

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software and Cisco Unified Communications Manager SIP DoS Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20080924-sip.shtml>

## Revision 1.0

For Public Release 2008 September 24 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 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities* and *Multiple Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerabilities* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

Multiple vulnerabilities exist in specific releases of Cisco IOS Software and Cisco Unified Communications Manager. These vulnerabilities are summarized in the following subsections:

**Memory Leak Vulnerability:** This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through a SIP packet using TCP ports 5060 and 5061 or UDP port 5060. An attacker could exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-3799.

**Device Reload Vulnerabilities:** These vulnerabilities can be exploited remotely without authentication and without user interaction. Successful exploitation of these vulnerabilities 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 SIP packets using TCP ports 5060 and 5061 or UDP port 5060. An attacker could exploit these vulnerabilities using spoofed packets. These vulnerabilities have been assigned CVE identifiers CVE-2008-38800, CVE-2008-3801 and CVE-2008-3802.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisories, which are available at the following links: <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml> and <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for these vulnerabilities. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

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

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

These protection mechanisms filter, drop, and verify the source IP address of packets that are attempting to exploit these vulnerabilities.

The proper deployment and configuration of Unicast RPF provides an 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 an effective means of protection against spoofing attacks at the access layer.

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:

- tACLs
- Unicast RPF

These protection mechanisms filter, drop, and verify the source IP address of packets that are attempting to exploit these vulnerabilities.

Cisco IOS NetFlow can provide visibility into network-based exploitation attempts using flow records.

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

## Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of these vulnerabilities. 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](#) 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 IOS Routers and Switches

#### Mitigation: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic 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. An iACL workaround cannot provide complete protection against these vulnerabilities when the attacks originate from a trusted source address.

The iACL policy denies unauthorized SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the 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. Whenever possible, infrastructure address space should be distinct from the address space 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 port
!

permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060

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

deny tcp any 192.168.60.0 0.0.0.255 eq 5060
deny tcp any 192.168.60.0 0.0.0.255 eq 5061
deny udp any 192.168.60.0 0.0.0.255 eq 5060

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

deny ip any 192.168.60.0 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
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no ip unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

### Mitigation: Transit Access Control Lists

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 are advised to deploy transit access control lists (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. A tACL workaround cannot provide complete protection against

the vulnerabilities that have a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the 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](#).

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

access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
access-list 150 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060

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

access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 5060
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 5061
access-list 150 deny udp any 192.168.60.0 0.0.0.255 eq 5060

!
!-- 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 150 deny ip any any

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

interface GigabitEthernet0/0
 ip access-group 150 in
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no ip unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

## Mitigation: Spoofing Protection

## Unicast Reverse Path Forwarding

Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing.

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 complete 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 are advised to 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 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. When properly deployed and configured, IPSG coupled with strict mode Unicast RPF provides the most effective means of spoofing protection for the vulnerabilities described in this document.

Additional information about the deployment and configuration of IPSG is available in [Configuring DHCP Features and IP Source Guard](#).

## 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 SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show ip access-lists Infrastructure-ACL-Policy** follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
40 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (5 matches)
50 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (7 matches)
60 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (18 matches)
70 deny ip any 192.168.60.0 0.0.0.255
router#
```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped the following packets that are received from an untrusted host or network:

- 5 SIP packets on TCP port 5060 for ACE line 40

- **7 SIP** packets on **TCP port 5061** for ACE line 50
- **18 SIP** packets on **UDP port 5060** for ACE line 60

For additional information about investigating incidents using ACE counters and syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper [Embedded Event Manager in a Security Context](#) provides additional details about how to use this feature.

### Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show ip access-lists 150** follows:

