Firewalls FAQ

TechRepublic®
Real World. Real Time. Real IT.

Introduction

Firewalls are one of the most basic security measures that you must have in place to protect your systems. We've gathered some of the most frequently asked questions regarding firewalls here and invited our expert, David M. Davis, to answer them and provide some additional resources.

The FAQ list will be constantly evolving, so you're invited to send us other questions you may have. Just e-mail them to us or post them in the discussion area at the end of this FAQ article.

Table of Contents

What is a firewall?

In its most basic terms, a firewall is a system designed to control access between two networks.

There are many different kinds of firewalls—packet filters, application gateways, or proxy servers. These firewalls can be delivered in the form of software that runs on an operating system, like Windows or Linux. Or, these firewalls could be dedicated hardware devices that were designed solely as firewalls.

This TechRepublic article explains the evolution, and differences, between these types of firewalls: "Understand the Evolution of Firewalls." For more information, see "Members answer members' firewall questions."

Why would you want a firewall?

Firewalls will protect your network from unwanted traffic. Many times, the unwanted traffic is harmful traffic from hackers trying to exploit your network. You want a firewall to protect your network, just as you want locks on your door and windows at your home.

Is a proxy server a firewall?

A proxy server is a form of a firewall. In legal terms, a proxy is someone who goes and performs some action on your behalf. A proxy server performs network transactions on your behalf. The most common use for this is a Web-proxy server. A Web-proxy will take requests from users' Web browsers, get the Web pages from the Internet, and return them to the user's browser. Many times, a proxy server also performs authentication to see who is requesting the Web pages and also logs the pages that are requested and the user they are from.

What is NAT?

NAT is Network Address Translation. NAT is usually used to translate from real/global/public Internet addresses to inside/local/private addresses. These private addresses are usually RFC1918 IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16).

NAT provides some security for your network as you do not have a real Internet IP address and your network, usually, cannot be accessed from the Internet without some outbound connection first being created from your private/inside network.

However, you still need a firewall to protect your network as NAT only hides your network but doesn't really stop any packets from entering your network.

Do firewalls stop viruses, Trojans, adware, and spyware?

No, in general, firewalls do not stop viruses, Trojans, adware, or spyware. Firewalls, usually, only protect your network from inbound traffic from an outside (Internet) network. You still need antivirus software, anti-adware and anti-spyware software applications to protect your system when it does go out on the Internet.

For more information, see "The Firewall in a multilayer security approach."

How do I know that my firewall is really protecting my network?

Just like any security system, a firewall should, periodically, be tested. To test a firewall, you could have a professional security-consulting company do a security vulnerability scan. However, this is usually something you can do yourself. To do this, you could use a port-scanner or a more advanced tool like a vulnerability assessment tool (such as Retina, Saint, or ISS).

For more information, see "How to make sure a firewall does its job."

What are the different types of firewalls?

The different types of firewalls are:

Packet filter – A packet filter looks at each packet entering the network and, based on its policies, permits or denies these packets. A Cisco IOS Access Control List (ACL) is a basic firewall that works in this way.

Stateful packet filter – A stateful packet filter also has rules; however, it keeps track of the TCP connection state so it is able to monitor the “conversations” as they happen on the network. It knows the normal flow of the conversations and knows when the conversations are over. Thus, it more intelligently is able to permit and deny packets entering the network. Because of this, a stateful packet filter (stateful firewall) is much more secure than a regular packet filter.

Application gateway – An application gateway is a system that works for certain applications only. It knows the “language” that that application/protocol uses and it monitors all communications. An example would be a SMTP gateway.

Proxy Server – A proxy server performs network transactions on your behalf. The most common use for this is a Web-proxy server. A Web-proxy will take requests from users’ Web browsers, get the Web pages from the Internet, and return them to the user’s browser.

What do VPNs have to do with firewalls?

Virtual Private Networks (VPN) are used to encrypt traffic from a private network and send it over a public network. Typically, this is used to protect sensitive traffic as it goes over the Internet. Many times, you will have a VPN encryption device combined with a firewall as the private network traffic that is being encrypted also needs to be protected from hackers on the public network.

If I have a firewall, do I have a DMZ?

No, you do not necessarily have a DMZ if you have a firewall. A DMZ is a network that is semi-protected (not on the public network but also not on the fully-protected private network). Many hardware firewalls create a DMZ for public mail servers and Web servers. Most small networks or homes do not have DMZ networks. Most medium-to-large corporate networks would have a DMZ.

What are IDS and IPS? Also, what do they have to do with firewalls?

An Intrusion Detection System (IDS) monitors for harmful traffic and alerts you when it enters your network. This is much like a burglar alarm.

An Intrusion Prevention System (IPS) goes farther and prevents the harmful traffic from entering your network.

