

Securing Exchange With ISA Server 2004

Jonathan Hassell 2004-10-19

You might be thinking that running Exchange Server 2003 on the Internet itself is tempting, however you should be concerned with the security issues in doing so -- there are many attacks and automated scripts in the hands of hackers that pound on Exchange machines and attempt to compromise them. Outlook Web Access can be a useful option, however there are security issues with deploying this as well. And the fact remains that sometimes you absolutely need to provide full access for Microsoft Outlook clients, and the Web Access front-end just won't cut it.

This article will highlight the security issues involved with providing Outlook Web Access or full Outlook client connections over the Internet, and then discuss how Microsoft's new ISA Server 2004 can be configured to mitigate these threats. We'll start with Outlook Web Access (OWA) as the simplest solution.

Before we begin, however, please note that this article does not focus on securing the Exchange message transfer agent (MTA) itself, instead we will only look at how to secure remote access to Exchange services from a user's perspective.

Securing Outlook Web Access with ISA 2004

Some of your users might be able to get away with just using Outlook Web Access, the great tool that mimics Outlook's interface in a web browser, in lieu of the traditional Outlook client. OWA is good for Exchange organizations because web browsers are prevalent, affording your users more opportunities to check e-mail while they're away from their desk. As well, the user interface is familiar to your users, so there is very little learning curve involved.

However, there are qualms about Outlook Web Access in regards to security. How might one go about securing it? OWA can use HTTPS [[ref 1](#)] -- the secure, tunneled version of the HTTP protocol -- but it lacks any intrusion detection features. More problematically, all versions of OWA but the most recent one do not include a session timeout feature, so clients will remain logged into their OWA session until they click the logout button. Picture an airport Internet kiosk, and your chief financial officer checking his e-mail through OWA. He simply closes the browser when he is finished, but the clever information spy will then re-open the browser after he has walked away, revisit the previous site, and gain access to a very sensitive and important e-mail account. That is certainly a very bad situation, and it's happened before.

The need for ISA 2004

To make OWA secure, there are four things that an administrator, must do:

- Inspect all SSL traffic at the application layer to make sure the traffic is what it claims to be. This prevents a significant portion of today's attacks.
- Maintain wire privacy, as sensitive information is very often transmitted through e-mail.
- You need to enforce the HTTP and HTML standards to make sure that nefarious code doesn't sneak through via weaknesses in these protocols and standards.
- You want to block URL-based attacks by enforcing only known URLs. This protects you against attacks that request unusual actions, have a large number of characters, or are encoded using an alternate character set.

All in all, when you have this quadruple-layered security scenario protecting OWA, you can feel reasonably confident that data trusted to OWA's mechanisms is secure.

Enter ISA Server 2004, which can help you enforce the above requirements. When you put ISA Server in front of your OWA front-end server or servers, there are numerous benefits. The ISA Server in effect becomes the bastion host, terminating all connections with its Web Proxy feature, decrypting HTTPS to inspect the content of the packets transmitted through the machine, enforcing known-URL access with URLScan, and ultimately re-encrypting everything for transmission to the OWA server, living safely behind the ISA frontline machine.

Pre-authentication of connections

ISA 2004 also provides another benefit: pre-authentication of connections. Here's how that works: the ISA Server actually hosts the forms that a user is used to seeing -- such as the login screen. This screen queries the user for her credentials, and once the user enters them into the form, ISA verifies them against Active Directory. Note that RADIUS is also supported, so even ISA machines that do not trust or are not members of a domain can do this pre-authentication. ISA then takes the result of that verification and embeds the credentials into the actual HTTP headers of the packets that it forwards to the front-end OWA server, so the user doesn't get a second prompt. In effect, the ISA server is vetting your users with an actual OWA form, ensuring they are who they say they are, and actually authenticating them at the perimeter of your network, before the packets ever hit the OWA server.

Figure 1, below, shows an overview of this process.

