

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Cisco Unified Communications Manager and Presence Server Vulnerabilities

Document ID: 97288

<http://www.cisco.com/warp/public/707/cisco-amb-20070711-cucm.shtml>

Revision 1.0

For Public Release 2007 July 11 1600 UTC (GMT)

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

[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 following PSIRT Security Advisories: [Cisco Unified Communications Manager Overflow Vulnerabilities](#) and [Cisco Unified Communications Manager and Presence Server Unauthorized Access Vulnerabilities](#) and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco Unified Communications Manager and Cisco Unified Presence Server. These vulnerabilities are summarized in the following subsections:

Certificate Trust List Provider Service Overflow: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or cause a denial of service (DoS) condition. The attack vector is packets sent to the Certificate Trust List (CTL) Provider service port. The default port is TCP port 2444. Administrators can verify the port used by the CTL Provider service by consulting the Cisco Unified Communications Manager GUI: Choose **System** > **Service Parameters**. From the Server drop-down list, choose the server. Then choose **Cisco CTL Provider (Inactive)** or **Cisco CTL Provider (Active)** from the Service drop-down list. The term (*Inactive*) or (*Active*) appended to the service name in this list indicates whether the service is enabled. After the service is chosen, the Port Number parameter is visible in the area below the Server and Service drop-down lists. The value for this parameter indicates the port used for the service when it is active. At the time of publication, there was no CVE ID associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070711-cucm.shtml>.

Real-Time Information Server Data Collector Heap Overflow: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or cause a denial of service (DoS) condition. The attack vector is packets sent to the Real-Time Information Server (RIS) Data Collector port. The default port is TCP port 2556. Administrators can verify the port used by the RIS Data Collector service by consulting the Cisco Unified Communications Manager GUI: Choose **System > Service Parameters**. From the Server drop-down list, choose the server. Then choose **Cisco RIS Data Collector (Inactive)** or **Cisco RIS Data Collector (Active)** from the Service drop-down list. The term (*Inactive*) or (*Active*) appended to the service name in this list indicates whether the service is enabled. After the service is chosen, the RIS Cluster TCP Port parameter is visible in the Clusterwide Parameters area. The value for this parameter indicates the port used for the service when it is active. At the time of publication, there was no CVE ID associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070711-cucm.shtml>.

Unauthorized Administrator Can Activate/Terminate Cisco Unified Communications Manager/Cisco Unified Presence Server System Services: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation may allow an unauthorized Cisco Unified Communications Manager/Cisco Unified Presence Server administrator to activate or terminate system services in a cluster environment. This may interrupt or stop critical voice services. The attack vector is the SSL protocol using TCP port 8443 packets. See [Cisco CallManager TCP and UDP Port Usage](#) for additional information about the ports used by the affected software. At the time of publication, there was no CVE ID associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070711-voip.shtml>.

Unauthorized Administrator Can View Cisco Unified Communications Manager/Cisco Unified Presence Server SNMP Settings: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation may allow an unauthorized administrator to browse the SNMP settings view on a Cisco Unified Communications Manager/Cisco Unified Presence Server cluster node's management interface. The attack vector is the SSL protocol using TCP port 8443 packets. See [Cisco CallManager TCP and UDP Port Usage](#) for additional information about the ports used by the affected software. At the time of publication, there was no CVE ID associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070711-voip.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the vulnerabilities described in this document. Administrators are advised to consider many of 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 transit access control lists (tACLs).

Effective 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 using transit access control lists (tACLs).

These protection mechanisms filter and drop packets attempting to exploit the vulnerabilities described in this document.

Cisco IOS NetFlow can provide visibility into 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 displayed in the output from **show** commands.

Risk Management

Organizations should follow their standard risk evaluation and mitigation process 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 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 IOS Routers and Switches

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 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.

The tACL policy denies unauthorized packets for the CTL Provider service on TCP port 2444, the RIS Data Collector on TCP port 2556, and the Cisco Unified Communications Manager/Cisco Unified Presence Server System Services on TCP port 8443 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 port(s)  
!
```

```

access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443

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

access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 2444
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 2556
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 8443

!
!-- 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 interface(s) 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. This could have the undesired effect of increasing CPU utilization because the device needs to generate these ICMP unreachable messages. 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 icmp unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

