

By Thomas W Shinder MD, MVP

ISA Server 2004 is more than just a multilayer filtering firewall and Web caching server. It's also a secure remote access VPN server or VPN gateway. Why use ISA Server 2004 instead of other popular VPN solutions? Let's look at 10 reasons ISA Server may be the best VPN choice for your network.

1 Stateful packet and application layer inspection for all VPN connections

The MS Blast (Blaster) worm was a wake-up call for network and firewall administrators. Not only did it remind us that we need to keep our systems up to date (Microsoft had already released an update to prevent this exploit), but it also reminded us that we need to firewall all connections to the corporate network. Many network administrators thought they were protected from the Blaster worm by blocking incoming connections to the RPC endpoint mapper (TCP 135) from the Internet. Unfortunately, their networks were hit by Blaster from client systems connecting over the VPN channel to access Exchange. Their VPN servers did not perform both packet and application layer inspection on VPN client communications.

If an ISA firewall-based VPN server had been in place, the Blaster worm would have been blocked and Outlook RPC communications over the VPN link would still work. That's because the ISA firewall performs both stateful packet and application layer inspection of all VPN client connections. The result is that you have the same level of firewall protection on communications sourcing from VPN clients as you have against connections coming from the Internet.

2 Active Directory integration for user authentication

The ISA firewall's VPN server enables you to leverage your current Active Directory user database and group classifications to authenticate with the VPN server. Most organizations have already created a comprehensive Active Directory structure where users are placed in groups based on their level of access and authority. Unlike hardware firewalls that depend on a local user database to authenticate users or that depend on RADIUS or other remote user authentication protocols, the ISA firewall's VPN server reduces firewall management overhead by taking advantage of the company's existing authentication and identity management infrastructure.

In addition to using the current Active Directory infrastructure to support remote access VPN security, the ISA firewall's VPN server allows you to disassociate VPN administrator privileges from domain administrator privileges by letting you create ISA firewall groups based on Active Directory users and groups. This allows you to create access controls based on Active Directory users and groups or create your own ISA firewall groups based on existing users and groups in the Active Directory.

3 RADIUS user mapping for non-Active Directory users

Not all connections to the ISA firewall's VPN server will be from Windows clients using the Windows VPN client software. Non-Windows clients can connect as remote VPN access clients but must use RADIUS for authentication. In this case, you can use the ISA firewall's user mapping feature.

The ISA firewall's VPN server allows you to map non-Windows users (those users unable to log on from a Windows operating system) to Windows accounts. When user mapping is enabled, you can create and enforce any firewall policy rules that apply to users. With user mapping enabled, when a RADIUS user presents credentials, the username and domain are mapped to the same username and domain, and the user is authenticated as if Windows integrated credentials had been presented. No other VPN server in the ISA firewall's class provides this level of access control for non-Windows clients when connecting to an Active Directory network over a VPN link.

4 User- and group-based access control for VPN clients

Typical remote access VPN servers allow users to connect to the corporate network from anywhere in the world. Once the user connects to the remote access VPN server, that user has access to any server, using any protocol. The only limitations to access are those configured on the server or workstation on the corporate network. The VPN server itself doesn't limit connections and treats all VPN clients the same way it would treat a connection from a client system locally connected to the corporate network.

In contrast to traditional hardware remote access VPN servers, the ISA firewall's VPN server enables you to control access based on user logon credentials. You can then create firewall policies that allow specific users or groups of users to access resources they require. Do all users need access to the SQL servers? Do all users need access to Exchange Server? Do all users need access to the development file server? The ISA firewall's VPN server enables you to lock down, on a per-user or per-group basis, what VPN users can do on the corporate network.

5 Granular access control over what VPN users can access on the corporate network

Unlike the typical hardware VPN server, the ISA firewall's VPN server enables you to easily control what users access once they connect to the corporate network through the VPN link. You can use the ISA firewall's per-user/per-group access controls and extend those to determine which resources users can access once connected. You can control connections based on:

- The IP address of the destination server.
- The name of the destination server.
- The protocol used to connect to the destination server.
- The time of day when the connection attempt is established.
- The user account attempting the connection to the destination server.

These finely-tuned access controls make it possible to easily configure a firewall rule set that allows VPN users to connect to only the resources they need access to in order to get their work done.

6 Enforce corporate firewall policy on VPN users' Internet access

One problem with most remote access VPN servers is lack of control over split tunneling. Split tunneling takes place when you allow remote access VPN clients to connect to the Internet via the already established network connection (not the VPN link) and at the same time connect to the corporate network over the remote access VPN connection. Split tunneling can pose a significant security risk because intruders on the Internet can route exploits from the Internet to the corporate network through the VPN link.

The ISA firewall's VPN server allows your VPN users to connect to the Internet while keeping split tunneling disabled. In addition, you can enforce corporate security and Internet access policy on VPN clients in the same way you enforce it on clients directly connected to the corporate network. The ISA firewall's VPN server ensures that VPN clients have the same strong access controls imposed on them as those applied to network clients connected locally to the corporate network.

7 Ensure VPN remote access client system health using remote access quarantine services

Remote access VPN client systems are different from those that typically connect to your corporate network. Your local corporate devices are managed devices, and you have some level of control over the security configuration of those devices that enables you to lower the risk of those machines being compromised by viruses and worms. This isn't the case for remote access VPN clients such as users' home computers or privately owned laptops.

The ISA firewall's VPN server supports remote access VPN client quarantine. Remote access VPN client quarantine enables you to check the software environment of the remote access VPN client and pre-qualify the host before allowing it to connect to the corporate network. In other words, you can require that the client have current security updates and service packs installed, antivirus software running, and personal firewalls enabled. You even have the option to remediate (update) the client so that problems with the remote access VPN client software environment are automatically fixed.

8

Comprehensive reporting on user activity when connected to the ISA VPN server

The typical remote access VPN server can record the IP address of the user logged into the VPN server. Some of them even record the activity related to that IP address. But very few remote access VPN servers can record in their log files what each user, regardless of the IP address that user might be using at any point in time, is doing when connected to the VPN server.

The ISA firewall's remote access VPN server logs all connections made through the VPN link and associates the user name with all activity generated by the VPN user. You can then use the ISA firewall's logging and reporting facilities to get comprehensive information on what your VPN users are doing or what a particular user is doing when connected via the VPN channel. You'll find that users accustomed to typical hardware firewall VPN servers and split tunneling will be surprised when you query them on their activities when connected to an ISA firewall-based VPN remote access server.

9

Simple licensing model that scales with your organization

Most hardware VPN servers have licensing requirements based on the number of users you want to allow to connect to the VPN server. This might be the total number of potential remote access VPN clients or a limit on the number of simultaneous VPN connections. In contrast, the ISA firewall's VPN server licensing is very simple:

- No Windows Client Access Licenses (CALs) are required for VPN or firewall connections.
- ISA Server 2004 Standard Edition supports up to 1,000 concurrent remote access VPN connections.
- ISA Server 2004 Enterprise Edition supports an unlimited number of VPN connections.

Another benefit is that you can use the VPN client software that's included with all versions of Windows and there is no additional charge for the remote access VPN quarantine feature, which is something you often have to pay a substantial premium for when using traditional remote access VPN servers.

10

Easy site-to-site VPN connectivity supporting EAP authentication

Site-to-site VPN connections enable you to connect entire networks to one another over the Internet. This can be a significant cost savings because you can potentially drop your dedicated WAN links and replace them with site-to-site VPN connections. However, the problem with typical hardware VPN server solutions for site-to-site VPNs is that they use IPsec tunnel mode connections and pre-shared keys, which are open to well-publicized "man-in-the-middle" attacks.

The ISA firewall's VPN server enables you to create site-to-site VPN links using certificate-based machine authentication. Certificate-based authentication is much more secure than pre-shared keys and much less susceptible to man-in-the-middle attacks. However, the ISA firewall's site-to-site VPN security doesn't stop at certificate-based machine authentication—you can also configure the remote access VPN gateways to require *user certificate authentication*. This provides a second layer of security that makes it virtually impossible for an intruder to hijack the site-to-site VPN link between two ISA firewall-based VPN gateways.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["10 things you should know about securing DNS"](#) (TechRepublic article)
- ["Twenty ISA Server 2004 tips to fine-tune your firewall"](#) (TechProGuild article)
- ["Optimizing ISA Server 2004 Firewall Policies"](#) (TechProGuild article)

Version history

Version: 1.0

Published: November 15, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team