

Cisco Router Firewall Security

Richard A. Deal

Cisco Press

800 East 96th Street
Indianapolis, Indiana 46240 USA

Cisco Router Firewall Security

Richard A. Deal

Copyright© 2005 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing August 2004

Library of Congress Cataloging-in-Publication Number: 2003111982

ISBN: 1-58705-175-3

Warning and Disclaimer

This book is designed to provide information about using Cisco routers as perimeter firewall solutions. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419, corpsales@pearsontechgroup.com.

For sales outside the U.S. please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	John Wait
Editor-in-Chief	John Kane
Executive Editor	Brett Bartow
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Nannette M. Noble
Acquisitions Editor	Michelle Grandin
Production Manager	Patrick Kanouse
Development Editor	Andrew Cupp
Project Editor	Marc Fowler
Copy Editor	Krista Hansing
Technical Editors	Scott Clayton, Stephen Marcinek, Umar Shafiq
Team Coordinator	Tammi Barnett
Book and Cover Designer	Louisa Adair
Composition	Interactive Composition Corporation
Indexer	Tim Wright

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PDX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Printed in the USA

intrusion-detection systems (IDS), multicast routing, connection authentication, Dynamic Host Configuration Protocol (DHCP) services, and many others. One of the driving forces of these enhancements, besides vendor competition, was the explosion of Internet usage in the mid- to late 1990s. This huge growth brought many beneficial services to individuals and companies, but it also brought its own set of problems, including hacking, break-ins, and other types of undesirable actions. Given these problems and the need to protect a company's assets, firewalls have become a common technology for not only enterprise companies, but also small businesses and personal computers that have Internet access.

As you will see in this chapter, many components make up a firewall solution; naturally, a firewall, or filtering device, is an important part of that solution. Normally, firewalls are seen as your first layer of defense when protecting company or personal assets. However, a complete firewall solution involves many components that are used to protect not only the perimeter of your network, but also your internal network infrastructure.

Definition of a Firewall

People use many descriptions when defining a firewall. Its first use had to do not with network security, but with controlling actual fires. A firewall is a method of constructing walls so that when a real fire breaks out, it can be contained easily within one part of a building instead of spreading to other parts.

Of course, when we talk about network security, the term *firewall* means something different, but the original essence is carried over: It is used to protect your network from malicious people and to stop their illicit actions at defined boundary points.

Basically, a firewall is a device or systems that control the flow of traffic between different areas of your network. Notice something important about this definition: The definition can include one or more devices. In simple, small network designs, such as a small office/home office (SOHO) environment, this typically is done with one device. For example, I use a wireless Linksys router at home to protect my home network. In an enterprise network, the firewall system includes many components, such as perimeter firewalls, stateful firewalls, VPNs, IDS solutions, and others.

Many people assume that firewalls are used to protect assets from external threats, such as those from the Internet, where the protocol used is TCP/IP. However, most malicious network threats and attacks occur, interestingly enough, within the interior of your network; in many instances, they come from a company's own employees. Many studies have found that between 60 and 70 percent of network attacks are internal, not external. On top of this, you might have more than one protocol running on your internal network, such as TCP/IP, IPX, AppleTalk, SNA, NetBIOS, and others. A comprehensive firewall solution must be capable of dealing not only with both internal and external threats, but also with multiple protocols.

These two problems, IP spoofing and DoS attacks, typically can be dealt with by causing an individual first to authenticate traffic before allowing it through the firewall. Unfortunately, a packet-filtering firewall examines only Layers 3 and 4 information. Performing authentication requires a firewall that processes authentication information, which is a Layer 7 (application layer) process.

Finally, packet-filtering firewalls typically support logging functions. However, their logging functions are limited to just Layers 3 and 4 information. If someone was executing a specific type of web server attack on port 80 and you were denying port 80 traffic, your packet-filtering firewall could log the deny action, but, unfortunately, the firewall wouldn't log the application-layer data encapsulated in the HTTP transport segment. Therefore, you, as an administrator, would know that someone was attempting to access port 80 on your server, but you would not know what that person was trying to do.