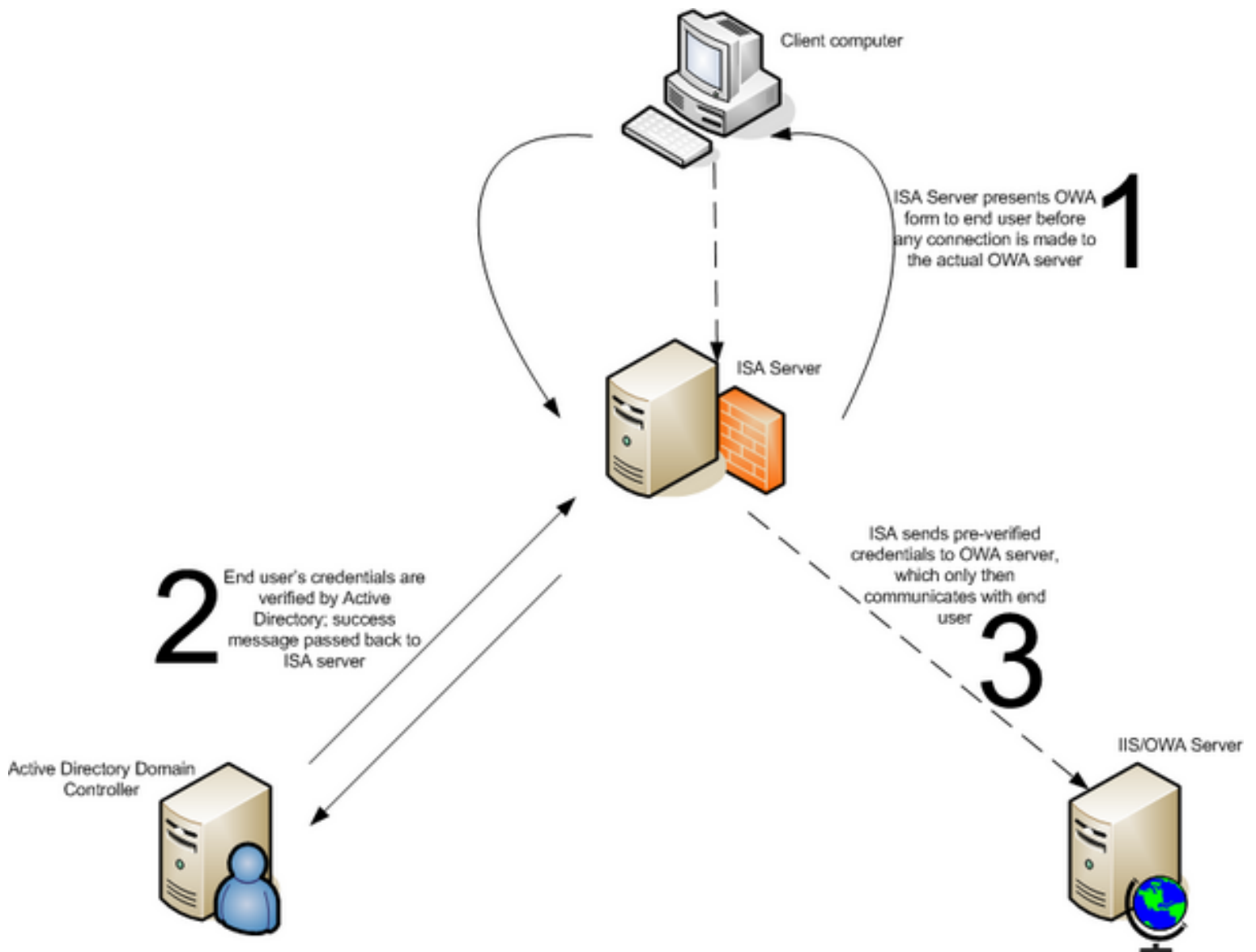


Figure 1: Forms-based authentication with ISA Server 2004 and OWA

More information on how you would configure this environment is available as a step-by-step document from Microsoft. [ref 2] Tom Shinder also has a great reference for configuring firewall publishing rules to allow external access to OWA sites at ISAServer.org. [ref 3]

Issues with the Outlook Client and VPN

VPN clients, present in all versions of Windows, are the typical choice for anyone needing to provide full Outlook client functionality to users across the Internet. However, VPN security leaves a lot to be desired, at least out of the box: while PPTP can be made secure, doing so requires an extensive knowledge of both the machines running the VPN software (a feat not always possible when you're dealing with your users' home machines) and a deep familiarity with encryption techniques and settings. Of course, there are also logistical hurdles you'll jump through when using a VPN -- they simply won't work in some public locations because of firewalls blocking the

needed ports, there are problems with using IPsec and L2TP across the Internet because of packet fragmentation issues, and other issues. And finally, while VPNs are useful tools to connect remote clients to corporate networks, they are less useful for connecting from a corporate network to an application service provider (ASP) that might be running your Exchange servers for you.

So therein lies the problem: how does one provide secure access to an Exchange server for remote users while not making those users jump through hoops to get access to their groupware application? The best answer to this may be to deploy a machine running Microsoft Internet Security and Acceleration Server 2004.

Securing the Outlook client with Exchange 2003 RPC and ISA 2004

The grim reality is that people have grown at best accustomed, and at worst absolutely dependent, on full Outlook client functionality. For example, suppose your corporation has standardized on LookOut, the popular Outlook search plug-in, or perhaps you have a third-party calendaring and agenda plug-in. You might also require the ability to synchronize your mailbox with a handheld PDA-like device, or your users might need Outlook 2003's ability to work seamlessly offline, with full Outlook functionality even when not connected to an Exchange server. Your front-line customer service users may depend heavily on custom functionality offered by client-side rules, or your organization may require its users to take advantage of a standard, business-wide address book.

