



SECURITY

Cisco Secure Firewall Services Module (FWSM)

Cisco Secure Firewall Services Module (FWSM)

Ray Blair, Arvind Durai

Copyright© 2009 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

First Printing September 2008

Library of Congress Cataloging-in-Publication Data:

Blair, Ray, 1965-

Cisco secure firewall services module (FWSM) / Ray Blair, Arvind Durai.

p. cm.

ISBN-13: 978-1-58705-353-5 (pbk.)

ISBN-10: 1-58705-353-5 (pbk.)

1. Computer networks—Security measures. 2. Firewalls (Computer security) 3. Cisco Systems, Inc. I. Durai, Arvind. II. Title.

TK5105.59.B563 2009

005.8—dc22

2008030575

ISBN-13: 978-1-58705-353-5

ISBN-10: 1-58705-353-5

Warning and Disclaimer

This book is designed to provide information about the Firewall Services Module, using practical design examples. 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

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States 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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	Paul Boger
Associate Publisher	Dave Dusthimer
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Executive Editor	Brett Bartow
Managing Editor	Patrick Kanouse
Development Editor	Dan Young
Senior Project Editor	Tonya Simpson
Copy Editor	Barbara Hacha
Technical Editors	Sunil Gul Wadwani, Bryan Osoro
Editorial Assistant	Vanessa Evans
Designer	Louisa Adair
Composition	Mark Shirar
Indexer	John Bickelhaupt
Proofreader	Kathy Ruiz



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn is a service mark, and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, OCVF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, IPHONE, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)

Introduction

Firewalls are one of the main components used in securing a network infrastructure, and having an in-depth understanding of how these devices function is paramount to maintaining a secure network.

This book was written to provide an understanding of the functionality of the Firewall Services Module (FWSM), from both a hardware and software perspective and to be a practical design guide with configuration examples for the design, implementation, operation, and management of FWSM in various deployment scenarios.

Who Should Read This Book?

This book is targeted at individuals who would like an in-depth understanding of the FWSM. It is focused primarily for those who design, implement, or maintain the FWSM, such as security/network administrators. To get the most value from the material, the reader should have at least an intermediate knowledge of networking and security.

How This Book Is Organized

This book is organized into five sections that cover the basic introduction of firewalls, initial and advanced configurations, design guides and configuration examples, and features and functionality introduced in FWSM version 4.x code:

- **Chapter 1, “Types of Firewalls”:** This chapter explains the functionality of the different types of firewalls.
- **Chapter 2, “Overview of the Firewall Services Module”:** This chapter covers specifications, installation information, performance, and virtualization; shows a comparison of IOS FW, ASA, and FWSM; and also explains the hardware and software architecture.
- **Chapter 3, “Examining Modes of Operation”:** This chapter examines the modes of operation (transparent/routed) and explains the advantages of each.
- **Chapter 4, “Understanding Security Levels”:** This chapter explains how traffic flows between interfaces, using both NAT and PAT and routed and transparent modes.
- **Chapter 5, “Understanding Contexts”:** This chapter provides an overview of the benefits of contexts and how to manage them.
- **Chapter 6, “Configuring and Securing the 6500/7600 Chassis”:** This chapter explains how to configure the host chassis to support the FWSM.
- **Chapter 7, “Configuring the FWSM”:** This chapter covers the initial configuration of the FWSM.
- **Chapter 8, “Access Control Lists”:** This chapter examines the use of ACLs.
- **Chapter 9, “Configuring Routing Protocols”:** This chapter explains the use of routing protocols on the FWSM.

- **Chapter 10, “AAA Overview”:** This chapter covers the principles of using authentication, authorization, and accounting.
- **Chapter 11, “Modular Policy”:** This chapter covers the use of class and policy maps.
- **Chapter 12, “Understanding Failover in FWSM”:** This chapter explains the use and configuration of using multiple FWSMs for high availability.
- **Chapter 13, “Understanding Application Protocol Inspection”:** This chapter covers the use and configuration of application and protocol inspection.
- **Chapter 14, “Filtering”:** This chapter examines how traffic can be filtered using filter servers and how Active X and Java filtering function.
- **Chapter 15, “Managing and Monitoring the FWSM”:** This chapter covers the different options of managing and monitoring the FWSM.
- **Chapter 16, “Multicast”:** This chapter explains the interaction of multicast with the FWSM and provides some practical examples.
- **Chapter 17, “Asymmetric Routing”:** This chapter provides an explanation of asymmetric routing and how it can be configured.
- **Chapter 18, “Firewall Load Balancing”:** This chapter covers the options of how to increase performance using multiple FWSMs.
- **Chapter 19, “IP Version 6”:** This chapter explains IPv6 and how it is configured on the FWSM.
- **Chapter 20, “Preventing Network Attacks”:** This chapter examines how to mitigate network attacks, using shunning, antispoofing, connection limits, and timeouts.
- **Chapter 21, “Troubleshooting the FWSM”:** This chapter explains how to leverage the appropriate tools to solve problems.
- **Chapter 22, “Designing a Network Infrastructure”:** This chapter covers an overview on placement of the FWSM in the network.
- **Chapter 23, “Design Scenarios”:** This chapter provides many practical examples of how the FWSM can be configured.
- **Chapter 24, “FWSM 4.x Performance and Scalability Improvements”:** This chapter covers the performance improvements in 4.x code.
- **Chapter 25, “Understanding FWSM 4.x Routing and Feature Enhancements”:** This chapter explains the use of commands introduced in 4.x code.

Understanding FWSM 4.x Routing and Feature Enhancements

Several significant additions to the 4.x code enhance routing and other features. Some of these additions include Enhanced Interior Gateway Routing Protocol (EIGRP) routing, route health injection, and some additional security features and application inspection enhancements.

Configuring EIGRP

EIGRP has been a long-awaited feature for the Firewall Services Module (FWSM). With EIGRP support, the FWSM can be integrated into an existing EIGRP network, minimizing the need to redistribute routing information into other routing protocols. This reduces the complexity of managing multiple routing processes and simplifies the network design, especially within the datacenter.

Redistribution of routes between routing protocols can be difficult because each routing protocol exercises different methods to classify routes (cost). For example, RIP uses hop-count, OSPF uses a metric (single value), and EIGRP uses bandwidth and delay by default. When routing information is exchanged, the methods used to classify them are also lost. Consequently, routing loops can easily occur if you redistribute a route into one process, change the cost, and inject the route back into the first routing process. Use caution if you find yourself in this situation.

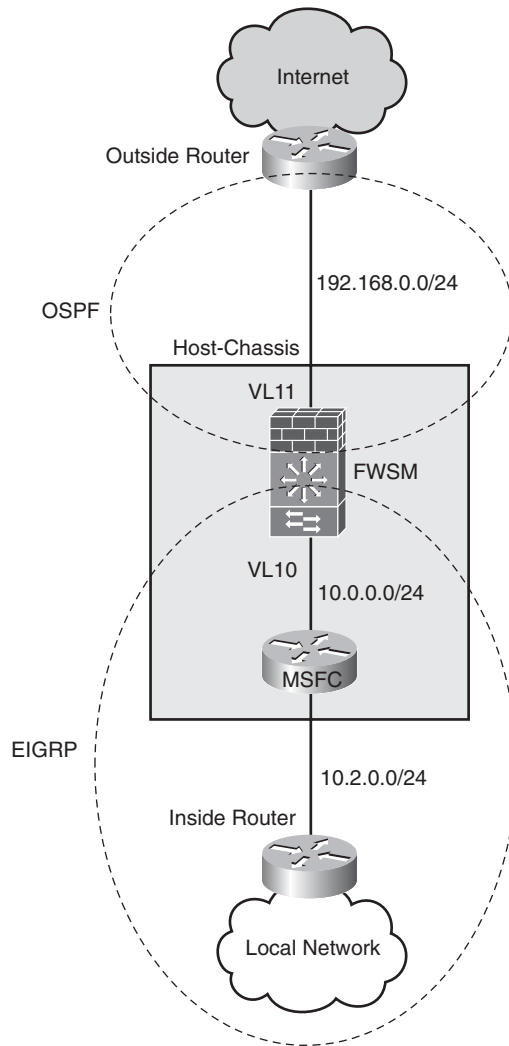
EIGRP is supported only in single-context mode and allows only one single EIGRP routing process. Unlike Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), which cannot be enabled simultaneously, EIGRP and RIP or EIGRP and OSPF can be. Where additional security is required, when connecting to the Internet or other untrusted connections, an EIGRP process can be used on the inside and another routing process can be used on the outside.

NOTE

EIGRP is supported only in single-context mode.

Using Figure 25-1, the following example shows how EIGRP is configured to exchange routing information with the local network and extend the default route learned from the OSPF process exchanged on the outside interface to the local network. In the event the router on the outside stops forwarding the default route to the FWSM, the FWSM will remove the route from the local routing table, consequently removing the default route in the local network.

Figure 25-1 *EIGRP and OSPF Route Redistribution*



To enhance the security for the routing information exchanged on the outside, OSPF Message Digest 5 (MD5) authentication has also been configured.

Example 25-1 shows the configuration of the FWSM (only the pertinent information is shown).

Example 25-1 *EIGRP Route Redistribution*

```
interface Vlan10
 nameif Inside
 security-level 100
 ip address 10.0.0.2 255.255.255.0
!
interface Vlan11
 nameif Outside
 security-level 0
 ip address 192.168.0.2 255.255.255.0
 ospf message-digest-key 1 md5 <removed>

router eigrp 1
 no auto-summary
 network 10.0.0.0 255.255.255.0
 redistribute ospf 1 metric 1000 2000 255 1 1500

!
!
router ospf 1
 network 192.168.0.0 255.255.255.0 area 0
 area 0 authentication message-digest
 log-adj-changes
 redistribute eigrp 1 subnets
 summary-address 10.0.0.0 255.0.0.0
```

As the output from the **show route** command shows in Example 25-2, the FWSM has learned about the routes from the local network via EIGRP. These routes are denoted with the letter “D,” and the route from the outside has been learned via OSPF denoted with the letter “O.”

Example 25-2 *EIGRP Redistributed Routes*

```
FWSM# show route
D 10.2.0.0 255.255.255.0 [90/26880256] via 10.0.0.1, 1:42:35, Inside
D 10.3.0.0 255.255.255.0 [90/27008256] via 10.0.0.1, 1:42:35, Inside
D 10.1.1.0 255.255.255.0 [90/130816] via 10.0.0.1, 1:42:35, Inside
O 10.0.0.0 255.0.0.0 is a summary, 1:42:43, Null0
C 10.0.0.0 255.255.255.0 is directly connected, Inside
D 10.4.0.0 255.255.255.0 [90/27008256] via 10.0.0.1, 1:42:35, Inside
C 192.168.0.0 255.255.255.0 is directly connected, Outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 192.168.0.1, 0:38:26, Outside
```


The FWSM is exchanging routing information with the Multilayer Switch Feature Card (MSFC) associated with the inside interface, as the output from the **show eigrp neighbors** command reveals in Example 25-3.

Example 25-3 *EIGRP Neighbors*

```
FWSM# show eigrp neighbors
EIGRP-IPv4 neighbors for process 1
H   Address                Interface           Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt  Num
0   10.0.0.1                V110               12 02:59:38 1    200  0   63
```

The OSPF adjacency has been established with the router on the outside interface, as the output from the **show ospf neighbor** command reveals in Example 25-4.

Example 25-4 *OSPF Neighbor*

```
FWSM# show ospf neighbor
Neighbor ID   Pri  State           Dead Time   Address        Interface
192.168.100.1  1   FULL/BDR       0:00:33    192.168.0.1   Outside
```

In Example 25-5, the last two lines from the **show ospf interface** command also indicate that the neighbor adjacency is using MD5.

Example 25-5 *OSPF Interfaces*

```
FWSM# show ospf interface
Outside is up, line protocol is up
  Internet Address 192.168.0.2 mask 255.255.255.0, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.2, Interface address 192.168.0.2
  Backup Designated router (ID) 192.168.100.1, Interface address 192.168.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 6
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.100.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
```

The challenges of complex redistribution scenarios from EIGRP to OSPF or RIP on adjacent routers are now eliminated with the capability of supporting EIGRP natively on the FWSM. Running EIGRP through the FWSM should be reserved for passing routing information internal to the network—for example, within the datacenter. This minimizes the impact of attacks targeting routing protocols.

The addition of EIGPR support makes the integration of the FWSM into networks taking advantage of the EIGRP routing protocol substantially easier, by not requiring the redistribution between routing protocols. When required, you still have the capability to redistribute routing information between routing protocols on the FWSM, but use caution that you do not cause a routing loop.

Configuring Route Health Injection

The FWSM has limited support for dynamic routing protocols when using “multiple-context” mode. Route Health Injection (RHI) has the capability of propagating routing information from individual contexts in routed-mode, including static routes, connected networks, and Network Address Translation (NAT) pools into the routing-engine on the host-chassis.

Because RHI has such a tight integration with the routing-engine, the minimum image needed on the Supervisor 720 and/or Supervisor 32 is 12.2(33)SX1.

RHI creates entries for static and directly connected routes in the MSFC.

Routes can be redistributed to any routing protocol: EIGRP, BGP, and so on.

RHI can also be used to advertise NAT pools into the MSFC.

RHI allows the FWSM to support more than one routing protocol in multi-context mode.

The following example shows how to propagate a default route into the routing-engine from a context on the FWSM.

Example 25-6 shows the configuration on the host-chassis.

Example 25-6 RHI MSFC Configuration

```
Host-Chassis(config)# firewall autostate
Host-Chassis(config)# firewall multiple-vlan-interfaces
Host-Chassis(config)# firewall module 9 vlan-group 9
Host-Chassis(config)# firewall vlan-group 9 10-100
Host-Chassis(config)# vlan 2-100,1000

Host-Chassis(config)# interface FastEthernet1/1
Host-Chassis(config-if)# switchport
Host-Chassis(config-if)# switchport access vlan 20
Host-Chassis(config-if)# switchport mode access

Host-Chassis(config)#interface FastEthernet1/2
Host-Chassis(config-if)# switchport
Host-Chassis(config-if)# switchport access vlan 21
Host-Chassis(config-if)# switchport mode access
```

The **firewall autostate** command sends messages from the host-chassis to the FWSM regarding the state of the VLANs associated with the FWSM. When an interface is

configured to be in the same VLAN as the FWSM, and in the event that physical interface transitions to a “down” state, information can be propagated to the FWSM, consequently “downing” the interface associated with the FWSM. When this happens, the RHI will no longer be propagated to the routing-engine on the host-chassis.

Example 25-7 shows the configuration of the context on the FWSM (only pertinent information is shown).

Example 25-7 *RHI FWSM Configuration*

```
FWSM/RHI(config)# interface Vlan20
FWSM/RHI(config-if)# nameif Outside
FWSM/RHI(config-if)# security-level 0
FWSM/RHI(config-if)# ip address 10.20.20.1 255.255.255.0
FWSM/RHI(config)#interface Vlan21
FWSM/RHI(config-if)# nameif Inside
FWSM/RHI(config-if)# security-level 100
FWSM/RHI(config-if)# ip address 192.168.1.1 255.255.255.0
FWSM/RHI(config)# route Outside 0.0.0.0 0.0.0.0 10.20.20.254 1
FWSM/RHI(config)# route-inject
FWSM/RHI(config)# redistribute static interface Inside
```

Under the route-inject subsection, the **redistribute** command also offers another great feature. You can apply an access list to static routes, NAT pools, and connected networks redistributed to the routing-engine on the host-chassis, consequently providing very granular control over which routes are redistributed.

From the FWSM, using the **show route-inject** command, you can verify that the route is being propagated to the routing-engine on the host-chassis, as shown in Example 25-8.

Example 25-8 *RHI on the FWSM*

```
FWSM/RHI# show route-inject
Routes injected:
Address      Mask           Nexthop      Proto  Weight  Vlan
-----
0.0.0.0     0.0.0.0       10.20.20.254 1      1       20
```

The host-chassis, using the **show ip route** command verifies that the route has been received, as shown in Example 25-9.

Example 25-9 *RHI on the MSFC*

```
Host-Chassis# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
```

Example 25-9 *RHI on the MSFC (Continued)*

```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

C    192.168.121.0/24 is directly connected, Vlan121
C    192.168.1.0/24 is directly connected, Vlan21
S*  0.0.0.0/0 [1/0] via 192.168.1.1, Vlan21

```

You can see that this route shows up as “static”. Now it can be redistributed into a dynamic routing protocol. In Example 25-10, we are using EIGRP.

Example 25-10 *Redistribution of RHI (Static) Routes on the MSFC*

```

router eigrp 1
 network 192.168.0.0 0.0.255.255
 no auto-summary
 redistribute static metric 1000 2000 255 1 1500

```

Downstream routers will now see that route in their local routing table, as shown in the output from the **show ip route** command in Example 25-11.

Example 25-11 *Downstream RHI Routes*

```

Downstream# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.121.1 to network 0.0.0.0

C    192.168.121.0/24 is directly connected, FastEthernet2/0
D    192.168.1.0/24 [90/28416] via 192.168.121.1, 00:48:10, FastEthernet2/0
D*EX 0.0.0.0/0 [170/28416] via 192.168.121.1, 00:47:09, FastEthernet2/0

```

When the FWSM interface goes down, the static route being redistributed into the routing-engine on the host-chassis will be removed.

NOTE

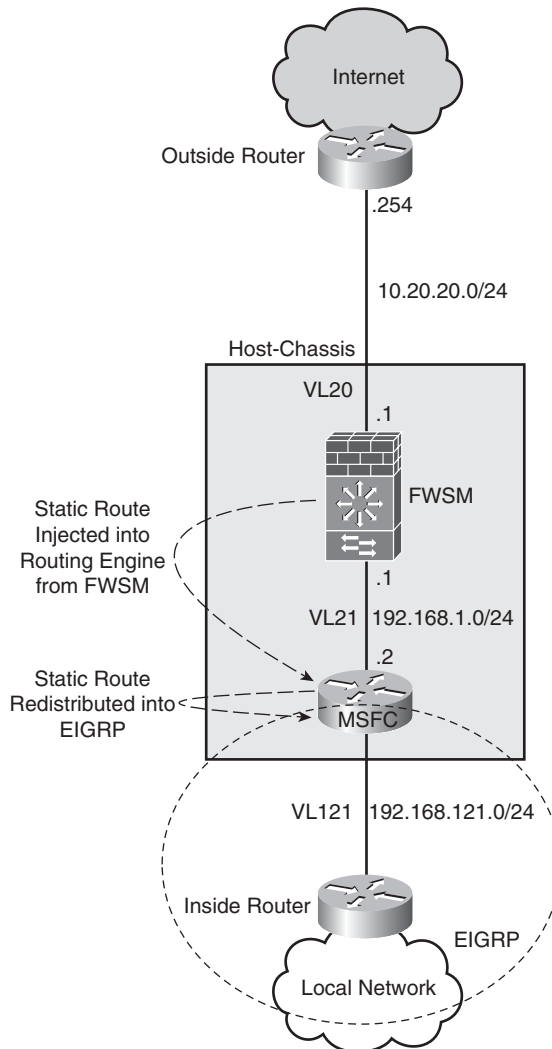
The automatic route removal feature will not be available on the initial release of 4.01 but will be part of the first maintenance release (4.02).

To really take advantage of the dynamic nature of RHI, only one interface should be assigned to the VLAN. In Example 25-11, interface FastEthernet1/1 is assigned to VLAN

20. In the event FastEthernet1/1 goes down, typically due to an upstream device or interface failure, the associated VLAN interface will also go down. If multiple interfaces have been assigned to the VLAN, all must go down to take down the interface of the FWSM. This completely nullifies the use for any type of dynamic changes.

Figure 25-2 shows a diagram of how RHI can be used.

Figure 25-2 *RHI Usage*



Although not really dynamic, it will automatically provide notification of the FWSM VLAN interface going down by removing the associated route. Something to be aware of is that it requires a physical failure. In the event the upstream had a Layer 3 problem, for example, the IP address changed, the VLAN interface would remain “up,” but traffic would drop because the next-hop would not be available. One other notable item is that the routes are not Virtual Routing and Forwarding (VRF) aware, meaning that it will not function with MPLS or VRF-lite (at least not using 4.01 code). Propagating routes from the FWSM to the routing-engine on the host-chassis will be placed in the “global” routing table.

NOTE Removal of routes using RHI requires that the VLAN on the FWSM must be down.

RHI helps to overcome the limitation that dynamic routing processes are not supported when the FWSM is operating the multi-context mode. Recognize that it requires a Layer 2 failure of the selected interface to retract routing information sent to the MSFC. Although some limitations exist, RHI is an excellent feature to have in your “tool kit.”

Understanding Application Support

The release of FWSM 4.01 code introduces a very powerful feature with regular expressions. Regular expressions allow you to match a variety of parameters using strings or variables that you assign. Also, four additional inspection engines have been added: DCEPRC, ESMTP, HTTP, and SIP.

NOTE For more information on DCEPRC, ESMTP, HTTP, and SIP, read on! The topics are covered later in this chapter.

Configuring Regular Expressions

If you have had an opportunity to work with Border Gateway Protocol (BGP), you may have been introduced to regular expressions. Regular expressions provide a way to match a group of characters using either an exact string match or by meta-characters that allow you to define a range, a character set, and so on. This feature can be used to match URL strings when inspecting HTTP traffic and perform an action based on a match, or perform an action on the traffic that does not match the regular expression.

The following configuration example shows how to implement regular expression matching. A client on the inside is connecting to a server on the outside. In this example,

you will be inspecting the content for the permutation of the keyword “flash.” If the keyword is found, the connection will be reset.

Step 1 The first step requires that you create a regular expression to match the specific content. Ensure that the regular expression command matches on the keywords of Flash, FLash, fLASH, and so on:

```
regex URL_NOFLASH "[Ff][Ll][Aa][Ss][Hh]"
```

Step 2 Create and set a regular expression (regex) class map to match the regular expression (URL_NOFLASH):

```
class-map type regex match-any RESTRICTED_URL
match regex URL_NOFLASH
```

Step 3 Add an inspection class map to match the previously created class map (RESTRICTED_URL):

```
class-map type inspect http match-all RESTRICTED_HTTP
match request uri regex class RESTRICTED_URL
```

Step 4 Add a policy map to search through the body of the HTTP string. The numeric value of 48 specifies how many characters to search through. The maximum length of the string can be from 1 to 4,294,967,295 characters. Longer search strings will impact the performance of the FWSM. When a match is found, using the class map RESTRICTED_HTTP, the action assigned is to reset and log the connection:

```
policy-map type inspect http HTTP_PMAP
parameters
  body-match-maximum 48
class RESTRICTED_HTTP
  reset log
```

CAUTION Longer search strings will impact the performance of the FWSM.

Step 5 Create and use a final policy map to match the policy map (HTTP_PMAP):

```
policy-map INSIDE_POLICY
class inspection_default
inspect http HTTP_PMAP
```

Step 6 Apply the service policy to the interface:

```
service-policy INSIDE_POLICY interface Inside
```

When a match is found, the following log message is generated:

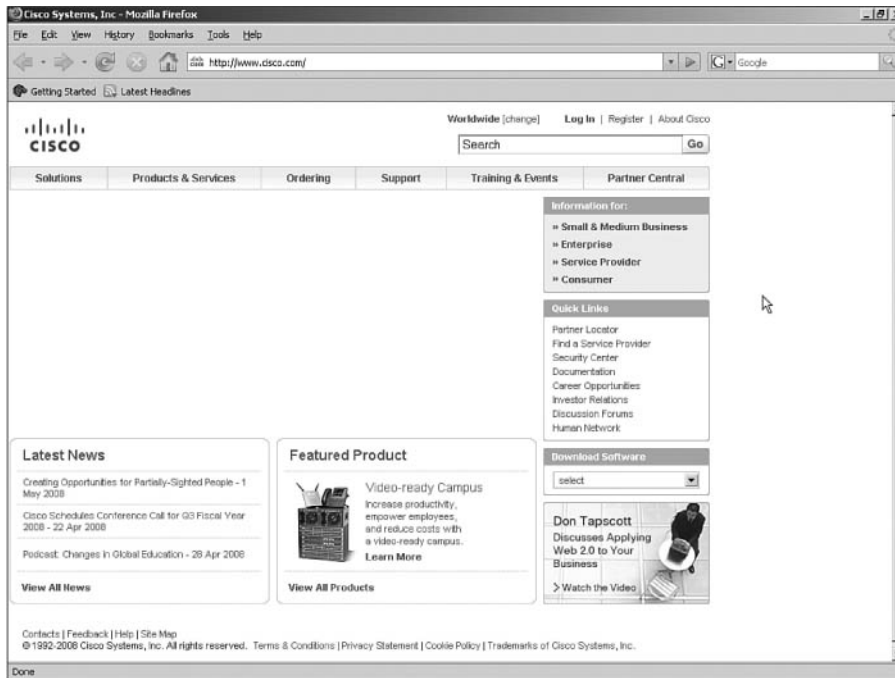
```
%FWSM-5-415006: HTTP - matched Class 23: RESTRICTED_HTTP in policy-map
HTTP_PMAP, URI matched - Resetting connection from
Inside:192.168.1.23/3898 to Outside:10.133.219.25/80
```

Figure 25-3 shows a screenshot of what the client's experience would be without the service policy.

Figure 25-3 *Regular Expression Without the Service Policy*



Figure 25-4 shows a screenshot of what the client's experience would be with the service policy.

Figure 25-4 *Regular Expression with the Service Policy*

Notice now that the graphic has been removed from the display.

There is also a simple tool that you can use to test a regular expression from the command line. Use the following test command:

```
FWSM# test regex http://www.cIsCo123.com [Cc][Ii][Ss][Cc][Oo][0-9]
INFO: Regular expression match succeeded.
```

The first argument is the string, and the second argument is the match criteria. Notice that both upper and lowercase characters will match the string “cIsCo” but must be followed by a numeric value.

In the next example, the hyphen does not match a numeric value, consequently the match fails.

```
FWSM# test regex http://www.cIsCo-123.com [Cc][Ii][Ss][Cc][Oo][0-9]
INFO: Regular expression match failed.
```

Regular expressions are a very helpful tool that could be used to match on viruses, worms, questionable material, and so on. A maximum of 100 characters can be used in the regular expression; remember that implementing regular expressions will impact the performance of the FWSM.

Inspecting content within a packet and matching against a user defined regular expression is a very powerful feature. Because additional CPU cycles are required when you employ this feature, use caution that you do not overwhelm the processor on the FWSM. As an alternative to the FWSM for high-performance regular expression matching, consider using an Intrusion Prevention System (IPS).

Understanding Application Inspection Improvements

One of the primary functions of the FWSM is to provide application inspection, looking for protocol conformance, changing imbedded IP addressing, and so on. Increasing the capabilities of this feature only adds benefit to the services you are offering to your customers.

Domain Name Service (DNS) guard is a feature used when a client requests DNS information through the FWSM to a DNS server or servers. The default behavior of the FWSM is to allow only a single reply and drop any additional responses, consequently helping to prevent against DNS poisoning attacks. Although not recommended because of the possibility of exploiting the host, the FWSM can be configured to allow all responses using the following command:

```
FWSM/Context-A(config)# no dns-guard
```

As you may have noticed from the preceding command syntax, this command also works in multi-context mode.

Policy maps are covered in detail in Chapter 11, “Modular Policy,” but the introduction of 4.01 includes additional support/enhancements for inspection policy and/or class maps for the following applications:

- **Distributed Computing Environment Remote Procedure Call (DCEPRC):** A protocol used across multiple computers to distribute the load. Policy map inspection is the new addition to 4.01.
- **Extended Simple Mail Transfer Protocol (ESMTP):** Added extensions to SMTP. The 4.01 code added the capability for application support and the capability to define inspection policy maps that match traffic using regular expressions.
- **HTTP:** A protocol used generally to transfer information across the Internet.
- **Session Initiation Protocol (SIP):** A signaling protocol used for voice communications over IP.

The following options are available using policy maps with the previously listed protocols, as follows:

- **drop:** Drops all packets that match the defined pattern.
- **drop-connection:** Drops the packet and closes the connection.
- **log:** Sends a syslog message.

- **mask:** Masks that portion of the packet that has been matched.
- **rate-limit:** Limits the rate of received messages.
- **reset:** Drops the packet; closes and resets the connection.
- **send-protocol-error:** Sends an error message when the packet does not match the ESMTP protocol.

The capability added with policy maps for DCEPRC, ESMTP, HTTP, and SIP adds tremendous functionality for the inspection of these protocols. With the option to drop, drop-connection, log, mask, rate-limit, reset, and send-protocol-error, for many of these protocols, the functionality also significantly improves.

Additional Support for Simple Network Management Protocol Management Information Base

Simple Network Management Protocol (SNMP) is used to get specific information from a device or to send it information for the purposes of configuration changes. Because the FWSM is a security device, you cannot send it information, but you can gather information for keeping track of interface statistics, packet counts, and so on. There have been two additions to the Management Information Base (MIB):

- ACL entries and hit counters located under CISCO-IP-PROTOCOL-FILTER-MIB
- Address Resolution Protocol (ARP) table entries located under IP-MIB

Table 25-1 shows the MIB additions with definitions.

Table 25-1 FWSM 4.01 MIB Additions

CISCO-IP-PROTOCOL-FILTER-MIB	cippfIpFilterTable	Command Line Interface (CLI) show run access-list
1.3.6.1.4.1.9.9.278.1.1.1.1.1	cippfIpProfileName	ACL name
1.3.6.1.4.1.9.9.278.1.1.3.1.1	cippfIpFilterIndex	Access Control Entry (ACE) line number
1.3.6.1.4.1.9.9.278.1.1.3.1.3	cippfIpFilterAction	Permit/Deny
1.3.6.1.4.1.9.9.278.1.1.3.1.4	cippfIpFilterAddressType	Either ipv4 or ipv6
1.3.6.1.4.1.9.9.278.1.1.3.1.5	cippfIpFilterSrcAddress	Source IP addr
1.3.6.1.4.1.9.9.278.1.1.3.1.6	cippfIpFilterSrcMask	Source IP mask
1.3.6.1.4.1.9.9.278.1.1.3.1.7	cippfIpFilterDestAddress	Destination IP addr
1.3.6.1.4.1.9.9.278.1.1.3.1.8	cippfIpFilterDestMask	Destination IP mask
1.3.6.1.4.1.9.9.278.1.1.3.1.9	cippfIpFilterProtocol	Protocol (IP/TCP/UDP/ICMP)
1.3.6.1.4.1.9.9.278.1.1.3.1.10	cippfIpFilterSrcPortLow	Src port low
1.3.6.1.4.1.9.9.278.1.1.3.1.11	cippfIpFilterSrcPortHigh	Src port high

Table 25-1 FWSM 4.01 MIB Additions (Continued)

CISCO-IP-PROTOCOL-FILTER-MIB	cippfIpFilterTable	Command Line Interface (CLI) show run access-list
1.3.6.1.4.1.9.9.278.1.1.3.1.12	cippfIpFilterDestPortLow	Dest port low
1.3.6.1.4.1.9.9.278.1.1.3.1.13	cippfIpFilterDestPortHigh	Dest port high
1.3.6.1.4.1.9.9.278.1.1.3.1.16	cippfIpFilterLogEnabled	Log enabled/disabled
1.3.6.1.4.1.9.9.278.1.1.3.1.17	cippfIpFilterStatus	ACL Active/Inactive
1.3.6.1.4.1.9.9.278.1.1.3.1.22	cippfIpFilterSrcIPGroupName	Src n/w object group name
1.3.6.1.4.1.9.9.278.1.1.3.1.23	cippfIpFilterDstIPGroupName	Dest n/w object group name
1.3.6.1.4.1.9.9.278.1.1.3.1.24	cippfIpFilterProtocolGroupName	Protocol object group name
1.3.6.1.4.1.9.9.278.1.1.3.1.25	cippfIpFilterSrcServiceGroupName	Src service object group name
1.3.6.1.4.1.9.9.278.1.1.3.1.26	cippfIpFilterDstServiceGroupName	Dest service object group name
1.3.6.1.4.1.9.9.278.1.1.3.1.27	cippfIpFilterICMPGroupName	ICMP object group
	cippfIpFilterStatsTable	CLI show access-list acl-name
1.3.6.1.4.1.9.9.278.1.1.1.1.1	cippfIpProfileName	ACL name
1.3.6.1.4.1.9.9.278.1.1.3.1.1	cippfIpFilterIndex	ACE line number within the ACL
1.3.6.1.4.1.9.9.278.1.2.1.1.1	cippfIpFilterHits	ACE hit-count
IP-MIB(RFC2011)	ipNetToPhysicalTable	CLI show arp
1.3.6.1.2.1.4.35.1.1	ipNetToPhysicalIfIndex	Interface number for the ARP entry
1.3.6.1.2.1.4.35.1.2	ipNetToPhysicalNetAddressType	IP address type for the ARP entry
1.3.6.1.2.1.4.35.1.3	ipNetToPhysicalNetAddress	IP address for the ARP entry
1.3.6.1.2.1.4.35.1.4	ipNetToPhysicalPhysAddress	Media Access Control (MAC) address for the IP address

When using SNMP, avoid using `ansnmp walk`. This process will start at the top of the MIB tree and get the statistics for each MIB, until it gets to the end of the tree. Because SNMP is not performed in hardware, this will put an undue burden on the FWSM.

NOTE

Gathering SNMP information from the FWSM will increase the load. Get only specific information when necessary.

SNMP is a very valuable tool to gather statistics from the FWSM, and with the addition of ACL entries, ACL counters, and ARP table entries, it becomes an even better tool. Just remember not to overwhelm the FWSM with too many queries.

Miscellaneous Security Features

DHCP option 82 is typically used in service-provider networks. It adds location information that can be used to differentiate services between customers. A filtering enhancement was also added to support HTTPS with SmartFilter.

Dynamic Host Configuration Protocol Option 82

Option 82 provides location information from the Dynamic Host Configuration Protocol (DHCP) relay agent—in this case, the FWSM to the DHCP server. This information can be used to differentiate DHCP clients, consequently offering distinctive services on a client basis.

You can use two commands to enable DHCP relay. The first command specifies the DHCP server IP address and the interface where it is located. Optionally, the **dhcprelay server *ip_address*** command can be configured under the outgoing interface. The second line enables clients on the inside interface to send and receive DHCP information.

```
FWSM/Context-A(config)# dhcprelay server 10.20.100.25 Outside  
FWSM/Context-A(config)# dhcprelay enable Inside
```

Option 82 can then be enabled on a specific interface, as shown by the following two commands:

```
FWSM/Context-A(config)# interface vlan vlan-number  
FWSM/Context-A(config-if)# dhcprelay information trusted
```

Option 82 can also be enabled on all interfaces using the global command that follows:

```
FWSM/Context-A(config)# dhcprelay information trust-all
```

If you are currently using the FWSM as a DHCP relay agent, the addition of option 82 will be a simple addition. Also, when enabling option 82 globally, all interfaces are trusted except the interface that is configured as the dhcprelay (outgoing) interface.

DHCP option 82 adds location information to clients, which can be used to differentiate services. Although used primarily in service provider networks, it could all be used in enterprise networks to differentiate client services.

Smartfilter HTTPS Support

For those of you looking for HTTPS support from SmartFilter on the FWSM, it has now arrived with the introduction of 4.01. See Chapter 14, “Filtering,” for configuration details.

Summary

The release of 4.x adds some very significant enhancements. The addition of EIGRP now provides the capability to integrate a FWSM into an EIGRP network without having to redistribute routes into other routing protocols. RHI allows static routes, NAT pools, and connected routes to be propagated to the routing engine on the host-chassis dynamically. Regular expressions give you the opportunity to match traffic based on custom signatures. Application inspection improvements and SNMP additions, option 82 support, and filter enhancements, make the FWSM an even better option to secure your valuable assets.

References

- RFC 1869—*SMTP Service Extensions*
- RFC 2011—*SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*
- RFC 3046—*DHCP Relay Agent Information Option 82*

Numerics

3DES, 253

6-gigabit EtherChannel (GEC), 26

6500/7600 chassis

configuration and security, 89

interaction with FWSM, 89, 92

securing

access control with port-based security, 99

ACLs, 100

Autosecure, 101

Control Plane Policing, 101

description, 94

environmental concerns, 95

layer 3, 100

management access, 96

physical access control, 95

Quality of Service, 101

spanning tree control, 99

unnecessary services, disabling, 97

A

AAA (authentication, authorization, and accounting)

accounting, 172

authentication, 171

authorization, 172

cut-through proxy, 178

fallback authentication, 175

fallback support, 175

local authorization, 177

MAC address authentication, 181

overview, 171

two step authentication, 175

ABRs (Area Backbone Routers), 140

access control lists. *See* ACLs,

access-list command, 126

ACE (application control engine), 313

ACEs (access control entries), 127

acknowledgement (ACK) flag, 350

ACLs (access control lists)

access list commit, 128

access list resources, monitoring, 129

access lists, 185, 377

ACEs (access control entries), 127

ACL types, 125

definition, 5, 100

EtherType Access Control Lists, 35

EtherType object groupings, 131

and higher-level interfaces, 54

inbound and outbound traffic flow control

examples, 131

IPv6 configuration, 334

nesting type object groupings, 130

network type object groupings, 130

object group and access list configurations, 129

object groups, 128

optimization, 464

protocol type object groupings, 129

service type object groupings, 130

traffic filtering, 125

uses in FWSM, 125

Active/Active mode, 198

Active/Standby Failover Configuration, 205

Active/Standby mode, 197

ActiveX controls, security risks, 235

ActiveX filtering, 241

Adaptive Security Appliance (ASA), 25

Adaptive Security Device Manager (ASDM), 249

Address Resolution Protocol (ARP) traffic, 36

admin context configurations, 112

admin-context, 75

allocate-interface command, 76

Anycast IPv6 addressing, 329

Anycast RP, 267

application engines, 187, 189

application inspection, 481. *See also* modular policy

application layer, 7

application protocol inspection

ARP inspection, 230

FTP (File Transfer Protocol), 222

HTTP (Hypertext Transfer Protocol), 220

primary functions, 219

supported application inspection engines,

224–225, 229

application/proxy firewalls, 7

areas, 139

ARP (Address Resolution Protocol), 36, 229

ARP table entries, displaying, 232
ARP test, 202
AS external ASBR summary link LSAs, 141
ASA (Adaptive Security Appliance), 25
ASBRs (Autonomous System Routers), 140
ASDM (Adaptive Security Device Manager), 249, 368
assignment of interfaces, 92
asymmetric routing
 avoiding through firewalls, 290
 configuration, 297
 and firewall design, 297
 NAT and, 287
 support
 between two contexts in active/active failover mode, 296
 in Active/Active mode, 295
 in active/standby mode, 294
 in FWSM, 292, 294
 in multiple context routed mode, 298–301
 with firewalls, 287, 289
 without firewalls, 287
Auto-RP, 267
Autosecure, 101
availability, 384

B

backbone routers, 140
BGP (Border Gateway Protocol)
 context A configuration in FWSM, 162
 context B configuration in FWSM, 164
 description, 158
 FWSM configuration, 159, 161
 limitations, 159
 message type states, 158
 router 1 configuration, 160
 stub configuration, 160
 summaries of neighbors, 168
 topology, 159
Bidirectional PIM, 266
BPDU (bridge protocol data units), 35
Bridge-Group Virtual Interface (BVI), 117
bridge groups, 35, 45
broadcast multi-access network type, 138
broadcast ping test, 202
BSR (Bootstrap Router), 267

buffer overflow, 10
BVI (Bridge-Group Virtual Interface), 117
BVI IP addressing, 37

C

capture command, 363
changeto command, 78
Cisco Adaptive Security Device Manager (ASDM), 249, 368
Cisco Security Manager (CSM), 260, 368
class maps, 185, 220
CLI (command-line interface), 245
Computer Telephony Integration Quick Buffer Encoding, 29
configuration of multiple routing and firewall instances, 384, 386–399
configuration, FWSM, 105
config-url, 76
connection limits, 351
content switch module (CSM), 307
context configurations, 111
contexts
 adding contexts, 75–76
 changing between contexts, 78
 configuration files, 77
 definition, 73, 384
 multiple contexts, advantages, 74
 multiple contexts, disadvantages, 74
 removing contexts, 77
CPP (Control Plane Policing), 101
crackers, 6
CSM (Cisco Security Manager), 260, 368
CSM (content switch module), 307
CTIQBE (Computer Telephony Integration Quick Buffer), 29
cut-through proxy, 178

D

datacenter, deploying FWSM in, 383
data-link layer, 8
DCEPRC (Distributed Computing Environment Remote Procedure Call) policy map options, 481
debug command, 362, 365

debug crypto isakmp command, 256
deep-packet inspection, 12
default inspect ftp configuration removal, 222
default inspection traffic, 185
default policy map, 190
Default Route Updates mode, 154
default routing, 137
default-information originate option, 144
dense mode PIM, 266
DES (Data Encryption Standard), 253
design scenarios

- data center environments
 - description, 430*
 - Layer 3 VPN segregation with Layer 2 FWSM, 432*
 - Layer 3 VPN segregation with Layer 3 FWSM, 430–431*
- dynamic learning of routes with FWSM
 - methods, 424–425*
 - OSPF single box solution, 425, 427–429*
- failover configuration in mixed mode
 - description, 408*
 - primary and secondary block switch configuration, 410*
 - primary FWSM system context configuration, 411–415*
- interdomain communication between security zones through one FWSM
 - description, 415*
 - FWSM configuration, 418–423*
 - PFC configuration, 416*
- Layer 3 VPN terminations at FWSM, 405
 - description, 401–402*
 - FWSM configuration, 406–407*
 - PFC configuration, 405*
- network virtualization, 401
- network virtualization solutions, 402
- primary and secondary block switch configuration, 410
- PVLAN
 - configuration, 438–444*
 - configuration in FWSM, 435*
 - description, 434*
 - scenario 1, 435*
 - scenario 2, 436*
- VRF, 401–402, 404

designated router, 267

DHCP (Dynamic Host Configuration Protocol)

- relay agent, 484

dhcrelay server ip_address command, 484
DNS (Domain Name Service), 62
DNS (Domain Name System), 29
DNS guard, 481
dynamic NAT, 67
dynamic PAT, 67

E

eBGP (external BGP), 158
egress interface, 135
EIGRP (Enhanced Interior Gateway Routing Protocol)

- configuration, 469
- context, 47
- EIGRP and OSPF route redistribution, 470
- single context mode, 469

embryonic connections, 61
enable password, 177
enabling timestamps, 362
Enhanced Interior Gateway Routing Protocol.
See EIGRP
ESMTP (Extended Simple Mail Transfer Protocol), 30
ESMTP policy map options, 481
EtherType access control lists (ACL), 35, 126
EtherType object groupings, 131
EXCLUDE List, 269
extended access list, 126
Extended Simple Mail Transfer Protocol.
See ESMTP
external link LSAs, 141

F

failover

- Active/Active mode, 198
- Active/Standby mode, 197
- configuring multiple context failover, 212, 214–217
- configuring poll intervals, 203
- configuring single context FWSM failover, 205, 207–212

- design principles for monitoring interfaces, 203
- failover link and state link, 199
- monitoring interfaces, 202
- primary and secondary firewall
 - synchronization, 201
- and redundancy, 197
- requirements, 201

fallback support in AAA configurations, 175

File Transfer Protocol (FTP), 29, 222

filter activex command, 241

filter url command, 239

filtering, 235–236, 238–240, 242

firewall autostate command, 473

firewall load balancing

- configuration example, 318
- design requirements, 304
- firewall configuration
 - FWSM1 configuration, 320*
 - FWSM2 configuration, 322*
 - IN2OUT policy configuration, 323*
 - MSFC configuration, 319*
- justification, 303
- purpose, 303
- redundancy, 304
- with content switch module, 307
- with policy-based routing, 305
- with the application control engine, 313

firewall multiple-vlan-interfaces command, 91

Firewall Services Module. *See* FWSM

firewalls

- application/proxy firewalls, 7
- failover configuration in mixed mode, 408
- IP addresses, reuse of, 13
- packet-filtering firewalls, 5
- packet-inspection firewalls, 12
- reverse-proxy firewalls, 10
- summary, 16
- types, 5

fixup command, 219

flexibility, 383

FTP (File Transfer Protocol), 29, 222

FTP filtering, 235, 240

ftp map, 222

FWSM (Firewall Services Module)

- compared to other security options, 24
- configuration in the switch, 105
- hardware architecture, 26–28

- installation, 20
- overview, 19
- performance, 22
- and security policy, 5
- software architecture, 29–31
- summary, 31
- virtualization, 23

FWSM Only, 382

FWSM-sandwich in routed-mode, 380

FWSM-sandwich in transparent-mode, 380

G

GEC (6-gigabit EtherChannel), 26, 89

General Packet Radio Service (GPRS) Tunneling Protocol (GTP), 29

global command, 67

global policy, 189

global_policy, 352

Global Routing prefix, 329

Global scope, IPv6 addresses, 329

GRE (generic routing encapsulation), multicast configuration through firewalls, 276

GRE tunnels, 402

Group Specific queries, 268

GTP (General Packet Radio Service Tunneling Protocol), 29

H

H.323, 29

hackers, 6

hardware architecture of FWSM, 26–28

HTTP (Hypertext Transfer Protocol), 29, 220

HTTP filtering, 240

HTTP policy map options, 481

http-map, 220

Hypertext Transfer Protocol. *See* HTTP

I

iBGP (internal BGP), 158

ICMP (Internet Control Message Protocol), 29

idle time parameters, 352

IGMP (Internet Group Management Protocol)
 versions, 268
IGMP join messages and requests, 266
ILS (Internet Locator Service), 29
IN2OUT policy configuration, 323
 inactive keyword, 126
INCLUDE Lists, 269
 inspect command, 187, 219
 interdomain communication between security zones, 415
Interface ID, 329
 interfaces, assignment to VLANs, 92
 internal routers, 139
Internet Control Message Protocol (ICMP), 29
Internet Locator Service (ILS), 29
Internet Operating System Firewall (IOS FW), 25
Inverse Neighbor Discovery, 330
IOS FW (Internet Operating System Firewall), 25
IP addresses, reusing, 13
ip bgp command, 168
ip pim bsr-candidate command, 267
ip route statement, 136
IP traffic, 36
ip verify reverse-path command, 350
ip verify statistics command, 350
IPv6 (IP version 6)
 address scope, 329
 address types, 329
 configuration
 ACL configuration, 334
 ACL verification, 343
 displaying routers, 342
 duplicate address detection, 333
 FWSM, 337
 ICMP traffic, 334
 in FWSM, 335
 interface, 331
 IPv6 timers, 334
 layer 3 devices on the inside security domain, 338
 PFC on the outside security domain, 336
 show command, usage of, 340
 static routes, 334
 verifying functionality, 339
 description, 327

and FWSM, 330
 global unicast address structure, 329
 NDP (Neighbor Discovery Protocol), 329
 packet headers, 327
ipv6 enable command, 332

J

Java filtering, 241
Java, security risks, 235

K

Keepalives, 158

L

L2TPv3 (Layer 2 Tunneling Protocol version 3), 402
Layer 2 mode, 35
Layer 3 security, 100
Layer 3 VPNs, 401
 layers of the OSI model, 7
Leave Group messages, 268
Link Up/Down test, 202
Link-local scope, IPv6 addresses, 329
load balancing, 26, 136. *See also* firewall load balancing
local authorization, 177
local keyword, 178
logging, 362
LSAs (link-state advertisements), 137, 141

M

MAC address authentication, 181
MAC entry configuration for ARP, 231
man-in-the-middle attacks, 229
MARS (Monitoring Analysis and Response System), 262
MD5 (Message Digest 5), 253
Media Gateway Control Protocol (MGCP), 30
memory allocation and partitioning, 458

memory allocation rules, 461
memory partitions, 80–85
MGCP (Media Gateway Control Protocol), 30
MIB (Management Information Base), 482
mixed mode contexts, 73
mode multiple command, 75
modes of operation, 35
modular policy
 application engines, 187
 default policy map, 190
 description, 183
 global policy configuration, 189
 policy maps, 189
 sample configuration, 191
 service policy configuration, 190
 traffic classification, 185
 using in FWSM, 183
module command, 107
monitor command, 202–203
MPLS Layer 3 VPNs, 402
MSDP (Multicast Source Discovery Protocol), 267
MSFC, 90
multicast
 configuration methods
 multicast through firewall in single context routed mode, 273
 multicast through firewall via GRE, 276
 multicast through transparent firewall in multiple context mode, 279
 description, 265
 feature matrix for FWSM 3.x code release, 270
 and FWSM 1.x and 2.x code releases, 269
 FWSM 3.x code release, 270
 IGMP versions, 268
 multicast stub configuration, 269
 multicast traffic across firewalls, 269
 multicast tree, 265
 PIM interface modes, 268
 protocol independent multicast, 265
 Rendezvous Point (RP), 267
 supporting multicast traffic across FWSM, 272
Multicast IPv6 addressing, 329
multi-context mode, 377
multiple bridge groups, 45
multiple context configuration, 35
multiple context mixed mode configuration, 119
multiple context mode, 109, 111

Multiple-context routed-mode inside/outside, 379
Multiple-context transparent-mode inside/outside, 380
multi-VRF, 402

N

NA (Neighbor Advertisement), 330
NAM (Network Analysis Module), 365
nameif command, 115
NAT (Network Address Translation)
 description, 13–14, 55
 disabling for non-NAT, 57
 dynamic NAT, 67
 NAT 0 or identity NAT, 68
 NAT bypass, 68
 NAT control, 67
 Static identity NAT, 68
 static NAT, 58
NBAR (Network-based Application Recognition), 453
NBMA (Non-Broadcast Multi-access) network type, 138
NDP (Neighbor Discovery Protocol), 329
nesting type of object grouping, 130
NetBIOS (Network Basic Input/Output System), 30
NetBIOS security-level dependency, 54
network activity test, 202
Network Address Translation. See NAT
network attacks, preventing, 345
Network Basic Input/Output System (NetBIOS), 30
network design
 considerations, 375
 deployment options, 377
 documenting the process, 376
 enterprise perimeter and the FWSM, 382
 placement, determining, 378
 planning, 375–378, 380, 382
network layer, 8
network link LSAs, 141
Network Management Protocol (SNMP), 30
network summary link LSAs, 141
network type object groupings, 130
network virtualization, 401

next hop address selection, 135
 not so stubby area, 141
 Notifications, 158
 NS (Neighbor Solicitation), 330
 NSSA configuration, 144
 NSSA External LSAs, 141

O

object groups, 128
 configuration, 129
 description, 128
 groupings
 by Ethertype, 131
 by nesting type, 130
 by network type, 130
 by protocol type, 130
 by service type, 130

Open Messages, 158
Open Shortest Path First. See OSPF
Open System Interconnection (OSI) model, 7
operational modes, FWSM
 routed mode, 46–47, 50
 transparent mode, 35–37, 39, 41–42, 44–46

OraServ security-level dependency, 54
OSI (Open System Interconnection) model, 7
OSPF (Open Shortest Path First) protocol
 areas, 139
 areas, summarization between, 143
 configuration, 142
 default routing information, 144
 description, 47, 137
 design example one, 144, 146–153
 design example two, 149
 in FWSM, 141
 interface-based configuration, 142
 LSAs, 137, 140
 network types, 138
 packets, 138
 stub area types, 141
 timers, 144

OUT2IN policy configuration, 319
outside static NAT, 59

P

packet classifier, FWSM context mode, 112
packet flow, 135
packet forwarding process, 135
packet-filtering firewalls, 5
packet-inspection firewalls, 12
PACLs (Port Access Control Lists), 100
Passive RIP mode, 154
password recovery, 369
PAT (Port Address Translation)
 description, 13, 15, 55
 dynamic PAT, 67
 static PAT, 64

PBR (Policy Based Routing), 91
PFC (Policy Feature Card), 335
PFC configuration, 116, 405
physical layer, 8
PIM (protocol independent multicast), 265
PIM dense mode, 266
PIM interface modes, 268
ping command, 339, 365
PISA (Programmable Intelligent Services Accelerator), 449, 453
PIX (Private Internet Exchange), 25
point-to-multipoint network type, 138
point-to-point network type, 138
Point-to-Point Tunneling Protocol (PPTP), 30
Policy Feature Card. See PFC
policy maps
 configuring global policy, 189
 configuring service policy, 190
 default policy map, 190
 description, 189

poll interval configuration, 203
port 23 configuration, 220
Port Access Control Lists (PACLs), 100
Port Address Translation (PAT), 13, 15
PPTP (Point-to-Point Tunneling Protocol), 30
preempt command, 215
presentation layer, 7
Private Internet Exchange (PIX), 25
proxy-blocking, 239

Q

QoS (Quality of Service), 101
 Queries, 268

R

RA (Router Advertisement), 330, 333
 RACLs (Routed-interface Access Control Lists), 100
 RADIUS security protocol, 173
 RaLFD (rapid link failure detection), 202
 Real-Time Streaming Protocol (RTSP), 30
 Redirect message, 330
 redistribute command, 474
 redundancy and disaster recovery, 197
 regular expressions, 477–478, 480
 Remote Shell (RSH), 30
 Reports, 268
 resource management, 79
 resource management in contexts, 113
 reverse-proxy firewalls, 10
 RHI (Route Health Injection)
 configuration, 473
 RIP (Routing Information Protocol)
 configuration example, 154–158
 context mode support, 47
 description, 154
 in FWSM, 154
 route classification, 469
 routed mode
 advantages and disadvantages, 48
 description, 48, 50, 108, 377
 multicast and, 270
 operation, 46–47, 50
 traffic from higher-level to lower-level, 54
 Routed-interface Access Control Lists (RACLs), 100
 router link LSAs, 141
 Routing Information Protocol. *See* RIP
 routing protocols
 configuring, 135
 default routing, 137
 FWSM, supported in, 136
 OSPF. *See* OSPF
 securing, 100
 static routing, 136

RP (Rendezvous Point), 267
 RPF (reverse path forwarding), 266
 RS (Router Solicitation), 330
 RSH (Remote Shell), 30
 RTSP (Real-Time Streaming Protocol), 30
 rule command, 463
 rules allocations, single and multiple context modes, 127

S

SCCP (Skinny Call Control Protocol), 30
 script kiddies, 6
 Secure Computing Smartfilter, 235
 secure shell version 2 (SSHv2), 247–248
 security level command, 53
 security levels, 53, 70
 security protocols, comparing, 173
 security risks of ActiveX controls, 235
 service type object groupings, 130
 service-acceleration parameter, 451
 service-policy commands, 190
 Session Initiation Protocol (SIP), 30
 session layer, 8
 set connection advanced-options service-acceleration option, 451
 Shared interfaces in routed-mode, 382
 shared outside interface mode, 112
 shared tree, 266
 show conn command, 353
 show eigrp neighbors command, 472
 show etherchannel load-balance module command, 26
 show failover command, 217
 show firewall command, 115
 show ip bgp summary command, 168
 show ip route command, 474
 show ipv6 access-list, 343
 show ipv6 interface command, 332
 show ipv6 routers command, 342
 show ipv6 traffic command, 341
 show mls netflow ip sw-installed command, 452
 show mode command, 115
 show module command, 92, 105
 show np 3 acl count 1 command, 463
 show ospf database command, 151
 show ospf interface command, 472

- show ospf neighbor command, 472
- show resource acl-partition command, 462
- show resource partition command, 459
- show resource rule partition number command, 461
- show route-inject command, 474
- show running-config command, 191
- show url-block block statistics command, 236
- show url-server statistics command, 238
- shun command, 347
- Simple Mail Transfer Protocol (SMTP), 30
- single context mode, 109, 377
- single context routed mode configuration, 114
- single context transparent mode configuration, 116
- Single-context routed-mode inside/outside, 378
- Single-context transparent-mode inside/outside, 379
- SIP (Session Initiation Protocol), 30
- SIP (Session Initiation Protocol) policy map options, 481
- Skinny Call Control Protocol (SCCP), 30
- SMTP (Simple Mail Transfer Protocol), 30
- SNMP (Simple Network Management Protocol), 30, 257, 482
- software architecture of FWSM, 29–31
- source tree, 266
- spanning tree, 99
- Sparse mode PIM, 266
- SPF (Shortest Path First) algorithm, 137
- spf-delay and spf-holdtime timers, 144
- Split Horizon and Split Horizon with Poison Reverse, 154
- spoofing, 349
- SSL (Secure Sockets Layer)
 - termination in reverse-proxy, 10
- SSM (Source Specific Multicast), 267
- standard access list, 126
- state link, 200
- stateful failover, 200
- static ARP table entries, 231
- static command
 - allowable number of TCP connections, 63
 - allowable number of UDP connections, 63
 - description, 58
 - DNS record, rewriting, 62
 - embryonic command, 61
 - norandomseq option, 62
 - simultaneous TCP connections, 61
- static NAT, 58
- static outside NAT, 60
- static PAT, 64
- static routing, 136
- Static RP, 267
- Structured Query Language SQL*Net/Net8, 30
- stub area, 141
- stub configuration, 143
- Subnet ID, 329
- summarization, 143
- summary-address command, 143
- Sun's Remote Procedure Call (SunRPC), 30
- supervisor acceleration. *See* Trusted Flow Acceleration
- SVIs (Switch Virtual Interfaces), 107
- Switch Virtual Interfaces (SVIs), 107
- symmetric routing
 - with redundancy, 292
 - without redundancy, 290
- Synchronize Sequence Number (SYN) flag, 350
- Syslog, 258
- system context configurations, 111

T

- TACACS+ security protocol, 173
- TCAM (Ternary Content Addressable Memory), 450
- TCP timeout, 184
- Telnet, 245
- TFTP (Trivial File Transfer Protocol), 30
- throughput, 383
- timeout command, 352
- timeouts, 351
- timeouts, configuring, 352
- time-range command, 126
- timestamps, enabling, 362
- totally stubby area, 141
- traffic classification, 185
- traffic flow between interfaces, 54
- traffic management protocols, 29
- transparent mode
 - advantages, 37
 - description, 39, 46, 109, 377

- disadvantages, 40
- inside to outside example, 41
- multiple bridge groups, 45
- operation, 35–37, 41–42, 44–45
- outside to inside example, 43
- traffic flow, 40
- traffic from higher-level to lower-level, 54

transparent layer, 8**Trivial File Transfer Protocol (TFTP), 30****troubleshooting**

- assessing issues, 357
- connectivity testing, 360
- FAQs, 363
- flow issues, 360
- management and monitoring tools, 368
- NAM, 365
- password recovery, 369
- troubleshooting logic, 357
- verifying ACL resource limits, 364
- verifying connectivity and packet flow through firewalls, 365
- verifying traffic forwarding to an interface, 363

Trusted Flow Acceleration

- accelerated flows, viewing, 452
- advantages, 449
- cautions, 452
- explanation, 449
- high availability infrastructure considerations, 452

two-step authentication, 175

U

- Unicast IPv6 addressing, 329**
- Unicast Reverse Path Forwarding (uRPF), 100**
- Unique-local scope, IPv6 addresses, 329**
- Update Messages, 158**

- URL filtering, 235**
- url-block url-mempool command, 238**
- url-block url-size command, 238**
- URL-caching, 238**
- uRPF (Unicast Reverse Path Forwarding), 100**

V

- VACLs (VLAN Access Control Lists), 100**
- virtual links network type, 138**
- virtualization, 23**
- virtualized networks, supporting, 384**
- VLAN Access Control Lists (VACLs), 100**
- VLAN assignment and failover, 106**
- vlan-group command, 106–107**
- VLANs (Virtual Local Area Networks)**
 - assignment and failover, 106
 - description, 106, 384
- VPN client configuration, 254**
- VPN termination configuration, 252**
- VRF (Virtual Route Forwarding), 401–402, 404**
- VRF-lite, 402**

W

- Websense Enterprise, 235**
- write standby command, 209**

X

- X Display Manager Control Protocol (XDMCP), 30**
- XDMCP (X Display Manager Control Protocol), 30**
- xlate-bypass command, 57**