

FIREWALL COMPARISON: WATCHGUARD FIREBOX AND CISCO PIX

Products: WatchGuard Firebox II/III firewall; Cisco Secure PIX firewall

Overview

The WatchGuard Technologies Firebox and Cisco System PIX firewall are two widely used firewall products. 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 Firebox and the PIX are described.

More Information

Subnetting

One key difference between the Firebox and the PIX is the need for subnetting. The Firebox has the ability to perform a “drop-in” installation. In a drop-in installation, all three interfaces on the Firebox assume the same IP address, and no subnetting is required. Consider the network shown below in Figure 1.

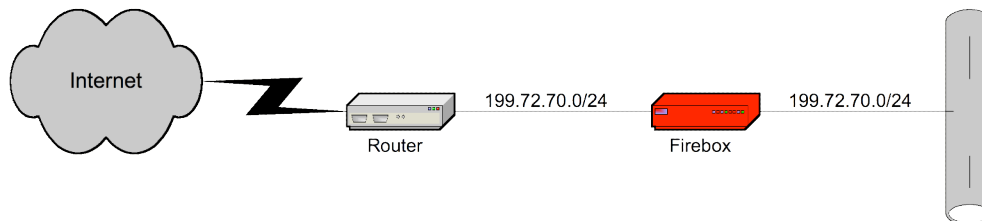


Figure 1. Typical Firebox Installation

In this installation, the link between the router and the Firebox as well as the network behind the Firebox use the same network address. The Firebox itself uses only one IP address for all three interfaces (trusted, optional, and external). Connectivity between the internal network and the external networks is accomplished through proxy ARP, where the Firebox substitutes its own MAC address for the MAC address of the destination.

In this kind of installation, no client changes are necessary. The default gateway can continue to be the router, and the network does not need to be broken into different subnets. The Firebox can

support other subnets as related networks (see the Routing section below) in case RFC 1918-style private addressing is utilized.

The PIX firewall, on the other hand, requires that each interface be attached to a different IP subnet. Compare the network shown in Figure 2 below with the earlier network diagram.

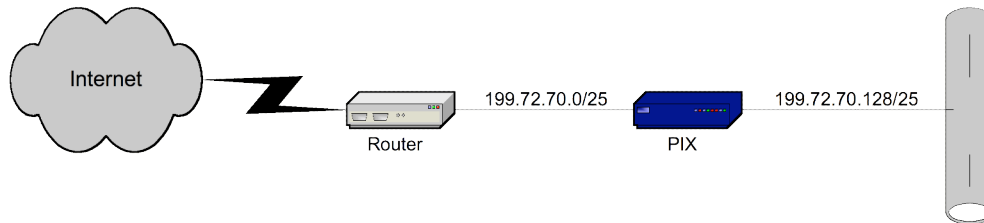


Figure 2. Typical PIX Installation

As you can see in this diagram, the external interface on the PIX uses an IP address from the 199.72.70.0/25 network, while the internal interface uses an IP address from the 199.72.70.128/25 network. Each interface must be on a different subnet. Unlike the Firebox, the PIX does not perform proxy ARP to provide connectivity between the subnets.

In this type of installation, the clients must set their default gateway to the IP address of the PIX firewall's internal interface. If the existing IP addressing scheme does not support multiple subnets, then the addressing schema must be modified to account for the need for at least two distinct IP subnets.

Network Address Translation (NAT)

Both firewalls support Network Address Translation (NAT), so that internal networks can utilize RFC 1918-style private addressing schemes. There are some significant differences in the NAT implementations, however.

The Firebox supports static one-to-one NAT (inbound or outbound) and dynamic many-to-one NAT (outbound). The PIX firewall supports static one-to-one NAT (inbound or outbound), dynamic one-to-one NAT (outbound), and dynamic many-to-one NAT (outbound).

In addition, the Firebox NAT rules are system-wide (affecting all interfaces), whereas the PIX NAT rules are interface-based and affect only the interface for which they are defined. It is possible to enable service-based NAT on the Firebox; in this instance, NAT can be disabled or enabled on a per-service basis. However, the Firebox lacks the ability of the PIX firewall to create access lists to selectively control NAT based on source and/or destination addresses.

Perhaps most importantly, however, is how the firewalls react to internal requests to translated addresses. The Firebox will accept (and route) packets from the trusted interface bound for an external address that is, in turn, translated to an internal address on the trusted interface. This allows for seamless integration into the existing network infrastructure, without requiring additional DNS entries or zones.

The PIX firewall, on the other hand, will not transmit packets out on the same interface on which they were received. As a result, a request from an internal host to an external address translated by the PIX back into an internal address will be dropped as a security violation. There are two solutions to this limitation (or feature, depending on how you look at it). First, implement a private DNS infrastructure. When clients request DNS resolution of a hostname, the internal DNS server(s) will provide an internal address, and the firewall doesn't even get involved.

Alternately, place the server(s) in question on a different interface than the clients that might be accessing that server.

Routing

The WatchGuard Firebox and the Cisco PIX handle routing differently as well. This can create some fairly significant limitations, especially when migrating from one firewall to the other (in particular, when migrating from a Firebox to a PIX).

The Firebox has the ability to route between networks on an interface, typically the trusted interface. It is very common to use a drop-in installation and then add RFC 1918-style private network addresses to the trusted interface as related networks. This allows the Firebox to route between public (registered) subnets and private subnets, serving as the default gateway for both subnets. This is illustrated in the following figure in Figure 3.

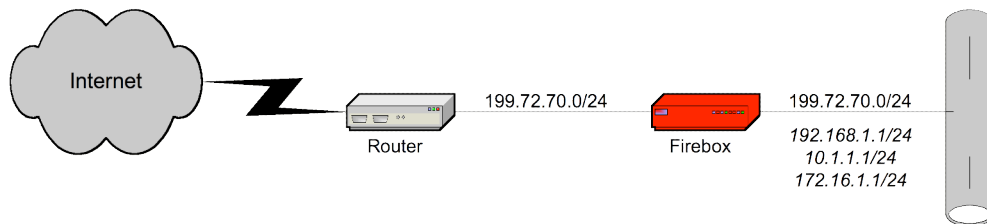


Figure 3. Related Networks on a Firebox's Trusted Interface

As shown in Figure 3, the Firebox can support a public (registered) network address as well as multiple private addresses (shown in italics) on the same interface, routing between them to provide full connectivity.

The PIX firewall, on the other hand, does not route between subnets on an interface. In fact, the PIX does not support multiple addresses assigned to the same interface. To support multiple subnets behind a PIX firewall, each subnet must be attached to a different interface on the PIX or a router must sit between the PIX and the other subnets. In the second instance, the PIX must be informed of the routes to those remote networks through the intermediate router.

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.