

[Solutions](#) | [Products](#) | [Ordering](#) | [Support](#) | [Partners](#) | [Training](#) | [Corporate](#)

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco PIX and ASA Appliances and Firewall Services Module

<http://www.cisco.com/warp/public/707/cisco-amb-20071017-asafwsm.shtml>

## Revision 1.3

Last Updated 2008 August 19 2100 UTC (GMT)

For Public Release 2007 October 17 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Cisco Response](#)  
[Device Specific Mitigation and Identification](#)  
[Additional Information](#)  
[Revision History](#)  
[Cisco Security Procedures](#)  
[Related Information](#)

---

## Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisories *Multiple Vulnerabilities in Cisco PIX and ASA Appliances* and *Multiple Vulnerabilities in Firewall Services Module* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

### Vulnerability Characteristics

There are multiple vulnerabilities in the Cisco PIX and ASA security appliances as well as the Firewall Services Module (FWSM) for the Catalyst 6500 series switches and Cisco 7600 series routers. These vulnerabilities are summarized in the following subsections:

**Crafted HTTPS Request:** This vulnerability can be exploited remotely without authentication and

without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. The attack vector for exploitation is through HTTPS packets to the FWSM web server port. The web server uses TCP port 443 by default. This vulnerability only affects the Firewall Services Module for the Catalyst 6500 series switches and Cisco 7600 series routers. This vulnerability has been assigned CVE name CVE-2007-5570.

**Crafted MGCP Packet:** This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through MGCP packets using the MGCP port for gateways for which UDP port 2427 is the default port. An attacker could exploit this vulnerability through spoofing attacks. This vulnerability affects the Cisco PIX and ASA appliances as well as the FWSM. This vulnerability has been assigned CVE name CVE-2007-5568.

**Crafted TLS Packet:** This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through HTTPS packets to the Cisco PIX or ASA web server port. The web server uses TCP port 443 by default. This vulnerability only affects Cisco PIX and ASA appliances. This vulnerability has been assigned CVE name CVE-2007-5569.

**Manipulation of ACL May Cause ACL Corruption:** This vulnerability can be exploited remotely with authentication and without user interaction. Successful exploitation of this vulnerability may cause access control list entries (ACEs) in an ACL that has been manipulated to not be evaluated. Exploitation of this vulnerability requires valid administrative credentials; no mitigation techniques will be discussed in this document. This vulnerability only affects the Firewall Services Module for the Catalyst 6500 series switches and Cisco 7600 series routers. This vulnerability has been assigned CVE name CVE-2007-5571.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisories [Multiple Vulnerabilities in Cisco PIX and ASA Appliances](#) and [Multiple Vulnerabilities in Firewall Services Module](#).

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the multiple vulnerabilities in the Cisco PIX and ASA appliances and Firewall Services Module. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS Software can provide effective means of exploit prevention using the following methods:

- Infrastructure access control lists (iACLs)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP source guard (IPSG)

These protection mechanisms filter and drop, as well as verify the source IP address of packets that are attempting to exploit the vulnerabilities that are described in this document.

The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

The proper deployment and configuration of IPSG provides the most effective means of protection against attacks with spoofed source MAC addresses.

Effective means of exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using the following:

- Transit ACLs (tACLs)
- Unicast RPF

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit the vulnerabilities that are described in this document.

The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

Cisco IOS NetFlow can provide visibility into these exploitation attempts using flow records.

Cisco IOS Software, Cisco ASA, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values that are displayed in the output from **show** commands.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit Crafted MGCP packet vulnerability.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through queries and event reporting.

## Risk Management

Organizations should follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping in Information Security Engagements](#) can help organizations develop repeatable security evaluation and response processes.

## Device Specific Mitigation and Identification



**Caution:** The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information about mitigation and identification is available for these devices:

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)

- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

## Cisco IOS Routers and Switches

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators should deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic that is sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured.