```
router#show ip access-lists 150
Extended IP access list 150
10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
40 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (2 matches)
50 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (4 matches)
60 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (19 matches)
70 deny ip any any
router#
```

In the preceding example, access list 150 has dropped the following packets received from an untrusted host or network:

- **2 SIP** packets on **TCP port 5060** for ACE line 40
- **4 SIP** packets on **TCP port 5061** for ACE line 50
- **19 SIP** packets on **UDP port 5060** for ACE line 60

For additional information about investigating incidents using ACE counters and syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper [Embedded Event Manager in a Security Context](#) provides additional details about how to use this feature.

### 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.

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

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.

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 cef interface** *type slot/port internal*, **show ip interface**, **show cef drop**, and **show ip traffic** commands to identify the number of packets that Unicast RPF has dropped.

Note: The **show command** | **begin** *regex* and **show command** | **include** *regex* command modifiers are used in the following examples to minimize the amount of output that administrators will 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.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
--CLI Output Truncated--
ip verify: via-rx (allow default), acl=0, drop=11, sdrop=0
router#
```

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

```
router#show ip interface GigabitEthernet 0/0 | begin verify
--CLI Output Truncated--
IP verify source reachable-via RX, allow default, allow self-ping
11 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           18         0        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
      18 no route, 18 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 **show cef drop** and **show ip traffic** examples, Unicast RPF has dropped **18 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Forwarding Information Base of the Cisco Express Forwarding.

## 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 are advised to 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 (90784136 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

  512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
1885 active, 63651 inactive, 59960004 added
129803821 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
0 active, 16384 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(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0

TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	1
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	00A1	3
<b>Gi0/0</b>	<b>192.168.10.201</b>	<b>Gi0/1</b>	<b>192.168.60.102</b>	<b>06</b>	<b>0984</b>	<b>13C4</b>	<b>1</b>
<b>Gi0/0</b>	<b>192.168.11.54</b>	<b>Gi0/1</b>	<b>192.168.60.158</b>	<b>11</b>	<b>0911</b>	<b>13C4</b>	<b>3</b>
<b>Gi0/0</b>	<b>192.168.11.54</b>	<b>Gi0/1</b>	<b>192.168.60.149</b>	<b>06</b>	<b>2811</b>	<b>13C5</b>	<b>5</b>
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
<b>Gi0/0</b>	<b>192.168.13.97</b>	<b>Gi0/1</b>	<b>192.168.60.28</b>	<b>06</b>	<b>0B3E</b>	<b>13C4</b>	<b>5</b>
<b>Gi0/0</b>	<b>192.168.10.17</b>	<b>Gi0/1</b>	<b>192.168.60.97</b>	<b>11</b>	<b>0B89</b>	<b>13C4</b>	<b>1</b>
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1

router#

In the preceding example, there are multiple SIP flows on TCP port 5060 (hex value 13C4), TCP port 5061 (hex value 13C5) and UDP port 5060 (hex value 13C4).

This traffic is sent to addresses within the 192.168.60.0/24 address block, which is used for infrastructure devices. The packets in these flows may indicate an attempt to exploit these vulnerabilities. Administrators are advised to compare these flows to baseline utilization for SIP traffic sent on TCP ports 5060 and 5061 and UDP port 5060 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for SIP packets on TCP ports 5060 (hex value 13C4) and 5061 (hex value 13C5) and UDP port 5060 (hex value 13C4), the commands **show ip cache flow | include SrcIf|\_11\_.\*13C4** and **show ip cache flow | include SrcIf|\_06\_.\*13C4|13C5** will display the related UDP and TCP NetFlow records as shown here:

### UDP Flows

```
router#show ip cache flow | include SrcIf|_11_.*13C4
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
<b>Gi0/0</b>	<b>192.168.73.201</b>	<b>Gi0/1</b>	<b>192.168.60.100</b>	<b>11</b>	<b>403C</b>	<b>13C4</b>	<b>6</b>
<b>Gi0/0</b>	<b>192.168.72.230</b>	<b>Gi0/1</b>	<b>192.168.60.120</b>	<b>11</b>	<b>AA09</b>	<b>13C4</b>	<b>1</b>

router#

### TCP Flows

```
router#show ip cache flow | include SrcIf|_06_.*13C4|13C5
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
<b>Gi0/0</b>	<b>192.168.12.110</b>	<b>Gi0/1</b>	<b>192.168.60.163</b>	<b>06</b>	<b>092A</b>	<b>13C4</b>	<b>5</b>
<b>Gi0/0</b>	<b>192.168.11.230</b>	<b>Gi0/1</b>	<b>192.168.60.20</b>	<b>06</b>	<b>0C09</b>	<b>13C5</b>	<b>2</b>

router#

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

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 are advised to 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. A tACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the 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](#).