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 CTL Provider service packets on TCP ports 2444, RIS Data Collector packets on TCP port 2556 and CUCM/CUPS System Service packets on TCP port 8443 that have been filtered. Administrators should 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 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444 (2 matches)
 20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556 (3 matches)
 30 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443 (3 matches)
 40 deny tcp any 192.168.1.0 0.0.0.255 eq 2444 (3 matches)
 50 deny tcp any 192.168.1.0 0.0.0.255 eq 2556 (4 matches)
 60 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 (5 matches)
 70 deny ip any any
router#

```

In the preceding example, access list 150 has dropped **3 packets on TCP port 2444** for ACE sequence ID 40, **4 packets on TCP port 2556** for ACE sequence ID 50, and **5 packets on TCP port 8443** for ACE sequence ID 60.

Identification: Access List Logging

The **log** or **log-input** 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. The CPU impact of ACL logging is driven by two factors: process switching as a result of packets that match log-enabled ACEs and log generation and transmission.

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

For additional information about the configuration and use of ACL logging, reference the Applied Intelligence white paper at <http://www.cisco.com/web/about/security/intelligence/acl-logging.html>.

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 potential 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 (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 .000

IP Flow Switching Cache, 4456704 bytes
1885 active, 63651 inactive, 59960004 added
129803821 aged 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	192.168.100.201	Gi0/1	192.168.1.102	06	0984	098C	1
Gi0/0	192.168.100.5	Gi0/1	192.168.1.158	06	0911	09FC	3
Gi0/0	192.168.105.60	Gi0/1	192.89.1.226	06	0016	12CA	1
Gi0/0	192.168.105.97	Gi0/1	192.168.1.28	06	0B3E	098C	5
Gi0/0	192.168.105.197	Gi0/1	192.168.1.248	06	0B3E	20FB	7
Gi0/0	192.168.1.17	Gi0/1	192.168.1.97	11	0B89	00A1	1
Gi0/0	192.168.105.7	Gi0/1	192.168.1.8	06	0B3E	20FB	4
Gi0/1	10.88.226.1	Gi0/0	192.168.202.22	11	007B	007B	1
Gi0/0	192.168.12.185	Gi0/1	192.168.1.239	06	0E8A	09FC	1
Gi0/1	10.89.16.226	Gi0/0	192.168.150.60	06	12CA	0901	1

router#

In the preceding example, there are several flows for the CTL Provider service on **TCP port 2444 (hex value 098C)**, the RIS Data Collector on **TCP port 2556 (hex value 09FC)**, and the Cisco Unified Communications Manager/Cisco Unified Presence Server System Service on **TCP port 8443 (hex value 20FB)**.

Administrators should compare these flows to baseline utilization for traffic sent on TCP ports 2444, 2556, and 8443 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for packets on TCP port 2444 (hex value 098C), packets on TCP port 2556 (hex value 09FC), or packets on TCP port 8443 (hex value 20FB), the command **show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)** will display the related NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.100.110	Gi0/1	192.168.1.163	06	0E2A	098C	6
Gi0/0	192.168.105.230	Gi0/1	192.168.1.20	06	0C09	098C	1
Gi0/0	192.168.101.131	Gi0/1	192.168.1.245	06	0B66	20FB	18
Gi0/0	192.168.100.7	Gi0/1	192.168.1.162	06	0D14	09FC	1
Gi0/0	192.168.100.86	Gi0/1	192.168.1.27	06	0B7B	09FC	2

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 CTL Provider service packets on TCP port 2444, RIS Data Collector packets on TCP port 2556, and Cisco Unified Communications Manager/Cisco Unified Presence Server System Service packets on TCP port 8443 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 port(s)
!

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 2444
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 2556
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 8443

!
!-- 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
255.255.255.0 eq 2444
access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0
255.255.255.0 eq 2556
access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0
255.255.255.0 eq 8443

!
!-- 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

!

```

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 CTL Provider service packets on TCP port 2444, RIS Data Collector packets on TCP port 2556, and Cisco Unified Communications Manager/Cisco Unified Presence Server System Service packets on TCP port 8443 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; 7 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 2444 (hitcnt=2) 0xacal615c
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 2556 (hitcnt=4) 0x991fbe7d
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 8443 (hitcnt=3) 0xd2687825
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255.255.0
eq 2444 (hitcnt=19) 0xc81a715d
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.1.0 255.255.255.0
eq 2556 (hitcnt=11) 0x67db99e7

```

```
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.1.0255.255.255.0
eq 8443 (hitcnt=7) 0xb322498f
access-list Transit-ACL-Policy line 7 extended deny ip any any(hitcnt=0) 0xc797eb99
firewall#
```

In the preceding example, access list Transit-ACL-Policy has dropped **19 packets for TCP port 2444**, **11 packets for TCP port 2556**, and **7 packets for TCP port 8443** 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 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 regexp** 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 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
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
inside:192.168.1.191/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 dst
inside:192.168.1.33/2556 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
inside:192.168.1.240/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 dst
inside:192.168.1.115/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
inside:192.168.1.38/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 dst
inside:192.168.1.250/2444 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL Transit-ACL-Policy show packets for **TCP port 2444**, packets for **TCP port 2556**, and packets for **TCP port 8443** 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](#).

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	2007–July–11	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](#)
- [Access Control List Logging](#)
- [Cisco IOS NetFlow – Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Firewall Products – Home Page on Cisco.com](#)
- [Common Vulnerabilities and Exposures List](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Jul 11, 2007

Document ID: 97288