### Mitigation: Infrastructure Access Control Lists

In the following example, the address block 192.168.1.0/24 is the infrastructure address space, and the host at 192.168.100.1 is considered a trusted endpoint. The iACL policy denies untrusted HTTPS packets on TCP port 443 and MGCP packets on UDP port 2427 sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic that is sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address space that is used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Additional information about iACLs is available in [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
ip access-list extended Infrastructure-ACL-Policy

!--- When applicable, include explicit permit statements for trusted
!--- sources that require access on the vulnerable ports

permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 443
permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2427

!--- The following vulnerability-specific access control entries
!--- (ACEs) can aid in identification of attacks

deny tcp any 192.168.1.0 0.0.0.255 eq 443
deny udp any 192.168.1.0 0.0.0.255 eq 2427

!--- Explicit deny ACE for traffic sent to addresses configured within
!--- the infrastructure address space

deny ip any 192.168.1.0 0.0.0.255

!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations

!--- Apply iACL to interfaces in the ingress direction

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in
```

## Unicast Reverse Path Forwarding

The Crafted MGCP packet vulnerability that is described in this document can be exploited by spoofed IP packets. The proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF) can provide protection mechanisms for spoofing that is related to this vulnerability.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators should take care to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature, because it can drop legitimate traffic that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

Additional information is available in the [Unicast Reverse Path Forwarding Loose Mode Feature Guide](#).

For additional information about the configuration and use of Unicast RPF, reference the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

## IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets that are based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. The proper deployment and configuration of IPSG coupled with strict mode Unicast RPF can provide the most effective means of spoofing protection to help mitigate the Crafted MGCP Packet vulnerability.

Additional information about the deployment and configuration of IPSG is available in the [Configuring DHCP Features and IP Source Guard](#) section of the Catalyst 3750 Switch Software Configuration Guide.

## Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of HTTPS packets on TCP port 443 or MGCP packets on UDP port 2427 that have been filtered on interfaces to which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for the **show ip access-lists Infrastructure-ACL-Policy** command follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 443
 20 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2427
 30 deny tcp any 192.168.1.0 0.0.0.255 eq 443 (44 matches)
 40 deny udp any 192.168.1.0 0.0.0.255 eq 2427
 50 deny ip any 192.168.1.0 0.0.0.255
router#
```

In the preceding example, the access list *Infrastructure-ACL-Policy* has dropped **44 HTTPS** packets on **TCP port 443** for access control entry (ACE) sequence ID 30.

## Identification: Access List Logging

The **log** and **log-input** access control list (ACL) option will cause packets that match specific ACEs to be logged. The **log-input** option enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.



**Caution:** Access control list logging can be very CPU intensive and must be used with extreme caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log-enabled ACEs.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging.

The **ip access-list logging interval** *interval-in-ms* command can limit the effects of process switching that are induced by ACL logging. The **logging rate-limit** *rate-per-second* [**except** *loglevel*] command limits the impact of log generation and transmission.

For additional information about the configuration and use of ACL logging, reference the [Understanding Access Control List Logging](#) Applied Intelligence white paper.

### Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, administrators can use the **show ip interface**, **show cef drop**, **show cef interface** *type slot/port internal*, and **show ip traffic** commands to identify the number of packets that Unicast RPF has dropped.

**Note:** The **show command** | **begin** *regexp* and **show command** | **include** *regexp* command modifiers are used in the following examples to minimize the amount of output that administrators need to parse to view the desired information. Additional information about command modifiers is available in the "[show command](#)" sections of the Cisco IOS Configuration Fundamentals Command Reference.

**Note:** The **show cef interface** *type slot/port internal* command is a hidden command that must be fully entered at the command-line interface. Command completion is not available for this command.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
```

```
!--- CLI Output Truncated
```

```

      IP verify source reachable-via RX
      2989 verification drops
      0 suppressed verification drops
router#
```

```

router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP      27           0           0           13        0        0
router#
```

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
```

*!--- CLI Output Truncated*

```
ip verify: via=rx, acl=0, drop=2989, sdrop=0
router#
```

```
router#show ip traffic
```

```
IP statistics:
Rcvd: 68051015 total, 2397325 local destination
      43999 format errors, 0 checksum errors, 33 bad hop count
      2 unknown protocol, 929 not a gateway
      21 security failures, 190123 bad options, 542768 with options
Opts: 352227 end, 452 nop, 36 basic security, 1 loose source route
      45 timestamp, 59 extended security, 41 record route
      53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
      361634 other
Frag: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
      0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 64666 received, 0 sent
Mcast: 1589885 received, 2405454 sent
Sent: 3001564 generated, 65359134 forwarded
Drop: 4256 encapsulation failed, 0 unresolved, 0 no adjacency
      13 no route, 2989 unicast RPF, 0 forced drop
      0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address
```

