SECURITY

Cisco Secure Firewall Services Module (FWSM)

Raymond Blair
Arvind Durai

ciscopress.com

Cisco Secure Firewall Services Module (FWSM)

Ray Blair, Arvind Durai

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

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.**

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.

CHAPTER 25

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.

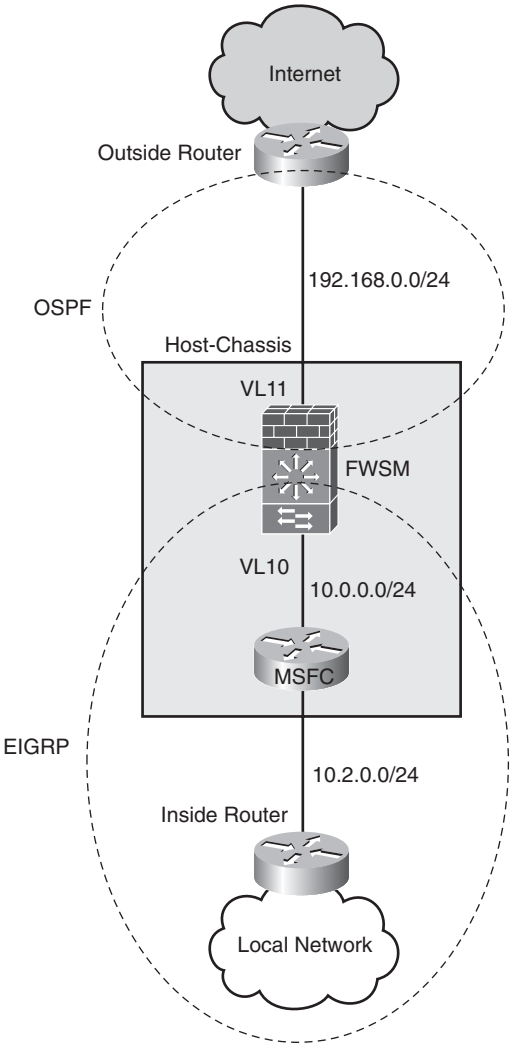
Redistribution of routes between routing protocols can be difficult because each routing protocol exercises different methods to classify routes (cost). For example, RIP uses hop-count, OSPF uses a metric (single value), and EIGRP uses bandwidth and delay by default. When routing information is exchanged, 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                Vl10             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)SXI.

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.

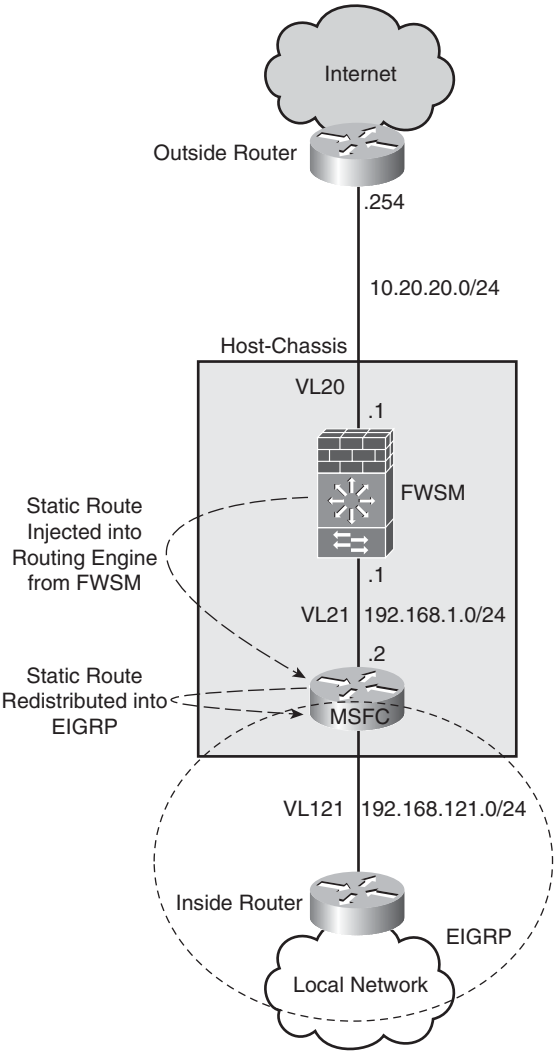
NOTE The automatic route removal feature will not be available on the initial release of 4.01 but will be part of the first maintenance release (4.02).

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:

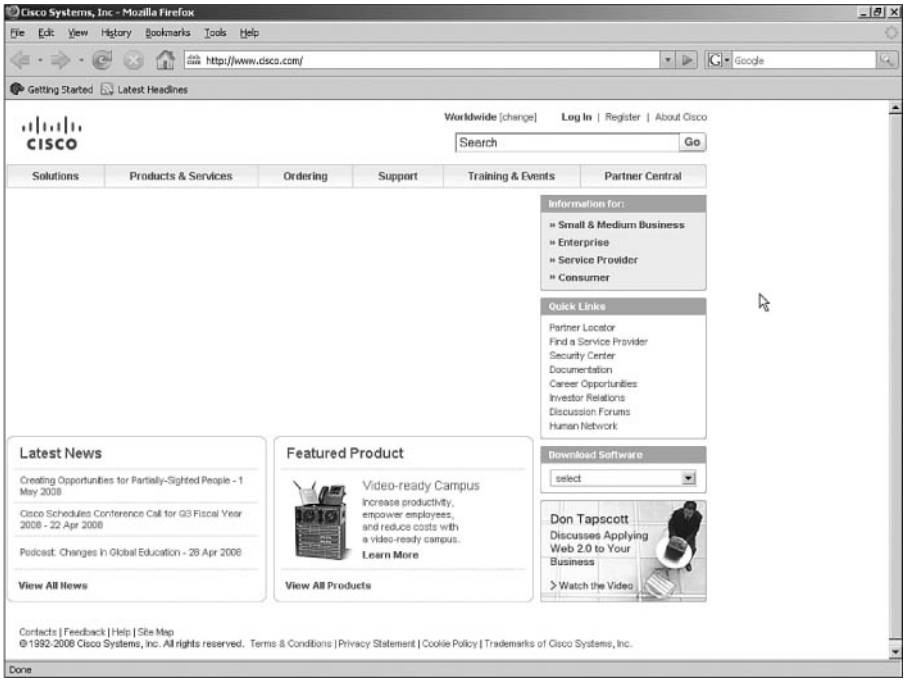
```
%FWSM-5-415006: HTTP - matched Class 23: RESTRICTED_HTTP in policy-map
 HTTP_PMAP, URI matched - Resetting connection from
 Inside:192.168.1.23/3898 to Outside:10.133.219.25/80
```

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*

INDEX

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X