

Search for:

- [Advanced Search](#)
- |
- [Search Help](#)

- [Login](#)
- [My Account](#)
- [View Cart](#)

- [Home](#)
- [Bookstore](#)
- [Safari Bookshelf](#)
- [Articles](#)
- [Reference Guides](#)

- [Site Help](#)

[Home](#) > [Articles](#) > [Networking and Communications](#) > [Cisco](#) > What's New in Cisco PIX Firewall 7.0

What's New in Cisco PIX Firewall 7.0

- By [David Hucaby](#).
- Article is provided courtesy of [Cisco Press](#).
- Date: Jun 10, 2005.

 [Save](#)  [Discuss](#)  [Print](#)  [E-mail](#)

 [Article Information](#)

Contents

1. What's New in Cisco PIX Firewall 7.0

Article Description

The Cisco PIX Firewall 7.0 has several new features, as well as some familiar features that have received upgrades. Find out what's new and what's improved in this article from David Hucaby.

Related Book



[Cisco ASA and PIX Firewall Handbook](#)

\$54.00 (Save 10%)

Cisco Systems®, Inc., recently released a major new version of the Cisco PIX® Firewall, version 7.0, and introduced the Cisco Adaptive Security Appliance (ASA) 5500 Series product suite. The Cisco PIX Firewall 7.0 software includes a staggering list of new features and enhancements that can breathe new life into a traditional firewall. As with anything, the more "knobs" there are to turn, the more flexibility (and complexity) is available.

Improved Inspection Engines

Traditionally, ICMP traffic has been difficult to inspect because it is stateless—one host can send one or more ICMP messages without expecting a reply. With PIX 7.0, a firewall can emulate a stateful inspection of ICMP by applying some intuitive rules. For example, if an inside host sends an ICMP echo (ping) packet to another host, the firewall will allow only a single reply packet to return. The firewall will also immediately tear down any address translations that were created for an ICMP "session." For TCP, you can configure very specific security policies that can take action on packets with unexpected values in any of the TCP header fields.

PIX 7.0 introduces very flexible scrutiny of web-based traffic using HTTP. For example, you can configure security policies that make sure HTTP packets conform to the relevant RFCs and standards. In addition, the security appliance can enforce the use of TCP port 80 for any non-HTTP applications.

Security policies can also be defined to inspect and act on instant messaging, peer-to-peer file sharing, and tunneling applications. As well, a firewall can perform deep packet inspection on applications like FTP, ESMTP, and 3G mobile wireless tunneling traffic.

Advanced IP Operation

Prior to PIX 7.0, firewalls were rather limited in handling IP multicast traffic and could only act as stub routers. PIX 7.0 introduces full Protocol Independent Multicast (PIM) routing functions so that security appliances can interoperate with other PIM routers in a network. This allows much more flexible multicast traffic forwarding and inspection, without any intervention.

PIX 7.0 also brings firewall support for IPv6. A security appliance can participate as an IPv6 device and can inspect traffic that uses IPv6 addresses and packet formats.

Transparent Firewall Mode

PIX firewalls have always operated on IP packets, where all of the stateful traffic inspection is performed at Layer 3. This is usually called *routed mode*, where the firewall acts more or less as a router and has IP addresses applied to its own interfaces.

With PIX 7.0, a security appliance can be configured to operate in routed or transparent firewall mode. Transparent mode makes the firewall act more like a Layer 2 bridge, where packets are handled by MAC addresses. Although this prevents the firewall from using IP addresses on its interfaces (except for a single management address), the firewall still inspects traffic using IP addresses and all of the inspection rules you're used to seeing.

Transparent mode has several benefits: without interface IP addresses, the firewall has no detectable presence on the network and malicious users won't be able to find the firewall at all. In addition, the firewall can inspect other non-IP traffic based solely on the EtherType field in the packet headers.

Multiple Context Mode

Traditionally, a Cisco® firewall appliance has been dedicated to running as a single physical firewall. This is also known as a *single security context*. With PIX 7.0, a single appliance can be configured to run multiple security contexts, allowing one hardware platform to emulate several virtual firewalls.

Each security context runs independently with its own set of security policies, access rules, logging configuration, and so on. The firewall appliance does run an administrative context as a means to control the operation of the appliance itself.

PIX 7.0 comes with a license for two simultaneous firewall contexts. You can upgrade to 5, 10, 20, or 50 contexts, depending on the security appliance model. This is especially important to service providers or enterprise environments, where one high-performance platform can provide virtual firewalls for an entire group of customers or departments.

High Availability

Cisco firewalls can operate as a failover pair to provide increased availability. Prior to PIX 7.0, the firewalls worked only as an active-standby pair, one firewall actively inspecting traffic while the other stayed in a standby role, waiting for the active unit to fail. PIX 7.0 introduces active-active failover operation so that both firewall units can be fully functional at the same time. This is accomplished by applying the original active-standby model to the individual security contexts in the multiple context mode.

For each context, one firewall is active while the other takes the standby role. If the active roles are distributed evenly across the contexts, both firewalls can be fully utilized all the time. Failover operation can also be tuned to respond more quickly to a failure—within a minimum of 1.5 seconds! As well, you can select one or more firewall interfaces to monitor when making a decision to failover.

