, Pocket PC Phone Edition as well as other Windows-based smart phones. EAS can perform both on-demand and scheduled synchronization to allow access to all folders in the mailbox. EAS provides access to message attachments allowing the server to send periodic "always up-to-date" (AUTD) notifications originating from the Exchange Server to the wireless carrier gateway. The NS Series appliances ensure that these communications are done securely through ISA 2004's advanced firewall features, allowing unfettered remote access regardless of the endpoint communication device.

SMTP, POP3, IMAP, NNTP

One of the ways to access your Exchange server without full Outlook configurations is through the use of the e-mail messaging thin client such as Outlook Express. However, Outlook Express uses POP3 and SMTP communications which can compromise an Exchange server through the use of buffer overflows. The NS Series Security Appliance's unique SMTP and POP3 filters protect mail servers, inspecting all content to block command sequences that disrupt services between remote clients and Exchange.

VPN Networking

The NS Series Security Appliance significantly enhances VPN components included with Windows 2000 and Windows Server 2003 routing and remote access services (RRAS). Administrators can enable, configure and manage the VPN server directly from ISA 2004's firewall management console without the back-and-forth between multiple Microsoft Management Consoles (MMC). Firewall policies can be applied to VPN client connections as well as VPN site-to-site connections. The NS Series also utilizes ISA 2004 VPN quarantine, SecureNAT client support, support for VPN Tunnel Mode using IPSec, the publishing of PPTP VPN servers and the monitoring of VPN client connections. The NS Series' VPN server and Gateway features make it the most powerful, co-located VPN and firewall solutions on the market today.

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