

## DEPLOYING ISA SERVER 2000 WITH ANOTHER FIREWALL

*Products: Internet Security & Acceleration (ISA) Server 2000; Cisco Secure PIX Firewall; WatchGuard Technologies Firebox*

### Overview

Most organizations have recognized the need for securing and controlling the traffic from the Internet into their internal network, and have deployed a firewall to accomplish that goal. In such environments, it may seem that Microsoft Internet Security & Acceleration (ISA) Server 2000 is redundant and unnecessary. However, there are scenarios in which the deployment of ISA Server 2000 in conjunction with an existing firewall can be very beneficial. This technical note describes some of these scenarios.

### More Information

There are two basic scenarios for deploying ISA Server 2000 with an existing firewall: one-armed or full firewall. These two basic scenarios are described below.

### One-Armed Deployment Scenarios

To avoid complexity, almost all of these scenarios deploy ISA Server 2000 in a “one armed” configuration, i.e., with a single network interface card (NIC). The diagram below, Figure 1, provides a general idea of the type of network layout involved in such a configuration.

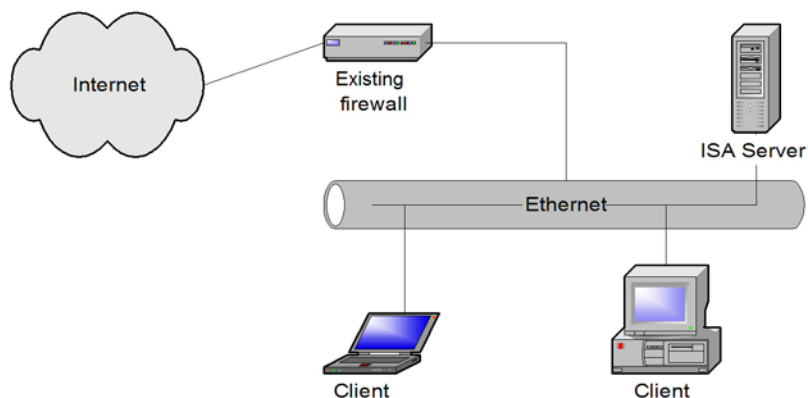


Figure 1. Typical One-Armed ISA Deployment

This configuration supports only ISA's proxying and caching functionality, but given that ISA is being deployed as a supplement to an existing firewall that already provides packet filtering, application proxying, and/or stateful inspection capabilities, this is not a drawback.

Deploying ISA Server 2000 in a "one-armed" configuration offers a number of advantages over a firewall alone. Some of these advantages and how they can be utilized are described below.

### Improving Performance Through Caching

ISA Server offers not only firewall functionality through packet filters and application filters, but also offers caching services for HTTP requests. This caching is handled transparently for SecureNAT clients (clients referencing ISA Server as their default gateway when ISA is configured for IP routing) by automatically proxying the web requests from the client to the Internet and caching the responses. In environments where a firewall already exists such as the environment depicted in Figure 1, the ISA Server is not the client's default gateway. However, the caching functionality of ISA can still be utilized by configuring the client's web browser to use the Web Proxy service on the ISA Server.

By configuring the user's browser to proxy requests to <http://isaserver:8080> (where "isaserver" is the name of the ISA Server) or <http://w.x.y.z:8080> (where "w.x.y.z" is the IP address of the ISA Server), ISA's caching functionality can still be employed. The request will be sent from the client to the Web Proxy service on the ISA Server, which will then check the cache to see if the request can be served from the cache. If so, the content is served from the cache and the request never even hits the Internet connection. Otherwise, the ISA Server requests the data from the destination server, caches it, and returns the response to the originating client.

Active Directory Group Policy Objects (GPOs) can be deployed to automatically configure client web browsers to use the ISA Server as a web proxy. This eliminates the need to configure each computer or user for ISA Server manually, and has the added benefit that the settings will be enforced every time the GPO is refreshed (by default, every 90 minutes). No other software needs to be installed on the clients, and no changes are required to the firewall to support this configuration.