IDS/IPS systems recognize more that just Layer 3 or Layer 4 traffic. They fully understand how hackers use traffic to exploit networks and detect or prevent that harmful traffic on your network.

Today, many IDS/IPS systems are integrated with firewalls and routers.

For more information, see "IDS: The Integrated partner for your firewall."

What is a DoS attack and will a firewall protect me from it?

A Denial of Service (DoS) attack is something that renders servers, routers, or networks incapable of responding to network requests in a timely manner.

Firewalls can protect your network and its servers from being barraged by DoS traffic and allow them to respond to legitimate requests, thus, allowing your company to continue its business over the network.

How do you configure, monitor, and control a firewall?

As there are many different types of firewalls, there are also many different types of firewall interfaces. You could have a command line interface (CLI), a Web-based interface, or some other proprietary program that is used to configure the firewall.

For example, with Cisco PIX firewalls, you can configure them with the CLI interface (called PixOs), or the PIX Device Manager (PDM), a Java-based interface that works with a Web browser.

For more information, see "Configure IT Quick: Configure a Cisco PIX firewall and select a topology."

How do I know what firewall I should use for my business?

The size of the firewall you choose is usually based on the volume of traffic your network links receive or the bandwidth of your network links. You also must take into consideration other things for which you might be using the firewall, such as VPN, IDS, and logging.

For more information, see "Cisco SAFE Blueprint (for securing and designing enterprise networks)" and "Product Review: Cisco's PIX puts the enterprise in firewalls."

What are some new features to look for in firewalls?

Firewalls, today, are offering more and more features built into the firewall. Some of them are: intrusion prevention, hardware-based acceleration, and greater recognition of applications (moving up the OSI model towards layer 7).

How can I configure an inexpensive firewall for my company?

There are a wide variety of firewalls available today. Perhaps the most basic firewall is the personal PC firewall, such as that built into Windows XP. Next come more advanced PC software firewalls, like ZoneAlarm Pro or BlackICE. There are midrange firewall solutions like Microsoft ISA or hardware firewalls. Next on the scale are large Cisco PIX or Checkpoint firewalls used for large businesses or Internet Service Providers.

You may also choose to create your own firewall, for next to nothing, using Linux and a PC with two NIC cards. Links on how to accomplish this include:

"Give old PC's a new lease on life as Linux Firewalls"
"Set up a Linux Firewall with ease using Firestarter"
"Build your Skills: Create a poor man's firewall with the Cisco IOS"

Related TechRepublic resources: Firewalls FAQ

TechRepublic books and CDs:

- Network Administrator's Hacks Pack
- Securing Your Enterprise: A Guide to Network Threat Management
- Wireless Networking Survival Guide

Downloads:

- A firewall checklist
- Firewall topology diagrams in Visio
- Example of costs for software-based firewall

Articles and columns:

- Top five don'ts in wireless security
- The weakest security link? It's you
- Lock down remote access to the Windows registry

TechRepublic:
The collective voice of IT professionals

TechRepublic communities engage IT professionals in the ultimate peer-to-peer experience, providing actionable information, tools, and services to help members get their jobs done. TechRepublic serves the needs of the professionals representing all segments of the IT industry, offering information and tools for IT decision support and professional advice by job function.

CIO Republic: Get analysis and insight on e-business, leadership, executive careers, business strategy, and technology.
IT Manager Republic: Access technology insights, project and personnel management tips, and training resources.
NetAdmin Republic: Get tips on Windows, NetWare and Linux/UNIX administration, infrastructure design, and network security.
Support Republic: Obtain detailed solutions to desktop hardware, software, and end-user support problems.
IT Consultant Republic: Find information and advice on client and vendor relations, project management, and technology.

TechRepublic site features

Free e-newsletters: Keep up-to-date on any aspect of the IT industry with e-newsletters—from tech stocks to daily software tips, from IT careers to hot trends—delivered right to your e-mail Inbox.
Free downloads: We've collected resources to make your job easier, including ready-to-use IT forms and templates, checklists, tools, executables, Gartner product analyses, and white papers.
TechRepublic's books and CDs: Find the latest books and CDs about today's critical IT topics, including PC troubleshooting, VPN, TCP/IP, Windows client and server issues, and Cisco administration.
Discussion center: Open a discussion thread on any article or column or jump into preselected topics: career, technology, management, and miscellaneous. The fully searchable Discussion Center brings you the hottest discussions and threads and allows you to sort them by topic and by republic.
Try our premium subscription product, TechProGuild, free for 30 days. Our online IT community provides real-world solutions and the latest articles, resources, and discussions affecting frontline IT pros. Get access to more than 250 full-text IT books, along with exclusive downloads and in-depth articles on network and system administration, PC troubleshooting, help desk and support issues, and more.