Quality of Service

Prior to PIX 7.0, a Cisco security appliance could inspect and forward traffic only in a best-effort fashion. The first packets into a firewall would be the first packets coming out, regardless of the application being used or the urgency of the traffic.

PIX 7.0 introduces priority queuing on firewall interfaces, so that urgent or time-sensitive traffic can be identified and placed in a strict priority queue. The firewall always makes sure that any packets in a priority queue are sent before any others. This is an important feature for applications like voice and video, where packets must be delivered in a consistently prompt fashion, without being affected by other traffic passing through the firewall.

Specific traffic can also be identified and held within configured bandwidth constraints. This is known as policing, a handy tool that can be used to keep less desirable or less important applications from hogging the links coming from a firewall.

Access List Processing

Cisco security appliances use access lists to define many types of security policies. PIX 7.0 allows access lists to be applied in the inbound, outbound—or both—directions on a firewall interface. Access lists can also be time-based, so they are only applied during a configurable time range. This adds the flexibility of security policies that can change as a function of date or time. In addition, individual access list entries or statements can be disabled without removing them from the firewall configuration.

Modular Policy Framework

In PIX 7.0, you can define security policies based on traffic flow. This offers much more granular control over how the firewall will inspect and enforce its policies. First, traffic is *matched* and grouped into specific classes. Then security policies are defined to take an action on one or more classes of traffic. For any given traffic class, the firewall can apply only the desired application inspection, set certain connection limits, adjust TCP parameters, send the traffic to an intrusion protection system module, police the traffic, or send the traffic to a priority queue.

Firewall Management

If you have ever struggled with entering PIX 6.3 configuration commands, you will appreciate the new context-based help and command completion features in PIX 7.0. For example, typing a question mark anywhere within a command line will show the possible keywords that can be entered.

PIX 7.0 also offers zero-downtime or "hitless" upgrades, allowing the software image to be upgraded on a pair of security appliances without downtime at all. You can also store several configuration files on the appliance flash memory so that new configurations can be backed out easily. Security appliances can be reloaded automatically, based on a predefined schedule. PIX 7.0 also supports the new Adaptive Security Device Manager (ASDM), a web-based management interface.

Firewall logs are vital collections of information, and PIX 7.0 offers plenty of flexibility when logging is configured. For example, you can use multiple syslog servers, each collecting a different set of information from logging level thresholds or logging policies.

Intrusion Protection

When PIX 7.0 is used on one of the new Cisco ASA platforms, traffic can be offloaded to an IPS module. A Cisco ASA 5500 model equipped with a Security Services Modules (SSM) can efficiently inspect, detect, and act on a wide variety of attacks and intrusions. The SSM provides the full set of more than 1100 attack signatures in its database.

VPN

The PIX 7.0 software introduces a rich feature set related to virtual private networks (VPN). An entirely new VPN configuration syntax is used, allowing very flexible VPN policies to be defined. The features are based on the Cisco VPN 3000 functionality. A security appliance can provide an automatic VPN client update and security posture enforcement. As well, two security appliances can be configured as a failover pair to provide VPN stateful failover.

On the Cisco ASA 5500 platforms, the PIX 7.0 software can also provide WebVPN or client-less VPN connectivity using the Secure Socket Layer (SSL) protocol. This is identical to the Cisco VPN 3000 WebVPN service.

Make a New Comment

You must [login](#) in order to post a comment.

You May Also Like

1. [IPSec Overview Part Four: Internet Key Exchange \(IKE\)](#)
 - o By [Andrew Mason](#)
 - o Feb 22, 2002
2. [Introduction to Cisco Network Design](#)
 - o By [Cisco Systems, Inc.](#)
 - o Feb 8, 2002
3. [Using Cisco for Remote Access](#)
 - o By [Steven Dangerfield](#), [Robert Myhre](#)
 - o Sep 6, 2002

[See All Related Articles](#)

Search Related Safari Books



Search electronic versions of over 1500 technical books:

Promotions

[Linux Journal's Readers' Choice Awards](#)

Expires: Jun 30, 2005

[TechEd Book Roundup](#)

Expires: Jul 31, 2005

[Inescapable Data: Harnessing the Power of Convergence Q&A Offer](#)

Expires: Jun 30, 2005

[See All Promotions](#)

Most Popular Articles

[Cisco Network Topologies and LAN Design](#)

By [Anthony Bruno](#), [Jacqueline Kim](#)

Nov 16, 2001

[Securing Cisco Routers](#)

By [Raman Sud](#), [Ken Edelman](#)

Dec 12, 2003

[Configuring the PIX Firewall for SSH \(Secure Shell\)](#)

By [David Chapman, Jr](#)

Feb 15, 2002

[About](#) | [Legal Notice](#) | [Privacy Policy](#) | [Press](#) | [Jobs](#) | [Write For Us](#) | [Contact Us](#) | [Advertise](#) | [Site Map](#)

© 2005 Pearson Education, Informit. All rights reserved.

800 East 96th Street, Indianapolis, Indiana 46240

informit network