Security features in Exchange 2003

Exchange 2003 itself has made great strides in this area, enabling new functionality called RPC-over-HTTP. RPC-over-HTTP is a beneficial addition to the product, because it allows RPC requests to be encapsulated in the HTTP protocol, for which most firewalls are already configured and allow access. RPC-over-HTTP depends on an element of Exchange 2003 called the RPC proxy, an ISAPI extension running in IIS (actually on a front-end Outlook Web Access server) that sets up an RPC session after authentication. Essentially, the Outlook client connects to this filter using RPC-over-HTTP, and the filter terminates the "over-HTTP" portion of the connection, takes out the RPC requests, and passes them back to the Exchange server.

However, RPC-over-HTTP isn't a panacea. It only supports basic HTTP authentication, so you need to make sure such the HTTP connection uses SSL. Also, there is no support for SecurID, and the

limitation here is two-fold. For one, there is no dialog within Outlook 2003 to ask for the SecurID PIN from the user's device. And secondly, Exchange has no built-in, direct ability to proxy authentication requests to an RSA ACE server and not to Active Directory. RADIUS authentication is also not possible with RPC-over-HTTP, nor is the use of client certificates in most cases. So, while RPC-over-HTTP solves some configuration problems and some legitimate security problems, there remain other issues to address.

ISA 2004 and the Exchange RPC Filter

ISA 2004 comes bundled with the Exchange RPC Filter, which takes the good parts of the RPC Proxy element that is included with the raw Exchange 2003 product to allow RPC-over-HTTP connections, and then marries them with a certain intelligence about how Exchange does its business. The Exchange RPC filter is programmed to know how Exchange RPC connections are established and what the proper format for that protocol is. It also allows only Exchange RPC UUIDs to be transmitted, all the while enforcing client authentication and requiring encryption.

Here's how it works:

- The client connects to the Exchange RPC filter's quasi-portmapper. This piece of the puzzle really isn't a portmapper -- it just acts like one, which reduces the attack surface by only responding to requests for Exchange-based RPC.
- Once the connection is established, the ISA Server returns the filter's Exchange RPC port numbers. Remember, the client is connecting to the filter which then uses the RPC element proxy in Exchange 2003 itself, so the client never directly touches the Exchange server during this stage.
- The client, filled with knowledge about the location of RPC ports, logs onto Exchange. During this process, Exchange refers the logon to Active Directory, which makes the final decision on whether the user is authenticated or not.
- The RPC filter on the ISA Server is monitoring this process the whole time, waiting for the approval from AD that the user is valid. Once it sees that approval, the filter makes sure that the connection is using encryption (if you specify that you want to require it), and then the client sees his mailbox open.

It's also important to note that the entire process just outlined is transparent from the client's perspective. They will see a username and password prompt when they open Outlook and they are away from the corporate network, but once the user enters those credentials, he will see an approximately five second delay and then his mailbox will open. Thus, this solution passes the

first litmus test of all security solutions -- make it easy for the user to do things securely.

This solution also protects you from various RPC-based attacks. For example, the ISA RPC filter is immune from reconnaissance attacks and denial of service attacks against the RPC portmapper. All known attacks fail, but even if an attack were successfully able to penetrate the RPC filter, recall that Exchange is still protected since ISA works at the perimeter to vet your connections before they ever touch your Exchange server. This solution is also impervious to service attacks, mainly because such attacks require reconnaissance information that is unavailable. Also, the back end of this RPC filter connection, the ISA to Exchange Server part of the transmission, simply dies if the first part of the connection (the client to the ISA server) isn't correctly positioned or formatted.

How would you go about deploying this solution? Figure 2 shows an example network diagram, with a standalone ISA 2004 machine in the de-militarized zone (DMZ) protecting the back-end Exchange servers and Active Directory. The ISA Server provides the forms-based authentication for OWA that I discussed in the previous section, and also provides secure RPC access for Outlook clients as well.