Uses for Packet-Filtering Firewalls

Because of these limitations, packet-filtering firewalls typically are used in the following areas:

- As a first line of defense (perimeter router)
- When security policies can be implemented completely in a packet filter and authentication is not an issue
- In SOHO networks that require minimal security and are concerned about cost

Many companies use packet-filtering firewalls as a first line of defense, with some other type of fully functioning firewall behind it providing additional security. An example of this is a Cisco PIX.

Likewise, packet-filtering firewalls can be used for internal access control between different subnets and departments where authentication is not necessary. In this example, you are concerned about controlling access to specific internal resources from your users; you are not as concerned about sophisticated hacking attacks from your users.

Many SOHO networks employ packet-filtering firewalls because of their simplicity and cost when compared to other types of firewalls. SOHOs are interested in basic security at a reasonable cost. You must realize, of course, that packet-filtering firewalls do not provide complete protection for the SOHO, but they do provide at least a minimal level of protection to keep out many types of network threats and attacks.

Stateful Firewalls

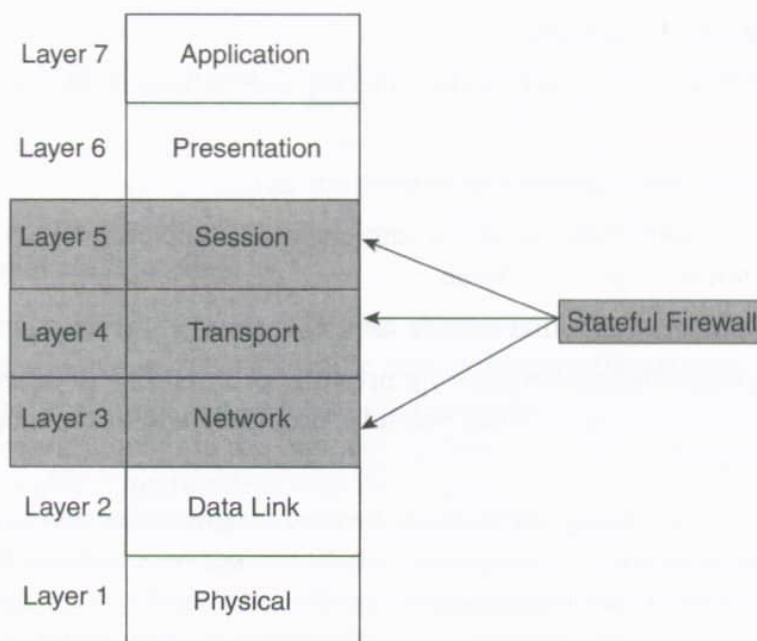
Unlike packet-filtering firewalls, stateful firewalls keep track of the state of a connection: whether the connection is in an initiation, data transfer, or termination state. This is useful

when you want to deny the initiation of connections from external devices, but allow your users to establish connections to these devices and permit the responses to come back through the stateful firewall.

Many security people disagree on what layer of the OSI reference model stateful firewalls function at: Layers 3 and 4 (transport), or Layers 3, 4, and 5 (session). From a transport layer perspective, the stateful firewall examines information in the headers of Layer 3 packets and Layer 4 segments. For example, it looks at the TCP header for SYN, RST, ACK, FIN, and other control codes to determine the *state* of the connection.

However, because the session layer establishes and tears down the connection—the transport layer handles the actual mechanics of the connection—some say that stateful firewalls operate at Layer 5, as shown in Figure 2-7. In either case, remember that stateful firewalls know about a connection and its state.

Figure 2-7 *Stateful Firewalls and the OSI Reference Model*



Problems with Packet-Filtering Firewalls

This section and the next one examine one of the issues that packet-filtering firewalls have with traffic and how stateful firewalls can deal with it.