### Controlling Outbound Web Access

Along the same lines, enforcing proxy settings on the clients so that they must send their requests through the ISA Server also provides a method of controlling outbound web access. ISA Server's Site & Content rules allow for complete control over the sites that users visit, as well as the types of content that are downloaded from those sites. In addition, authentication can be required so that all users must authenticate through ISA Server (which uses Active Directory as its authentication database) before outbound web access is granted. Once outbound web authentication is activated, then access can be controlled on a per-user basis, so that UserA can browse the web but UserB cannot. (However, be aware that there are some limitations with using authentication on outbound web requests for certain types of clients.)

As with the previous scenario, no software needs to be installed on the client, and browser proxy settings can be enforced through an Active Directory GPO. No firewall changes are required, although a greater degree of control can be achieved by allowing outbound web access only from the ISA Server. This then further enforces that all web requests must go through the Web Proxy service on the ISA Server instead of directly to the Internet.

## Controlling Inbound Web Access Through Web Publishing Rules

When deployed with only a single NIC, ISA Server still supports the use of web publishing rules. Web publishing rules provide a way to “reverse proxy” internal web sites or web servers, making them accessible to the Internet. By using ISA Server in this fashion in conjunction with a more traditional firewall product, strong security advantages are gained.

Most firewalls in use today provide only packet filtering and/or stateful inspection capabilities, neither of which have the ability to fully peer into Hypertext Transfer Protocol (HTTP) requests (operating at ISO Layer 7) and make decisions on the information found therein. As a result, allowing TCP port 80 for HTTP through the firewall also allows all forms of malicious HTTP traffic. ISA Server, on the other hand, uses the Web Proxy service to fully decode the HTTP URL and then intelligently route the request to the appropriate internal server. This provides a much greater degree of control and security.

To support inbound web access via ISA in this kind of scenario, a couple of steps are required. These steps are described briefly below.

- First, configure the firewall to allow TCP port 80 (and TCP port 443 if SSL is required) only to the ISA Server and not to any other internal host. This ensures that the ISA Server handles all inbound web traffic.
- Second, configure the ISA Server with the appropriate policy elements (destination sets and web publishing rules) to direct the inbound traffic to the appropriate server. For example, a request to <http://www.company.com/exchange> could be directed to an Exchange 2000 server providing Outlook Web Access, and SSL could be enforced. However, a request for <http://www.company.com/> could be directed to an internal web site, and no SSL would be needed.

Once these steps are completed, external (Internet-based) users should be able to access internal web-based resources via the ISA Server.

## Full Firewall Deployment Scenarios

Of course, it is possible to deploy ISA Server 2000 as a full firewall even when another firewall already exists. This scenario is particularly attractive in situations where the existing firewall is a hardware-based firewall such as a Cisco PIX or a WatchGuard Firebox. (Other hardware-based firewalls would work, but this technical document only examines these two types.)

### Deployment with a Cisco PIX

Figure 2, below, shows a typical deployment scenario in which ISA Server 2000 is deployed in integrated mode along with a Cisco PIX. This configuration assumes that the public IP address space is sufficient enough to allow for additional subnetting to occur to support two subnets, shown as Subnet A and Subnet B in Figure 2. If that is not the case (i.e., the public address space is too small to support splitting it into two separate subnets), then the PIX can be deployed inside the ISA Server.

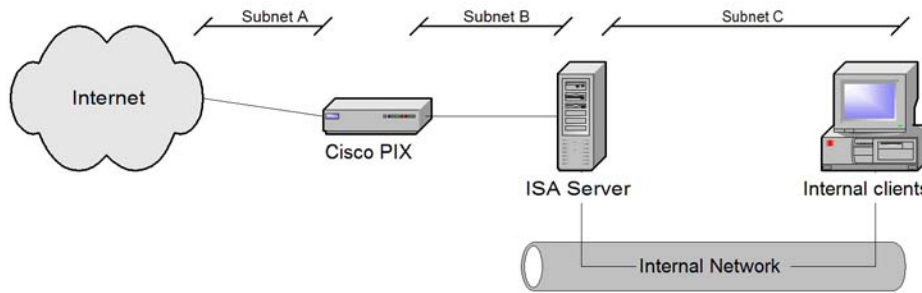


Figure 2. ISA Deployment with a Cisco PIX

In this scenario, each interface on the PIX firewall is attached to one of the two public subnets. Network address translation (NAT) is disabled on the PIX, allowing the ISA Server to handle all NAT functions (since NAT cannot be disabled on ISA Server).