*!--- CLI Output Truncated*

```
router#
```

In the preceding examples, Unicast RPF has dropped **2989 IP packets**. These packets were received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Cisco Express Forwarding Information Base.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerabilities described in this document. Administrators should investigate flows to determine whether they are attempts to exploit these vulnerabilities or whether they are legitimate traffic flows.

```
router#show ip cache flow
IP packet size distribution (748 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
  .473 .526 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .00
      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
```

```

89 active, 4007 inactive, 89 added
526 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
0 active, 1024 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics never
Protocol          Total    Flows   Packets Bytes   Packets Active(Se) Idle(Se)
-----          Flows   /Sec   /Flow  /Pkt   /Sec   /Flow   /Flow

SrcIf            SrcIPAddress    DstIf            DstIPAddress     Pr  SrcP  DstP  Pk
Et0/0            192.168.235.183 Et0/0/1          192.168.81.86    06 2361 7509
Et0/0            192.168.226.38  Et0/0/1          192.168.114.44  11 BBD8 1355
Et0/0            192.168.20.126  Et0/0/1          192.168.1.228   06 3411 01BB
Et0/0            192.168.25.117  Et0/0/1          192.168.94.210  11 6C1A 30B8
Et0/0            192.168.47.0    Et0/0/1          192.168.21.239  11 2A3F CAE1
Et0/0            192.168.85.69   Et0/0/1          192.168.219.125 06 FA81 20A6
Et0/0            192.168.206.192 Et0/0/1          192.168.78.108  06 D564 493E
Et0/0            192.168.112.136 Et0/0/1          192.168.129.218 11 654C 81FD
Et0/0            192.168.181.155 Et0/0/1          192.168.151.2   11 B334 49D6
Et0/0            192.168.100.5   Et0/0/1          192.168.180.196 11 9D7D DB6A
Et0/0            192.168.205.146 Et0/0/1          192.168.1.246   06 2FE1 01BB
Et0/0            192.168.168.12  Et0/0/1          192.168.38.183  06 5E08 0914
Et0/0            192.168.227.98  Et0/0/1          192.168.90.209  11 A833 4A17
Et0/0            192.168.202.183 Et0/0/1          192.168.25.132  11 2FFD A416
Et0/0            192.168.72.121  Et0/0/1          192.168.1.240   06 AB76 01BB
Et0/0            192.168.93.254  Et0/0/1          192.168.80.74   11 CD35 D32D
Et0/0            192.168.240.89  Et0/0/1          192.168.163.100 11 49D6 DA83
Et0/0            192.168.54.13   Et0/0/1          192.168.68.155  06 7590 6101
Et0/0            192.168.241.115 Et0/0/1          192.168.1.169   11 8AD6 097B
Et0/0            192.168.199.172 Et0/0/1          192.168.129.128 06 B573 4106
Et0/0            192.168.122.72  Et0/0/1          192.168.103.29  11 9164 7243

```

In the preceding example, there are multiple flows for **HTTPS** on **TCP** port **443** (hex value **01BB**) and **MGCP** on **UDP** port **2427** (hex value **097B**). This traffic is sent to addresses within the 192.168.1.0/24 address block, which is used for infrastructure devices. The packets in these flows may be spoofed and may indicate an attempt to exploit the vulnerabilities described in this document. Administrators should compare these flows to baseline utilization for HTTPS packets on TCP port 443 and MGCP packets on UDP port 2427. Administrators should also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

The **show ip cache flow | include SrcIf|\_06\_.\*01BB** command will display only the traffic flows for packets on TCP port 443 (hex value 01BB), as shown here:

```

router#show ip cache flow | include SrcIf|_06_.*01BB
SrcIf            SrcIPAddress    DstIf            DstIPAddress     Pr  SrcP  DstP  Pk
Et0/0            192.168.247.13  Et0/0/1          192.168.1.62    06 D407 01BB
Et0/0            192.168.228.251 Et0/0/1          192.168.1.235   06 7264 01BB
Et0/0            192.168.71.39   Et0/0/1          192.168.1.103   06 0EFF 01BB
Et0/0            192.168.243.186 Et0/0/1          192.168.1.183   06 118A 01BB
Et0/0            192.168.26.1    Et0/0/1          192.168.1.205   06 866D 01BB
Et0/0            192.168.17.30  Et0/0/1          192.168.1.63    06 0F6A 01BB
router#