Refer to Figure 2-8 for the example. In the figure, the packet-filtering firewall has a rule placed on its inbound interface from the Internet stating that any external traffic sent

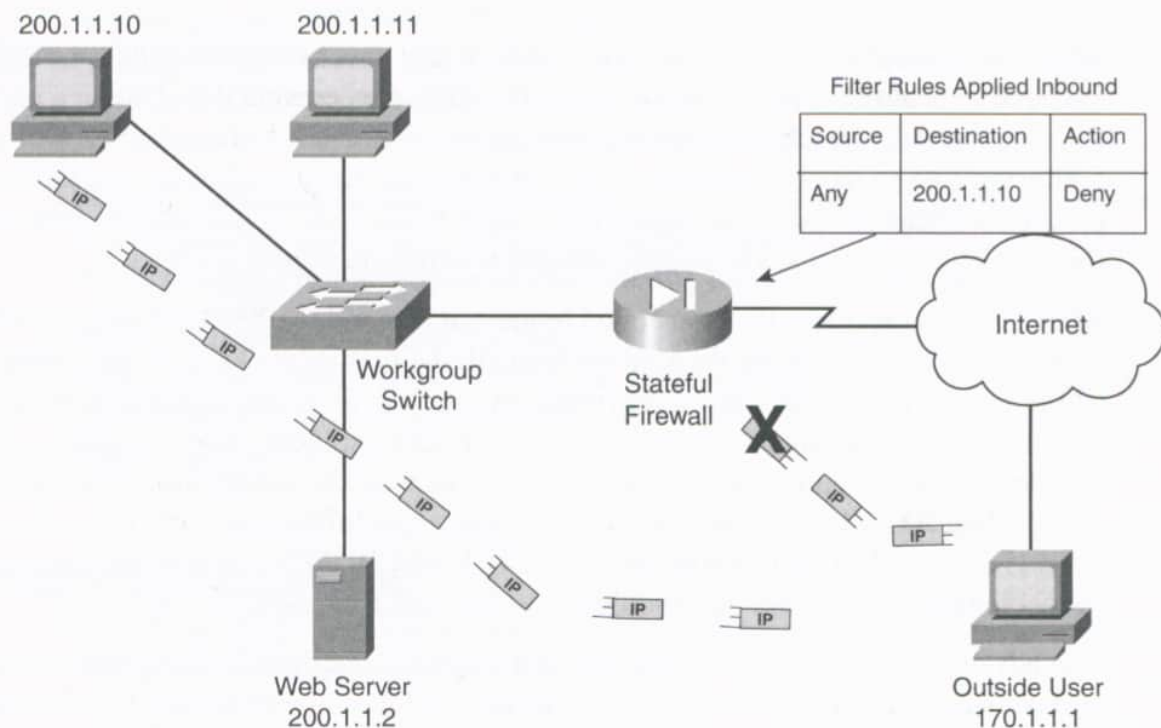
an external device, such as 170.1.1.10. However, the packet-filtering firewall cannot distinguish between a valid response and a fake response. With a fake response, a hacker generates TCP segments with certain code flags set, trying to gain access through your firewall. A packet-filtering firewall, cannot distinguish between the two types of traffic.

CAUTION The **established** Cisco parameter for TCP extended ACLs examines the code flags and allows returning traffic into the network. However, a hacker can manipulate this returning traffic, opening you to reconnaissance, DoS, and other types of attacks.

State Table

Unlike packet-filtering firewalls, stateful firewalls use a mechanism to keep track of the state of a connection. See Figure 2-12 and Figure 2-13 for an illustration of this. Figure 2-12 uses the same network discussed in the last section with a packet-filtering firewall. In this example, the packet-filtering firewall has been replaced by a stateful firewall, but the filtering rule is unchanged: Any traffic sent to 200.1.1.10 is dropped.

Figure 2-12 *Stateful Firewall Filtering Example—Part 1*



Assume that 170.1.1.1 sends traffic to 200.1.1.10. As shown in Figure 2-12, this traffic is dropped. Now assume that 200.1.1.10 opens a web connection to 170.1.1.1, as shown in the bottom part of Figure 2-12. When 200.1.1.10 does this, it uses a TCP segment with a source port of 10,000 and a destination port of 80. It uses a SYN flag in the control field.

Using the wrong product to solve a security problem can open you to all kinds of security threats. For example, assume that you want to use an IDS to detect different kinds of network threats. You notice that your Cisco router has the capability in the Cisco IOS Firewall feature set, and you decide to enable it, feeling secure that your Cisco router will generate an alarm when an attack occurs. If you had taken time to read the security material related to Cisco routers, you would have realized that Cisco routers can detect only a few dozen different kinds of networking attacks (typically, the most common ones). Therefore, for all the other hundreds of kinds of attacks, your Cisco router will not be capable of detecting them, leaving you exposed. In this example, a better solution would have been to purchase an IDS solution that can detect hundreds of different kinds of attacks.

Using Old Junk to Solve New Problems

As a consultant, I repeatedly hear from customers that they want an inexpensive (that is, “cheap”) solution that reuses a lot of the networking gear that they already have in their current design. Unfortunately, with a network that has equipment that is more than 5 years old, this presents a problem because that technology is outdated and probably useless.

When designing a network, especially as it relates to security, you first must come up with a simplified design that describes the basic components that are required. Then you must determine which actual products you will use for these components, based on the features and functions you need. Never try to approach this backward by trying to fit a product to your design: You create problems by doing this instead of solving them. Also remember that there is no such thing as a networking product that will do everything: Do not force yourself to cut corners by trying to make one device do everything.

Creating a Layered Defense

A security design typically uses a layered defense approach. In other words, you usually do not want one layer of defense to protect network. If this one layer is compromised, your entire network will be exposed.

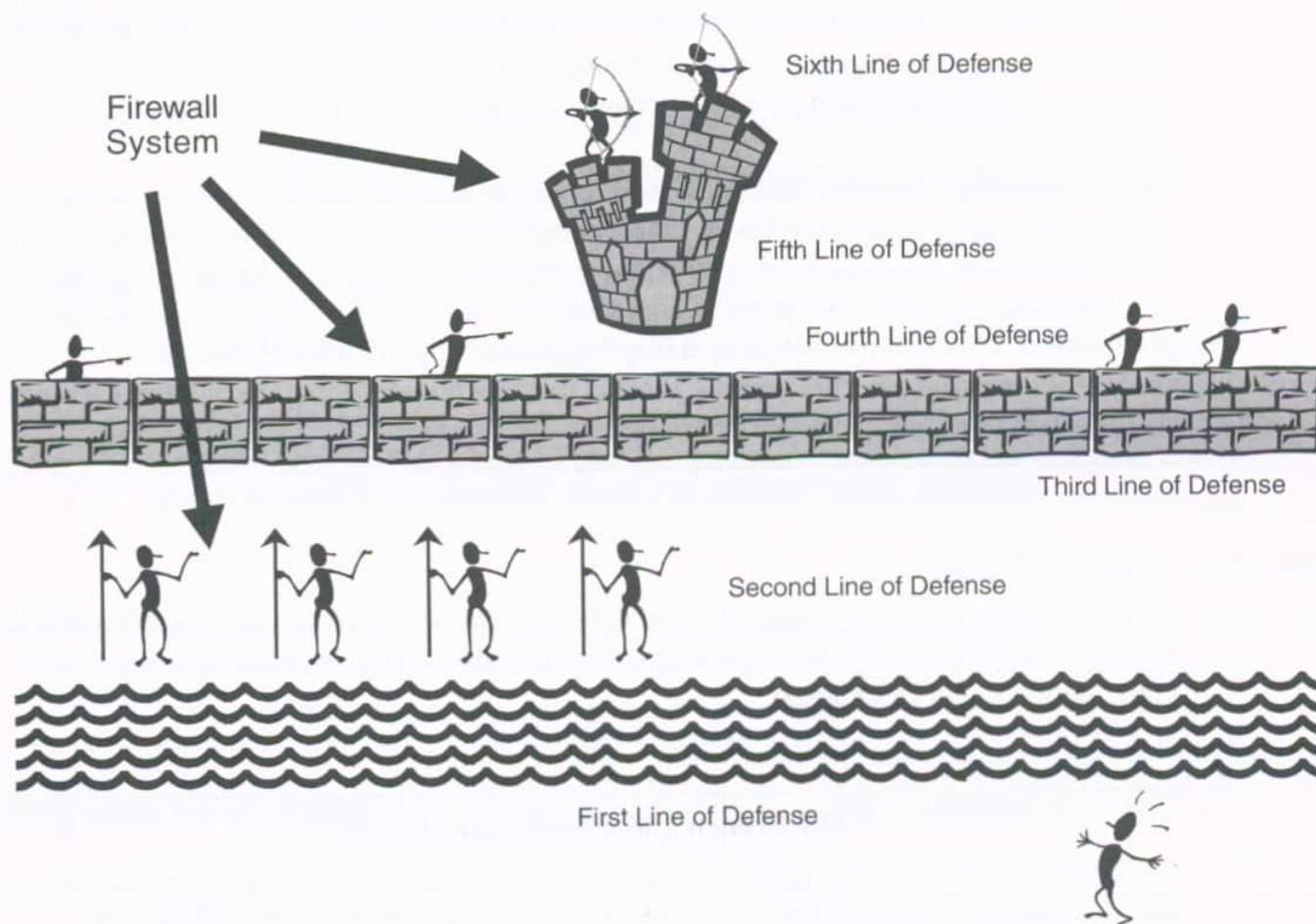
The French and a One-Layer Defense

The French learned the one-layer defense limitation the hard way during World War II with the Maginot line, a physical barrier between Germany and France. The Maginot line extended only the distance of the border between France and Germany. The Germans were smart: They went north and west and came down through the Netherlands, bypassing this fortification and allowing them to easily conquer France.

Instead, you should use a multilayer defense in your firewall system design. With multiple layers, if one layer is compromised, you still have other layers behind it protecting you.

One of the examples that I like to use to describe a firewall system is the fortification systems that kings used to protect their castles in medieval times. Figure 2-22 shows an example of this. In this figure, the first line of defense is the moat surrounding the castle. For the second line of defense, spearmen are behind the moat, preventing anyone from trying to swim across it. Behind the spearmen is the third line of defense: the castle wall, which can be as little as 3 meters high but typically was much higher than this. On the wall are swordsmen, providing the fourth layer of defense. Inside the castle wall are the castle grounds and the castle itself. The castle is built with very high stone walls and turrets, providing the fifth layer of defense. And in the windows of the wall and on top of the turrets are the archers, providing the last layer of defense. As you can see from this system, an attacker must go through many layers of defense to capture or kill the king.

Figure 2-22 *A Medieval Firewall System*



Dealing with Internal Threats

Too often, security personnel are concerned about protecting a company's resources and assets from outside threats. Remember that it is much easier to attack your assets from

As you can see in this example, you easily can protect important resources in your network from other internal users. Internal DMZs enable you to accomplish the following:

- Control traffic between areas
- Localize security problems

I already have discussed the first bulleted point. For the second, imagine that a hacker somehow could compromise your perimeter defenses and access an internal resource such as a file server. By using an internal DMZ, you still are protecting important resources. In Figure 2-27, the accounting and engineering resources are protected from the hacker if an internal resource connected to the lower-level internal interface was compromised.

Components

Now that you have a basic understanding of firewall system design practices, this section takes a closer look at the components that make up a firewall system. A good firewall system typically contains the following components:

- Perimeter router
- Firewall
- VPN
- IDS

It is important to point out here that I used the word *component*, not *device*, to describe what is included in a firewall system. This is because many devices can support multiple components. For example, a Cisco IOS router can act as a perimeter router or a main firewall, can terminate VPN connections, and can perform IDS—all in one chassis. Remember my caution, though, if you are using a single layer for defense: Using multiple layers provides for a better design and protection. The following sections cover the different components used in a firewall system.

Perimeter Router Component

The main purpose of the perimeter router is to provide a connection to a public network, such as the Internet, or a different company. It is used to convert data-link layer media types from a LAN to either a WAN or MAN medium.

The functions of the perimeter router can include the following:

- Routing through static routes or a dynamic routing protocol
- Filtering through either packet filtering or stateful filtering
- Terminating VPN connections
- Providing address translation