Access lists (or conduits, for older Cisco PIX OS versions) are configured to allow traffic to the IP address or addresses attached to the external interface on the ISA Server, and the ISA Server is configured with the appropriate packet filters, server publishing rules, and web publishing rules to allow traffic to selected internal hosts as needed. All internal clients reference the ISA Server as their default gateway, and the ISA Server references the Cisco PIX firewall as its default gateway.

In this deployment scenario, all clients (regardless of configuration) will be able to take advantage of ISA’s caching functionality, thus improving performance and reducing utilization on the Internet connection. Administrators will also be able to use ISA’s Site & Content Rules to control access to Internet-bound resources and content.

**Deployment with a WatchGuard Firebox**

Figure 3, below, shows a typical deployment scenario in which ISA Server 2000 is deployed in integrated mode along with a WatchGuard Firebox. Variations on this scenario are very possible; for example, consider situations in which only a single public IP address is available for use. In that case, the Firebox could be deployed inside the ISA Server instead of outside.

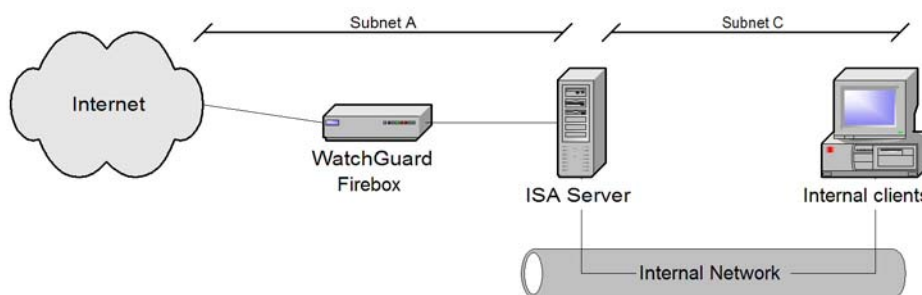


Figure 3. ISA Deployment with a WatchGuard Firebox

Figure 3 looks remarkably similar to Figure 2, but there is one key difference. Although NAT can be disabled on a Cisco PIX, each interface on the PIX must still attach to a different subnet. A WatchGuard Firebox, on the other hand, has the ability to run in “drop-in” mode, acting as a transparent bridge and physically separating the subnets without also requiring a logical separation of the subnets. In this scenario, the ISA Server performs all NAT, translating the

internal Subnet C addresses into a public IP address, and the WatchGuard Firebox simply passes those public addresses on to the Internet without further modification. This leaves Subnet A (the public subnet) intact and simplifies the network configuration without compromising security.

The WatchGuard Firebox is configured to allow traffic to the IP address or addresses attached to the external interface on the ISA Server, and the ISA Server is configured with the appropriate packet filters, server publishing rules, and web publishing rules to allow traffic to selected internal hosts as needed. All internal clients reference the ISA Server as their default gateway, and the ISA Server references the WatchGuard Firebox or the router beyond the Firebox (not shown in the diagram above) as its default gateway.

As in the deployment with a Cisco PIX, all clients (regardless of configuration) will be able to take advantage of ISA's caching functionality, thus improving performance and reducing utilization on the Internet connection. Administrators will also be able to use ISA's Site & Content Rules to control access to Internet-bound resources and content.

## **Other Notes**

For additional information on some of the differences and similarities between a Cisco PIX Firewall and a WatchGuard Firebox, see the technical note titled "Firewall Comparison: WatchGuard Firebox and Cisco PIX."

For additional information on specific uses of ISA Server's web publishing rules, refer to the following technical notes:

- Publishing Outlook Web Access via ISA Server
- Publishing SharePoint Portal Server via ISA Server

Both of these technical notes provide additional information on the creation and configuration of web publishing rules to support internal servers, and both are applicable in the scenarios described in this document.

## **Related Articles/Resources**

None

## **Legal Information**

This document was created by Mercurion Systems, Inc., and may be freely distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.