```

The **show ip cache flow | include SrcIf|\_11\_.\*097B** command will display only the traffic flows for packets on UDP port 2427 (hex value 097B), as shown here:

```

router#show ip cache flow | include SrcIf|_11_.*097B
SrcIf            SrcIPAddress    DstIf            DstIPAddress     Pr  SrcP  DstP  Pk

```

```

Et0/0          192.168.84.132  Et0/1          192.168.1.137   11 4FEA 097B
Et0/0          192.168.239.182 Et0/1          192.168.1.237   11 437C 097B
Et0/0          192.168.61.94   Et0/1          192.168.1.17    11 DB32 097B
Et0/0          192.168.70.55   Et0/1          192.168.1.173   11 E0AE 097B
Et0/0          192.168.163.178 Et0/1          192.168.1.186   11 CFC6 097B
router#

```

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators should deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

The tACL policy denies unauthorized HTTPS packets on TCP port 443 and MGCP packets on UDP port 2427 that are sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is available in [Transit Access Control Lists: Filtering at Your Edge](#) Applied Intelligence white paper.

```

!--- Include any explicit permit statements for trusted sources
!--- that require access on the vulnerable ports

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.16
access-list Transit-ACL-Policy extended permit udp host 192.168.100.1 192.16

!--- The following vulnerability-specific access control entries
!--- (ACEs) can aid in identification of attacks

access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0 255.255.255
access-list Transit-ACL-Policy extended deny udp any 192.168.1.0 255.255.255

!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations

!--- Explicit deny for all other IP traffic

access-list Transit-ACL-Policy extended deny ip any any

!--- Apply tACL to interfaces in the ingress direction

access-group Transit-ACL-Policy in interface outside

```

### Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

The Crafted MGCP packet vulnerability described in this document can be exploited by spoofed IP packets. The proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF) can provide protection mechanisms for spoofing that is related to the Crafted MGCP packet vulnerability.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide 100 percent spoofing protection, because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and at the internal access layer on the user-supporting Layer 3 interfaces.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [ip verify reverse-path](#) and the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

### Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of HTTPS packets on TCP port 443 or MGCP packets on UDP port 2427 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
access-list Transit-ACL-Policy line 2 extended permit udp host 192.168.100.1
access-list Transit-ACL-Policy line 3 extended deny tcp any 192.168.1.0 255.
access-list Transit-ACL-Policy line 4 extended deny udp any 192.168.1.0 255.
access-list Transit-ACL-Policy line 5 extended deny ip any any (hitcnt=12)
firewall#
```

In the preceding example, the access list *Transit-ACL-Policy* has dropped **172 HTTPS** packets on **TCP port 443** and **137 MGCP** packets on **UDP port 2427** that have been received from an untrusted host or network. In addition, syslog message *106023* can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the IP protocol for the denied packet.

### Identification: Firewall Access-list Syslog Messages

Firewall syslog message *106023* will be generated for packets denied by an access control entry (ACE) that does not have the **log** keyword present. Additional information about this syslog message is available in [Cisco Security Appliance System Log Message - 106023](#).

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following example, the **show logging | grep regex** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit the vulnerabilities described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is available in [Using the Command Line Interface](#).

```

firewall#show logging | grep 106023
Oct 01 2007 19:07:56: %ASA-4-106023: Deny udp src outside:192.168.37.111/262
  inside:192.168.1.90/2427 by access-group "Transit-ACL-Policy"
Oct 02 2007 18:47:43: %ASA-4-106023: Deny tcp src outside:192.168.167.161/50
  inside:192.168.1.19/443 by access-group "Transit-ACL-Policy"
Oct 03 2007 17:29:54: %ASA-4-106023: Deny udp src outside:192.168.214.14/120
  inside:192.168.1.58/2427 by access-group "Transit-ACL-Policy"
Oct 04 2007 10:47:27: %ASA-4-106023: Deny udp src outside:192.168.196.168/38
  inside:192.168.1.96/2427 by access-group "Transit-ACL-Policy"
Oct 05 2007 08:36:01: %ASA-4-106023: Deny udp src outside:192.168.224.138/58
  inside:192.168.1.123/2427 by access-group "Transit-ACL-Policy"
Oct 06 2007 06:37:26: %ASA-4-106023: Deny tcp src outside:192.168.216.26/257
  inside:192.168.1.219/443 by access-group "Transit-ACL-Policy"
firewall#

```

In the preceding example, the messages that are logged for the tACL *Transit-ACL-Policy* show **HTTPS** packets on **TCP** port **443** and **MGCP** packets on **UDP** port **2427** sent to the address block assigned to the network infrastructure.

Additional information about syslog messages for ASA and PIX security appliances is available in [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available in [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

### Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

Firewall syslog message *106021* will be generated for packets that are denied by Unicast RPF. Additional information about this syslog message is available in [Cisco Security Appliance System Log Message - 106021](#).

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following example, the **show logging | grep regex** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit the vulnerabilities described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is available in [Using the Command Line Interface](#).

