



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

FIREWALL COMPARISON: CISCO PIX AND ISA SERVER 2000

Products: Cisco Secure PIX Firewall; Microsoft Internet Security & Acceleration Server 2000

Overview

The Cisco Systems PIX firewall is a widely used and highly regarded firewall product. Microsoft offers Internet Security & Acceleration (ISA) Server 2000, a caching/firewall product that offers tight integration with Active Directory. The purpose of this document is not to provide a feature comparison of these two products, but instead to compare the products from a configuration and installation perspective. This should help engineers who are familiar with one product to find it easier to install the other product.

This document is organized according to sections. In each section, the differences between the Cisco PIX and ISA Server 2000 are described.

More Information

Subnetting

Both the Cisco PIX and ISA Server 2000 require that each interface on the firewall be connected to a separate IP subnet, as illustrated below in Figure 1. This requirements ensures that the firewall (PIX or ISA Server) is the only means by which traffic moves between the two subnets. In this regard, there are little, if any, differences between the two products. (This is in direct contrast with solutions such as the WatchGuard Firebox, which have the ability to operate in a “drop-in” mode that does not require subnetting the network. For a more detailed information on the WatchGuard Firebox, refer to the technical note titled “Firewall Comparison: WatchGuard Firebox and Cisco PIX.”)

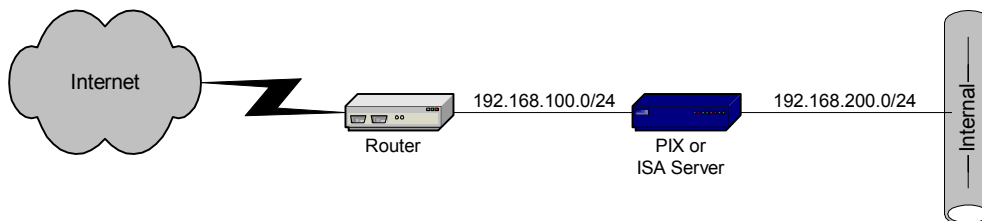


Figure 1. Typical PIX or ISA Server installation

Network Address Translation (NAT)

Both the Cisco PIX and ISA Server 2000 can use network address translation (NAT) to hide RFC 1918-compliant IP addresses and provide an additional layer of security. However, the implementation of NAT in each product is very different.

NAT operates in two directions: outbound and inbound.

Outbound NAT

The PIX allows outbound NAT to be controlled, i.e., enabled or disabled, based on a variety of criteria. One key example is the use of access lists to control NAT, as shown in the following excerpt of a PIX configuration:

```
access-list 101 permit ip 10.1.0.0 255.255.0.0 10.2.0.0 255.255.0.0
nat (inside) 0 access-list 101
nat (inside) 1 10.0.0.0 255.0.0.0
global (outside) 1 192.168.1.100 255.255.255.255
```

This access list specifies that packets originating on the 10.1.0.0/16 network and bound for the 10.2.0.0/16 network should not be translated, but all other packets from the 10.0.0.0/8 network should be translated as 192.168.1.100. (Cisco refers to this as Port Address Translation, or PAT; more commonly this is known as Network Address Port Translation, or NAPT. Other vendors refer to this as masquerading.)

Furthermore, the use of NAT IDs allows for even more complex configurations. Take the following excerpt of a PIX configuration.

```
access-list 11 permit 10.1.0.0 255.255.0.0
access-list 12 permit 10.2.0.0 255.255.0.0
nat (inside) 1 access-list 101
nat (inside) 2 access-list 102
global (outside) 1 192.168.1.100 255.255.255.255
global (outside) 2 192.168.1.200 255.255.255.255
```

In this example, NAT is controlled based on source IP address (access list 11 matches all source IP addresses in the 10.1.0.0/16 network, while access list 12 matches all IP addresses in the 10.2.0.0/16 network), and then translates them to different external addresses. Addresses matching access list 11 are translated to one external IP address, while addresses matching access list 12 are translated to a different external IP address. As you can see, this provides the network designer/engineer with a great deal of control over how and when NAT should be used.

ISA Server 2000, on the other hand, does not provide any real form of control or configuration over outbound NAT. All outbound traffic is masqueraded as the IP address of the ISA Server itself, and this functionality cannot be disabled or modified.

Inbound NAT

As with outbound NAT, the Cisco PIX offers explicit control over inbound NAT. The PIX OS `static` command is used to define static inbound NAT mappings. The following commands, for example, show several usages of the `static` command.

```
static (inside,outside) 192.168.1.1 10.1.1.1
static (dmz,outside) 192.168.1.2 10.1.2.1
static (inside,outside) tcp interface 80 10.1.1.3 80
```

The first command above creates a permanent static NAT mapping between the public address 192.168.1.1 and the private internal address 10.1.1.1 (which resides on the network attached to the interface named “inside”). The second command, on the other hand, creates a permanent static NAT mapping between the public address 192.168.1.2 and the private address of 10.1.2.1, which resides on the interface named “dmz”. Finally, the third command employs port redirection (also known as port forwarding) to forward TCP port 80 bound for the PIX’s external interface to the internal IP address 10.1.1.3 on port 80.