```
!  
!-- Include any explicit permit statements for trusted sources  
!-- that require access on the vulnerable ports  
!  
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255  
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255  
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255  
  
!  
!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks  
!  
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 506  
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 506  
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 506  
  
!  
!-- 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 tACL-Policy extended deny ip any any  
  
!  
!-- Apply tACL to interface(s) in the ingress direction  
!  
access-group tACL-Policy in interface outside
```

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

The vulnerabilities that are described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast RPF as a protection mechanism against spoofing.

Unicast RPF can be configured at the interface level or the global level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide complete 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 SIP packets on TCP ports 5060 and 5061 and UDP port 5060 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the vulnerabilities that are described in this document. Example output for **show access-list tACL-Policy** follows:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.6
access-list tACL-Policy line 4 extended deny tcp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 5 extended deny tcp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 6 extended deny udp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 7 extended deny ip any any (hitcnt=8)
firewall#
```

In the preceding example, the messages logged for the tACL tACL-Policy show potentially spoofed **SIP** packets for **TCP ports 5060** and **5061** and **UDP port 5060** sent to the address block assigned to affected devices.

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 System Log Messages](#).

For additional information about investigating incidents using syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

In the preceding example, access list *tACL-Policy* has dropped the following packets received from an untrusted host or network:

- **10 SIP** packets on **TCP port sip** for ACE line 4
- **5 SIP** packets on **TCP port 5061** for ACE line 5
- **19 SIP** packets on **UDP port sip** for ACE line 6

## 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 [Monitoring the Security Appliance - Configuring and Managing Logs](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Monitoring the Firewall Services Module](#).

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 potential attempts to exploit the vulnerabilities that are 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 [Creating a Regular Expression](#).

```
firewall#show logging | grep 106023
Jul 21 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.2.18/2944
dst inside:192.168.1.191/5060 by access-group "tACL-Policy"
Jul 21 2008 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945
dst inside:192.168.1.33/5060 by access-group "tACL-Policy"
Jul 21 2008 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.144/2946
dst inside:192.168.1.33/5061 by access-group "tACL-Policy"
Jul 21 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.2.99/2947
dst inside:192.168.1.240/5060 by access-group "tACL-Policy"
Jul 21 2008 00:15:13: %ASA-4-106023: Deny udp src outside:192.168.2.100/2948
dst inside:192.168.1.115/5060 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL tACL-Policy show potentially spoofed **SIP** packets for **TCP ports 5060** and **5061** and **UDP port 5060** sent to the address block assigned to affected devices.

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 System Log Messages](#).

For additional information about investigating incidents using syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

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

Firewall syslog message *106021* will be generated for packets 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 [Monitoring the Security Appliance - Configuring and Managing Logs](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Monitoring the Firewall](#)

## [Services Module.](#)

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 potential attempts to exploit the vulnerabilities that are 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 [Creating a Regular Expression](#).

```
firewall#show logging | grep 106021
Jul 21 2008 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.0.1 to 192.168.0.100 on interface outside
Jul 21 2008 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.0.1 to 192.168.0.100 on interface outside
Jul 21 2008 00:15:13: %ASA-1-106021: Deny UDP 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 the Unicast RPF feature has dropped, as shown in the following example:

```
firewall#show asp drop frame rpf-violated
Reverse-path verify failed                21
firewall#
```

In the preceding example, Unicast RPF has dropped **21 IP packets** received on interfaces with Unicast RPF configured. Absence of output indicates that the Unicast RPF feature on the firewall has not dropped packets.

For additional information about debugging accelerated security path dropped packets or connections, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

## 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 1.0	2008-September-24	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

- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [NetFlow Performance Analysis](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider](#)
- [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)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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

[of Cisco Systems, Inc.](#)