```

firewall#show logging | grep 106021
Oct 01 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
  192.168.0.1 to 192.168.0.100 on interface outside
Oct 01 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
  192.168.0.1 to 192.168.0.100 on interface outside
Oct 01 2007 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
  192.168.0.1 to 192.168.0.100 on interface outside
firewall#

```

The **show asp drop** command can also identify the number of packets that Unicast RPF has dropped, as shown in the following example:

```

firewall#show asp drop

Frame drop:
  Reverse-path verify failed 11
  Flow is denied by configured rule 855
  Expired flow 1
  Interface is down 2

Flow drop:

firewall#

```

In the preceding example, Unicast RPF has dropped **11 IP packets** received on interfaces with Unicast RPF configured.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

## Cisco Intrusion Prevention System

### Mitigation: Cisco IPS Signature Event Actions

Administrators can use the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the Craft MGCP packet vulnerability described in this document. This vulnerability may be detected by the following signatures:

- 5913/0 - PIX/ASA/FWSM MGCP DoS
- 5913/1 - PIX/ASA/FWSM MGCP DoS

#### 5913/0 - PIX/ASA/FWSM MGCP DoS

Starting with signature update S307 for sensors running Cisco IPS version 6.x or 5.x, the Crafted MGCP packet vulnerability described in this document can be detected by signature 5913/0 (Signature Name: PIX/ASA/FWSM MGCP DoS). Signature 5913/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **produce-alert**. Signature 5913/0 fires when a single packet sent to UDP destination port 2427 is detected. Firing of this signature may indicate a potential exploit of the Crafted MGCP packet vulnerability described in this document.

#### 5913/1 - PIX/ASA/FWSM MGCP DoS

Starting with signature update S307 for sensors running Cisco IPS version 6.x or 5.x, the Crafted MGCP packet vulnerability described in this document can be detected by signature 5913/1 (Signature Name: PIX/ASA/FWSM MGCP DoS). Signature 5913/1 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **produce-alert**. Signature 5913/1 fires when a single packet sent from UDP source port 2427 is detected. Firing of this signature may indicate a potential exploit of the Crafted MGCP packet vulnerability described in this document.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the Crafted MGCP packet vulnerability described in this document.

Because UDP-based exploits can easily be spoofed, an attack that contains spoofed addresses may

cause a configured event action to inadvertently deny traffic from trusted sources. Event actions that perform blocking through ACLs or the **shun** command are usually configured on sensors deployed in promiscuous mode.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the Crafted MGCP packet vulnerability. Threat prevention is achieved through a default override that performs an event action of **deny-packet-inline** for triggered signatures with a *riskRatingValue* greater than 90. Additional information about the risk rating and the calculation of its value is available in [Cisco IPS Risk Rating Explained](#).

## Identification: IPS Signature Events

### Signature: 5913/0 - PIX/ASA/FWSM MGCP DoS

```
IPS# show events alert | include id=5913

evIdsAlert: eventId=1184086129278933092 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:28:38 2007/10/17 12:28:38 CDT
  signature: description=PIX/ASA/FWSM MGCP DoS id=5913 version=S307
    sigId: 0
    sigDetails: Malformed MGCP Header
    marsCategory: DoS/Network/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
      port: 1100
    target:
      addr: locality=OUT 192.168.130.150
      port: 2427
      os: idSource=unknown relevance=unknown type=unknown
  triggerPacket:
```

*!--- CLI Output Truncated*

```
riskRatingValue: targetValueRating=medium watchlist=25 73
threatRatingValue: 73
interface: ge0_0
protocol: udp
```

### Signature: 5913/1 - PIX/ASA/FWSM MGCP DoS

```
IPS# show events alert | include id=5913

evIdsAlert: eventId=1184086129278936717 severity=medium vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 18:30:47 2007/10/17 13:30:47 CDT
  signature: description=PIX/ASA/FWSM MGCP DoS id=5913 version=S307
```

```
subsigId: 1
sigDetails: PIX/ASA/FWSM MGCP DOS
marsCategory: DoS/Network/Misc
marsCategory: Info/Misc
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 2427
  target:
    addr: locality=OUT 192.168.130.150
    port: 1000
    os: idSource=unknown relevance=unknown type=unknown
triggerPacket:
```

*!--- CLI Output Truncated*

```
riskRatingValue: targetValueRating=medium watchlist=25 73
threatRatingValue: 73
interface: ge0_0
protocol: udp
```

## Cisco Security Monitoring, Analysis, and Response System

### Identification: Cisco Security Monitoring, Analysis, and Response System Query Type and Keyword

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the Crafted MGCP packet vulnerability using a query type and keyword. Using the keywords of **NR-5913/0** and **NR-5913/1** for IPS signatures 5913/0 and 5913/1 respectively, which were created for this vulnerability, and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the events created by IPS signatures 5913/0 and 5913/1.

The following screen shot shows the values used to query for events created by IPS signatures 5913/0 (Signature Name: PIX/ASA/FWSM MGCP DoS) and 5913/1 (Signature Name: PIX/ASA/FWSM MGCP DoS).

The screenshot shows the Cisco MARS Query Reports interface. At the top, there is a navigation bar with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, and ADMINISTRATION. Below this is a sub-navigation bar with tabs for Query, Batch Query, and Report. The current page title is 'QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3'. The user is logged in as Administrator (pnadmin) and the date is Oct 17, 2007 1:41:23.

The main content area is titled 'Load Report as On-Demand Query with Filter'. It includes two dropdown menus: 'Select Group...' and 'Select Report...'. To the right, there are input fields for 'Incident ID:' and 'Session ID:'. Below this is the 'Query Event Data' section, which instructs the user to 'Click the cells below to change query criteria:'. The query type is 'Event Raw Messages ranked by Time, 0h:05m'. The query criteria table is as follows:

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5913/0 OR NR-5913/1	None	ANY	ANY

The 'Keyword' cell contains the text 'NR-5913/0 OR NR-5913/1', which is highlighted with a red box. Below the table are buttons for 'Save As Report', 'Save As Rule', and 'Submit Initial Query'. At the bottom left, there is a copyright notice: 'Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.' At the bottom right, there is a breadcrumb trail: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Administration'.

The following screen shot shows the query results for IPS signatures 5913/0 and 5913/1 created by the Cisco Security MARS appliance using a query type and keyword regex query.

**Query type: Event Raw Messages ranked by Time, 0h:05m** [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5913/0 OR NR-5913/1	None	ANY	ANY

[Save As Report] [Save As Rule] [Sub]

**Query Results**

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tr
E:260635676, S:260635676	Unknown Device Event Type [a]	Oct 17, 2007 1:40:01 PM CDT	R4-IPS4240a	192.168.208.63/0 --> 192.168.130.150/0 UDP Unknown Device Event Type, NR-5913/1, Time:1192646401, Risk Rating:73, VLAN:0, Port List:,0	[Icon]	Fa Pc Tr
E:260635667, S:260635667	Unknown Device Event Type [a]	Oct 17, 2007 1:39:01 PM CDT	R4-IPS4240a	192.168.208.63/0 --> 192.168.130.150/0 UDP Unknown Device Event Type, NR-5913/1, Time:1192646397, Risk Rating:73, VLAN:0, Port List:,0	[Icon]	Fa Pc Tr
E:260635653, S:260635653	Unknown Device Event Type [a]	Oct 17, 2007 1:39:01 PM CDT	R4-IPS4240a	192.168.208.63/0 --> 192.168.130.150/2427 UDP Unknown Device Event Type, NR-5913/1, Time:1192646386, Risk Rating:73, VLAN:0, Port List:,2427	[Icon]	Fa Pc Tr

1 to 4 of 4 | 25 per page

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Adm

## Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

## Revision History

Revision 1.3	2008-August-19	Corrected link in Identification: Spoofing Protection Using Unicast Reverse Path Forwarding section
Revision 1.2	2007-October-19	Added CVE Information.
Revision	2007-	Updated to include IPS and MARS

1.1	October-17	information.
Revision 1.0	2007-October-17	Initial public release

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

## Related Information

- [Applied Mitigation Bulletins](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)

### Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

---

(256 character limit)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)