Note that defining the static NAT mapping does not automatically allow access to that mapping; that is controlled through an access list as described in the following section, “Access Control.”

ISA Server 2000, on the other hand, does not provide any form of static NAT mapping for inbound traffic. The mapping of external IP addresses and internal IP addresses is done on a case-by-case basis through the use of publishing rules, which associate a specific external socket (public IP address and port) with a specific internal socket (private IP address and port). Unlike the Cisco PIX, in which inbound NAT and access control are separate, ISA Server combines inbound NAT and access control in publishing rules. ISA’s publishing rules are described in more detail in the following section, “Access Control.”

Access Control

One of the most basic functions of a firewall is access control, i.e., controlling the movement of traffic into and out of a network. As with NAT, access control is defined both outbound and inbound, and the PIX and ISA Server 2000 each handle access control very differently.

Access Control on the PIX

For both outbound and inbound access control, the Cisco PIX employs access lists. These access lists are used to match traffic to be permitted or denied. With every access list, there is always an implicit “deny all” rule that is processed last. This means that any traffic not already explicitly allowed or denied will be denied by this hidden implicit deny all rule. In addition, it is important to note that access lists are only processed until the first match is found. The PIX will not apply the best match, it will apply the first match—and no additional rules in the access list will be processed once a match is found.

The following PIX configuration excerpt shows an access list created and applied to inbound traffic on the outside interface.

```
access-list acl_out permit icmp any any
access-list acl_out permit tcp any host 192.168.1.1 eq www
access-list acl_out permit tcp any host 192.168.1.2 eq pop3
access-list acl_out permit tcp any host 192.168.1.2 eq smtp
access-list acl_out permit tcp 192.168.2.0 255.255.255.0 host 192.168.1.2 eq 22
access-group acl_out in interface outside
```

This access list allows HTTP (TCP port 80) to the 192.168.1.1 external address from any source address, allows POP3 (TCP port 110) and SMTP (TCP port 25) to the 192.168.1.2 external address from any source address, and allows SSH (TCP port 22) to the 192.168.1.2 external address only from the 192.168.2.0/24 source network. The final command in the excerpt actually applies the access list to the interface.

This same mechanism is used for both inbound traffic (applied inbound to the outside interface) and outbound traffic (applied inbound to the inside interface). Keep in mind that an implicit “deny all” exists at the end of every access list.

Access Control with ISA Server

ISA Server, on the other hand, uses a variety of mechanisms to control access for inbound and outbound traffic. There are four primary components: packet filtering rules, protocol rules, site & content rules, and publishing rules.

The first three (packet filtering rules, protocol rules, and site & content rules) are used for both inbound and outbound traffic. The properties of the rule itself determine the direction (inbound or outbound) and disposition (permitted or denied). The Cisco PIX can easily match the packet filtering functionality and the protocol functionality through access lists. Additionally, the PIX access lists can duplicate the site functionality of ISA’s site & content rules; however, the content functionality cannot be duplicated on the PIX without additional third-party software.

ISA Server’s publishing rules, on the other hand, are used only for inbound traffic, and they can be compared to the `static` command on the PIX firewall combined with an access list. No inbound traffic is allowed without a publishing rule; i.e., all inbound traffic is automatically denied unless it matches a publishing rule. If packet filtering is also being employed, the appropriate packet filters must also be opened in order for the publishing rule to operate.

There are two types of publishing rules: server publishing rules and web publishing rules. Both types of rules operate at higher layers in the network stack; server publishing rules operate a Layer 4 (Transport layer) by working off the TCP or UDP port number. Web publishing rules operate at Layer 7 (Application layer) by working on the HTTP headers and URLs themselves.

Server publishing rules are used to make non-HTTP services available externally; essentially, a server publishing rule can be considered a port forwarding rule. For example, a server publishing rule could be created to publish an SSH server by forwarding SSH traffic (TCP port 22) from the ISA Server to the desired internal server. This corresponds directly to a port redirection rule on a Cisco PIX (see the section above titled “Inbound NAT”). As with port redirection rules on the PIX, this limitation means that it is only possible to publish a single server of each type (i.e., SMTP server, POP3 server) for each external IP address. Fortunately, both the Cisco PIX and ISA Server 2000 allow for multiple IP addresses to be assigned to the external interface.

Web publishing rules are used to publish HTTP-based services according to URL. For example, the URL “<http://www.domain.com/application>” could be directed to one internal web server, while the URL “<http://www.domain.com/information>” could be directed to an entirely different internal web server. ISA examines the incoming URL and then directs the request to the appropriate internal web server. This functionality means that it is theoretically possible to publish a virtually unlimited number of web servers/sites on a single IP address, using host headers or virtual directories in the web publishing rule.

Note that the Cisco PIX has no corresponding functionality without the addition of separate and independent third-party applications.

Other Notes

None

Related Articles/Resources

None

Legal Information

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