

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

Applied Mitigation Bulletins

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Multicast Virtual Private Network Data Leak

<http://www.cisco.com/warp/public/707/cisco-amb-20080326-mvpn.shtml>

Revision 1.1

Last Updated 2008 August 19 1900 UTC (GMT)

For Public Release 2008 March 26 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 Advisory *Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco IOS[®] software contains a vulnerability when processing a specially crafted Multicast Distribution Tree (MDT) Data Join message. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability can allow information disclosure, which enables an attacker to receive traffic from VPNs that are not connected to the same Provider Edge (PE) router. The attack vector for exploitation is through MDT packets with UDP port 3232. An attacker can exploit this vulnerability with spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2008-1156.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. 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 with these 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 attempt to exploit the vulnerability that has a network attack vector.

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 must be deployed as close to all traffic sources as possible.

The proper deployment and configuration of IPSG provides an effective means of protection against spoofed packets at the access layer.

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

- Transit access control lists (tACLs)
- Unicast Reverse Path Forwarding (Unicast RPF)

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that attempt to exploit the vulnerability that has a network attack vector.

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

Cisco IOS Software, Cisco ASA, 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 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](#) 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, or 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

In order 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. Deployed iACLs must be applied in the ingress direction on all interfaces that connect to untrusted networks. Due to the nature of this vulnerability, all MDT packets received on interfaces that are connecting to untrusted networks must be denied.

The iACL policy denies unauthorized MDT packets on UDP port 3232 that are sent to affected devices. In the following example, 192.168.1.0/24 is the IP address space that is used by the affected devices. Care must be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space must be distinct from the address space that is used for user and services segments. The use of this addressing methodology assists 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

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

deny udp any any eq 3232

!
!-- 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
!
```

Note that filtering with an interface access list elicits the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages can 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 with the interface configuration command **no ip unreachable**. ICMP unreachable rate limiting can be changed from the default with the global configuration command **ip icmp rate-limit unreachable *interval-in-ms***.

Mitigation: Anti-Spoofing Protection

Unicast Reverse Path Forwarding

The vulnerability described in this document has a network attack vector and can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding 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 must not rely on Unicast RPF to provide complete spoofing protection because spoofed packets can 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 can 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 vulnerability described in this document that has a network attack vector.

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 identifies the number of MDT packets on UDP port 3232 that have been filtered on interfaces on which the iACL is applied. Administrators must investigate filtered packets to determine whether they are attempts to exploit this vulnerability. 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 udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 3232
 20 deny udp any 192.168.1.0 0.0.0.255 eq 3232 (101 matches)
 30 deny ip any 192.168.1.0 0.0.0.255
router#
```

In the preceding example, the access list *Infrastructure-ACL-Policy* has dropped **101 MDT** packets on **UDP** port **3232** for access control entry (ACE) sequence ID 20.

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

Embedded Event Manager can be utilized 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 on how to utilize this feature.

Identification: Access List Logging

The **log** or **log-input** access control list (ACL) option causes 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 with 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: Anti-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 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=18, sdrop=0
router#

```

Note: The `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 this command.

```

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 Cisco Express Forwarding 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 can be attempts to exploit the vulnerability described in this document that has a network attack vector. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```

router#show ip cache flow
IP packet size distribution (647 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
    .692 .307 .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
  100 active, 3996 inactive, 100 added
  672 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 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(Sec) Idle(Se
-----      Flows      /Sec      /Flow  /Pkt   /Sec      /Flow   /Flow

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pk
Et0/0      192.168.74.232 Et0/0/1    192.168.160.50 06 782B 31AD
Et0/0      192.168.204.236 Et0/0/1    192.168.87.119 11 5D4A 4D1F
Et0/0      192.168.103.19  Et0/0/1    192.168.141.158 06 19A0 2E17
Et0/0      192.168.101.203 Et0/0/1    192.168.216.111 11 1E21 34A2
Et0/0      192.168.128.192 Et0/0/1    192.168.1.140  11 0F85 F955
Et0/0      192.168.87.133  Et0/0/1    192.168.133.241 11 788E 41D9
Et0/0      192.168.80.15   Et0/0/1    192.168.167.27  06 C47B 3886
Et0/0      192.168.74.242  Et0/0/1    192.168.1.86    11 5C06 0CA0
Et0/0      192.168.145.200 Et0/0/1    192.168.156.226 11 5D7A 2E71
Et0/0      192.168.201.67  Et0/0/1    192.168.165.241 06 919D B4C7
Et0/0      192.168.53.212  Et0/0/1    192.168.253.32  11 560A 89CE
Et0/0      192.168.30.134  Et0/0/1    192.168.58.249  11 82AD 2607
Et0/0      192.168.233.55  Et0/0/1    192.168.243.52  11 7F0E 0E9D
Et0/0      192.168.68.131  Et0/0/1    192.168.233.5   11 1FC9 B7CB
Et0/0      192.168.26.161  Et0/0/1    192.168.1.126   11 7D00 0CA0
Et0/0      192.168.18.119  Et0/0/1    192.168.1.205   11 56B6 0CA0
Et0/0      192.168.200.130 Et0/0/1    192.168.248.55  11 FFD8 18F6
Et0/0      192.168.192.147 Et0/0/1    192.168.16.233  11 9101 7624
Et0/0      192.168.149.222 Et0/0/1    192.168.66.239  11 FA21 2C1A
Et0/0      192.168.188.243 Et0/0/1    192.168.70.218  06 FB9D F1B8
Et0/0      192.168.113.253 Et0/0/1    192.168.1.6     11 78CA 0CA0
Et0/0      192.168.154.6   Et0/0/1    192.168.1.223   11 FF7E 0CA0
Et0/0      192.168.176.157 Et0/0/1    192.168.23.149  11 60B9 CF53
Et0/0      192.168.224.160 Et0/0/1    192.168.227.244 11 DBAB F72E
Et0/0      192.168.203.132 Et0/0/1    192.168.211.190 11 2C58 8B88
router#

```

In the preceding example, there are multiple flows on **UDP port 3232 (hex value 0CA0)**. The packets in these flows can be spoofed and can indicate an attempt to exploit the vulnerability described in this document that has a network attack vector. Administrators are advised to compare these flows to baseline utilization for traffic sent on UDP port 3232 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

In order to view only the traffic flows for MDT packets on UDP port 3232 (hex value 0CA0), use the command **show ip cache flow | include SrcIf|_11_.*0CA0**, as shown here:

```

router#show ip cache flow | include SrcIf|_11_.*0CA0
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pk
Et0/0      192.168.121.191 Et0/0/1    192.168.1.158 11 3387 0CA0
Et0/0      192.168.58.149  Et0/0/1    192.168.1.162 11 6EBE 0CA0

```

```

Et0/0      192.168.156.232 Et0/1      192.168.1.167    11 053A 0CA0
Et0/0      192.168.193.201 Et0/1      192.168.1.212   11 7DFD 0CA0
Et0/0      192.168.150.22  Et0/1      192.168.1.202   11 AEA6 0CA0
Et0/0      192.168.255.189 Et0/1      192.168.1.250   11 C713 0CA0
Et0/0      192.168.14.83   Et0/1      192.168.1.254   11 58A0 0CA0
Et0/0      192.168.22.25   Et0/1      192.168.1.106   11 476A 0CA0
Et0/0      192.168.188.60  Et0/1      192.168.1.80    11 1DB9 0CA0
router#

```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In order to protect the network from traffic that enters the network at ingress access points, which can 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 the vulnerability that has a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized MDT packets on UDP port 3232 that are sent to affected devices. In the following example, 192.168.1.0/24 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 must 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
!-- requiring access on the vulnerable ports
!

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 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 interface(s) in the ingress direction
!

access-group Transit-ACL-Policy in interface outside

```

!

Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

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

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators must not rely on Unicast RPF to provide 100 percent spoofing protection because spoofed packets can 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 can 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 [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 MDT packets on UDP port 3232 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 3 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1
access-list Transit-ACL-Policy line 2 extended deny udp any 192.168.1.0 255.
access-list Transit-ACL-Policy line 3 extended deny ip any any (hitcnt=108)
firewall#
```

In the preceding example, access list *Transit-ACL-Policy* has dropped **431 MDT** packets on **UDP port 3232** 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* is 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 can indicate potential attempts to exploit the vulnerability described in this document that has a network attack vector. 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
Dec 18 2007 09:26:05: %ASA-4-106023: Deny udp src outside:192.168.121.189/52
    inside:192.168.1.46/3232 by access-group "Transit-ACL-Policy"
Dec 19 2007 01:42:50: %ASA-4-106023: Deny tcp src outside:192.168.11.110/436
    inside:192.168.1.141/80 by access-group "Transit-ACL-Policy"
Dec 19 2007 16:20:13: %ASA-4-106023: Deny udp src outside:192.168.108.123/63
    inside:192.168.1.195/3232 by access-group "Transit-ACL-Policy"
Dec 20 2007 01:22:14: %ASA-4-106023: Deny udp src outside:192.168.50.161/650
    inside:192.168.1.75/3232 by access-group "Transit-ACL-Policy"
Dec 20 2007 22:28:27: %ASA-4-106023: Deny udp src outside:192.168.253.224/59
    inside:192.168.1.104/3232 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show potentially spoofed packets for **UDP port 3232** 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](#).

For additional information about investigating incidents with 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* is 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 [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 can indicate potential attempts to exploit the vulnerability described in this document that has a network attack vector. 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
Feb 21 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
Feb 21 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
Feb 21 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 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 1.1	2008- August- 19	Corrected link in Identification: Anti-Spoofing Protection Using Unicast Reverse Path Forwarding section
Revision 1.0	2008- March-26	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. 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](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Understanding Access Control List Logging](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [Embedded Event Manager in a Security Context](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Understanding Control Plane Protection](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [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)

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.](#)