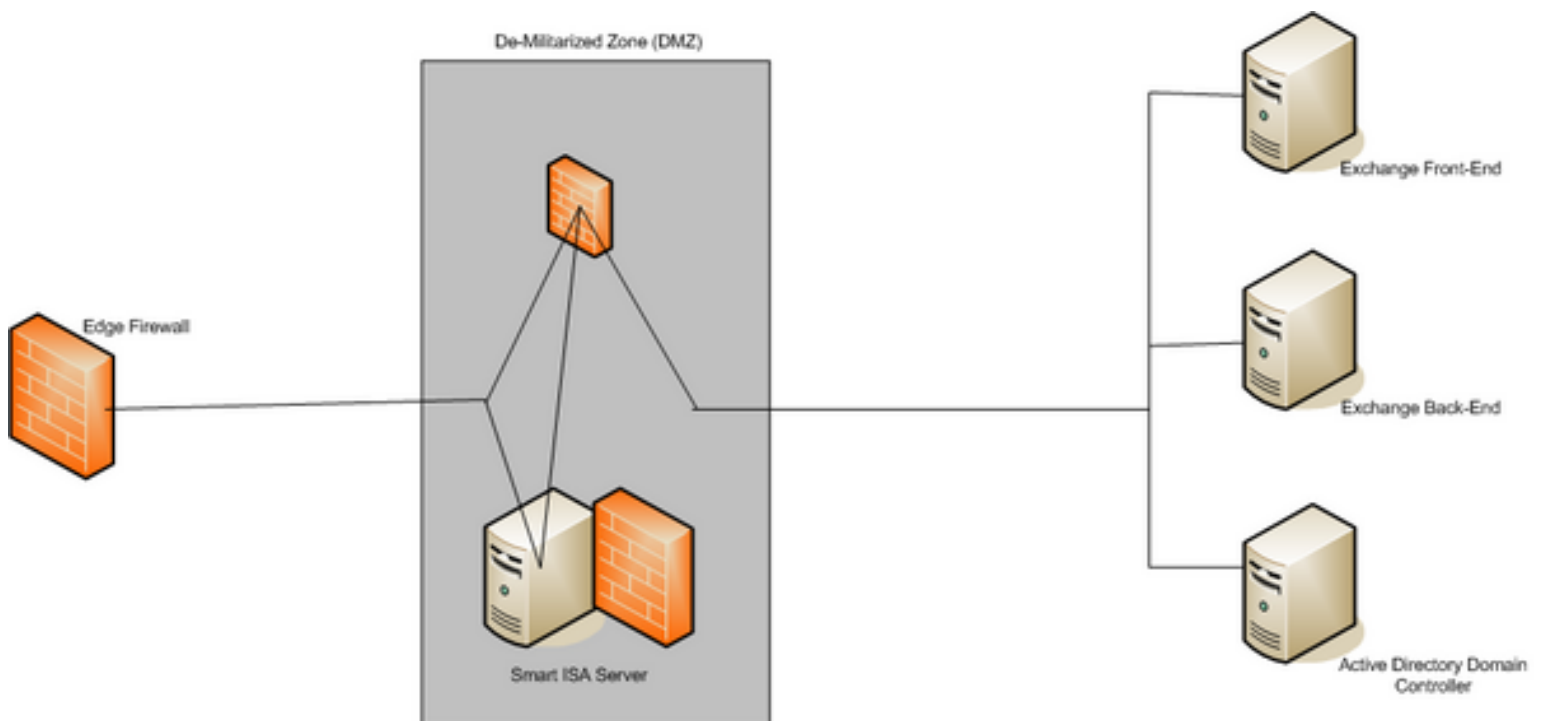


Figure 2: An example deployment of ISA Server 2004 to protect public-facing Exchange services

Microsoft has a detailed reference to deploying ISA Server 2004 in front of Exchange front-end and back-end servers on their website [ref 4].

Conclusion

Deploying Exchange Server 2003 on the Internet to support remote users can be a daunting task. However, Microsoft has supplied logic within ISA Server 2004 that can intelligently protect and defend your Exchange deployment against attacks, both for users of Outlook Web Access and for other users that require RPC-based access for full Outlook client functionality.

The links provided in the Further Reading section can help you with your implementation plan. Additionally, if you are interested in learning more in-depth information about the ISA Server 2004 product itself, I recommend purchasing Tom Shinder's book, *ISA Server and Beyond*, available from Syngress [[ref 5](#)].

Further Reading

[[ref 1](#)] "[How to publish an SSL Web site by using SSL tunneling in ISA Server 2004](#)" (Microsoft.com)

[[ref 2](#)] "[How to publish a Microsoft Exchange server for Outlook Web Access in ISA Server 2004](#)" (Microsoft.com)

[[ref 3](#)] "[Publishing OWA Sites using ISA Firewall Web Publishing Rules \(2004\)](#)" (ISAServer.org)

[[ref 4](#)] "[Using ISA Server 2004 with Exchange Server 2003](#)" (Microsoft.com)

[[ref 5](#)] Dr. Tom Shinder's book, "[ISA Server and Beyond](#)" (Syngress)

About the author

[Jonathan Hassell](#) is an author and consultant specializing in Windows administration and security. He is the author of *Managing Windows Server 2003* and *RADIUS*, both published by O'Reilly & Associates, and *Hardening Windows*, published by Apress. He also holds periodic public seminars; see www.hardeningwin.com for details. He has written for *Windows & .NET Magazine* and *WindowsITSecurity.COM* and is a contributor to *PC Pro*, a leading computer magazine in the United Kingdom.

View [more articles](#) by Jonathan Hassell on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus