

ISA Server Installation Basics

By Glenn Barnas – InnoTech Consulting Group

The installation of ISA Server can be complex and mysterious for first time users. This document will attempt to help get you running in a basic configuration, explaining the steps as we go. The configuration presented is appropriate for a lab or small office environment, but the concepts can easily be adjusted to fit any size organization. We'll assume that you have a basic AD infrastructure available, including DNS.

To Domain or Not to Domain?

Really, it isn't a question you should even be asking! Every ISA server should be a member of your user domain. There are more reasons to do this than I want to explain (and there's a great article on www.isaserver.org that explains this in great detail), but there are two compelling reasons that I will discuss here.

1. Joining a domain after ISA Server installation is difficult. The ISA installation wizard will detect domain membership and automatically define policies (access rules, really, but specific to ISA) to permit all of the required access to the domain. If you install on a standalone server and later decide to join the domain, you will need to create / edit all of these policies. While this is certainly possible, it's often easier to export your configuration, uninstall ISA, join the domain, and finally reinstall ISA and restore the configuration.
2. When ISA Server is a member of the primary user domain, it can apply rules based on AD users and groups. This will permit you to define rules for specific users or groups of users.

Prepare the Server

You should fully prepare your server *before* you install ISA Server. Once ISA is installed and running, it blocks access to everything until you define some fundamental rules. Here are the things you should consider doing before you begin the ISA installation:

- Obviously, install the O/S. ISA server will run on 64-bit hardware, but *will not* run on a 64-bit operating system, so be sure you have a 32-bit O/S installed! (One of the reasons that 64-bit versions are not supported is that ISA replaces the network subsystem. With the network subsystem under the control of ISA, it's impossible for a Windows network vulnerability to be exploited.)
- Go to Windows Update and download/install all patches and updates. I recommend this even if you use WSUS or some other patching process. Remember, this is a firewall and should be fully patched before it is permanently placed on the public network!
- Install any diagnostic or administrative support tools. I usually install a set of tools to aid in system diagnostics, including utilities like the PSTools suite and the KiXtart scripting engine.
- Configure disk and paging file settings based on your organization's best practices. I usually create a 12-16G C: drive for the O/S, D: for applications, and a 4.5 to 9G X: drive for a paging file. Unless you are running an Enterprise version of Windows, 4.5G is enough for your paging file.

drive. Create a small paging file on C: for mini-dumps, and the large page file on the dedicated drive. Set the minimum/maximum size values identically to minimize fragmentation.

- Configure your network interfaces in Network Properties:
 - Identify the physical ports for each interface defined. Plug them into a switch, one at a time, and note which interface shows “connected”. Label the interfaces on the computer – I like to draw a simple diagram in Paint with a rectangle to represent the back of the computer and a small box for each NIC port. Number the NIC port boxes, and create a table that relates the numbers to the use for each port.
 - As you identify each of the ports in Network Properties, rename them so you can easily identify them moving forward. “Wireless LAN” is so much better than “Local Area Adapter 3”! Use short, descriptive names. ISA standards are “Internal” for all trusted networks and “External” for the Internet. Avoid using the term “Internet” for your external port as it is too easy to confuse “Internal” and “Internet”, with potentially disastrous results. I prefer names like “Perimeter LAN” for the DMZ and “Wireless LAN” (or “WLAN”) for a secure wireless segment.
 - Configure the IP settings on each interface. Routers are often the first or last address in the subnet – follow your organization’s practices, but try to assign each interface the same host ID. If you don’t have any specific practices defined, assign the first available IP address to each interface that is statically configured.
 - Internal – Define the IP address, netmask, and DNS servers only. Leave the Gateway blank. The DNS server(s) should point to your internal AD-DNS servers, just like any other server. Due to extreme overuse, I generally avoid the lower ranges of 192.168 public networks. If you use this public network address for your protected networks, I’d suggest starting with the 192.168.8.0 network.

As you configure the remaining interfaces, disable all network protocols, clients, and services except TCP/IP. Note that you may not be able to disable certain hardware monitoring and teaming services – this is OK. You do not want any Windows File Sharing components active on the following interfaces.

- External – This is often a DHCP interface, so simply enable DHCP for the network address. Do not enable DHCP for the DNS servers – choose “use these DNS servers”, but leave the entry blank. If you are using a static address, define the IP Address, Netmask, and Gateway values. If ISA is to be an edge firewall, this will likely need to be a public IP Address.
- Perimeter (if used) – Define IP Address and Netmask values only. I like to use higher network ranges, such as 192.168.255.0, so it’s clear to any administrator that this network is “special”. Leave this cable disconnected until later.
- Wireless (if used) – This configuration will permit a secure wireless subnet. Many organizations will use methods such as preconfigured SSID and WPA2 encryption to secure a wireless access point connected directly to the Internal

network. This can make it difficult to allow “guests” to connect to the wireless network for basic Internet access. Defining a Wireless network to ISA will allow an “open” network to be defined, permitting basic Internet access, but requiring VPN connections to access the Internal LAN. Configuration of this subnet will be documented separately. Suffice to say that you will need to specify only an IP Address and Netmask on this interface.

- Connect to the Internal network and test connectivity.
- Join the domain! Log off and back on with domain credentials to verify the connections.

Installing ISA Server Software

You are now ready to install the ISA Server software. There are two versions of ISA Server software – Standard and Enterprise. If you are running the Enterprise version, there are also two components to consider – the firewall and the configuration storage. If you expect to have more than one ISA server, I’d strongly recommend that you first deploy a central Configuration Storage Server (CSS). With it, you can maintain configuration settings for all of your ISA firewalls in one place. The configurations updates are synchronized between the CSS and ISA firewalls every few seconds.

Regardless of which version you will be installing, you should install the ISA Management Client on your workstation. If you use a Terminal Server connection to install ISA, the workstation you use will automatically be added to the list of “Authorized Management Computers” during the installation. Choose your remote installation client wisely!

I won’t go into the detail of the ISA installation, as there are plenty of documents that already discuss that. Further, the installation wizard is pretty straightforward. Just make sure you only define the External and Internal interfaces during the installation, even if you have Perimeter or Wireless subnets. When prompted to select a configuration template, choose “Edge Firewall”. The templates configure specific predefined access rules, which might be appropriate in some situations. I prefer the Edge Firewall template, since it has only a default Deny All rule. This allows me to be very specific in the configuration that I define.

When the installation is complete, I strongly recommend that you follow the prompt to connect to Windows Update again and download/install any ISA patches. There might also be O/S patches that will be applied only if ISA is detected, which would not have been applied earlier. Now would be a good time to reconnect the cable to the External network port! *Caveat* – You might need to configure the External interface with a public DNS server temporarily, since outbound access from your internal DNS servers will be blocked until you define a rule permitting it. Remove this definition when the update completes.

Configuring Basic Rules

If you try to connect to the Internet from either the ISA server or any protected client, you will find that access is denied. We will need to perform some basic configuration steps to permit access.

DNS Servers

The DNS servers must be able to perform queries to other DNS servers on the Internet. The configuration process is two-fold. You want to limit access to your DNS servers only, and you want to permit outbound DNS queries.

- Define a Computer Set for your DNS servers. The computers in this set will be permitted to make outbound DNS queries.
 - Select “Firewall Policy” from the ISA management tree. Expand the right-side toolbar.
 - Select the “Toolbox” tab.
 - Select the “Network Objects” bar.
 - Click New, select “Computer Set”.
 - Enter “DNS Servers” in the name field, add “Computers permitted to make DNS queries” in the description field.
 - Click Add, choose Computer, and define your DNS server. Repeat for each DNS server that will make outbound queries.
 - Click OK to complete the definition.

- Define an access rule to permit DNS traffic from the DNS Servers computer set:
 - Select the “Tasks” tab on the right-side toolbar.
 - Click the “Create Access Rule” link.
 - The access rule name is “Permit DNS Queries to External”. Click Next
 - This is a “permit” rule, so select “Allow” and click Next.
 - Verify that “Selected Protocols” is highlighted and click Add.
 - Expand the Infrastructure group, select and add DNS. Click Close, then Next
 - Define the sources of the DNS traffic – Expand “Computer Sets”, select and add “DNS Servers”. Click Close, then Next.
 - These servers must make queries to the Internet. On the Destinations screen, click Add, expand Networks, select and add “External”. Click Close, then Next.
 - This rule will not apply to specific users – click Next to permit all users.
 - Click Finish to complete the definition.

- Click Apply, and OK to save the changes.

You should be able to perform a simple test at this point. From a workstation on the protected network, perform an nslookup of a domain. You should try to use a domain that isn’t in your DNS server’s cache, so you can verify the connection to an external source. For example,

```

Nslookup ibm.com

Server:  dns.mydomain.lan
Address:  192.168.0.8:53

```

Name: ibm.com
Addresses: 129.42.17.103, 129.42.18.103, 129.42.16.103

Note that it does not say “Non-authoritative answer”, which would indicate that your DNS server had cached an earlier query.

Internet Access

The next rule will be defined to permit basic Internet access from the protected networks.

- Define an access rule to permit Internet traffic from “All Protected Networks:
 - Select the “Tasks” tab on the right-side toolbar.
 - Click the “Create Access Rule” link.
 - The access rule name is “Permit Internet Access”. Click Next
 - This is a “permit” rule, so select “Allow” and click Next.
 - Verify that “Selected Protocols” is highlighted and click Add.
 - Expand the Common Protocols group, select and add HTTP, HTTPS, FTP, POP3, SMTP. Click Close, then Next
 - Define the sources of the Internet traffic – Expand “Network Sets”, select and add “All Protected Networks”. Click Close, then Next.
 - On the Destinations screen, click Add, expand Networks, select and add “External”. Click Close, then Next.
 - This rule will not apply to specific users – click Next to permit all users.
 - Click Finish to complete the definition.
- Click Apply, and OK to save the changes.

Your test workstation should now be able to browse web sites on the Internet.

Allow NTP Time Synchronization

The local PDC Emulator and select other network devices must be able to reach an external time server to properly synchronize time. Most network devices can be pointed to your domain controllers, as long as the DCs are configured to use NTP protocol. Some network devices, however, can only obtain time from well-known external time sources. Following a procedure similar to how DNS access was defined, we need to create a Computer Set for “NTP Clients”, and a rule to “Permit NTP to External”.

I won’t repeat the detailed instructions in detail in the following rule definitions unless there is a significant change, or additional detail is required.

- Define a Computer Set called “NTP Clients”
 - Add the PDC Emulator to this set

- Add any network device that supports NTP but does not permit definition of the NTP server to this list. Many Linksys and DLink wireless routers fall into this category.
- Define an Allow rule called “Permit NTP to External”
 - Add the “NTP (udp)” protocol from the Infrastructure group
 - Define the “NTP Clients” computer set as the traffic source
 - Define “External” as the destination network

If you add network devices or secondary time servers in the future, simply add them to the “NTP Clients” computer set, and they will be permitted access.

Allow Instant Messenger Access

I define a separate rule for IM access because it is one of the few rules that might be applied to specific users or groups. Many organizations do not permit unrestricted IM access, so one or more IM rules might be required in those situations. In our simple configuration, we will define a single rule that allows access to all IM clients. Feel free to modify the choices here to suit your needs.

ISA has protocols defined for MSN and AIM, but not for others such as Yahoo IM. If you need to permit these protocols, you must define them yourself.

- Add other IM protocols, as required.
 - On the Toolbox tab of the Right-side menu bar, select Protocols, then click New/Protocol.
 - Enter a descriptive name (ie: Y! Instant Messenger)
 - Add a port definition. For Yahoo IM, the start and end port is “5050”. No secondary connections are needed.
- Define an Allow rule called “Permit IM Protocols to External”. You could define separate access rules for each IM protocol if you prefer, or your requirements dictate.
 - Add the protocols for the IM services you use. Remember that the extra protocols you may have defined will be listed under “User Defined Protocols”
 - Define “All protected networks” as the traffic source.
 - Define “External” as the destination network.

Other Rules to Consider

The rules above are just the basics necessary for fundamental access. Here are some other rules you might need to consider implementing.

VPN Access

Users inside the protected network, especially guest users, might need to utilize a VPN to connect to their “home” network. Other users might need to make VPN connections into customer or vendor networks. This is another case where a user-specific rule might be appropriate.

Create a rule that permits use of VPN protocols from the Protected Networks to External. If you need to restrict access to this rule, consider creating an AD group called “Third-Party VPN Users”, and restricting the access rule to that user group.

Restricted Sites

Company policy might forbid access to certain web sites, or sites with specific content. While there are many (expensive) products that do an excellent job of this, ISA can provide similar functionality if you are willing to perform manual updates of the blacklisted sites.

Create a Network Objects “Domain Name Set” called “Blocked Domains”. Add any domain you wish to block to this set, using a “*.domain.com” format.

Create a Network Objects “URL Set” called “Blocked URLs”. Add to this any specific URL you wish to block. For example, you might wish to allow “www.yahoo.com” but block “personals.yahoo.com”.

Define a Deny rule called “Deny Blocked Domains and URLs”. Define “All Outbound Traffic” in the protocols tab, “All Protected Networks” as the source, and add the “Blocked Domains” and “Blocked URLs” sets to the destination. This is another situation where you might want to create an AD group called “Restricted Users” and apply this rule to that user group.

Summary

This should provide you with a basic, operating ISA server configuration. Look for other how-to documents that will discuss specific configurations, such as

- Publishing an SSH server
- Configuring a secure wireless segment
- Configuring VOIP access
- Creating a Reverse Application Proxy

One of the best web resources for ISA is www.isaserver.org. It has a wealth of how-to documents, tutorials, as well as interactive discussion forums.