

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Document ID: 91388

<http://www.cisco.com/warp/public/707/cisco-amb-20070502-asa.shtml>

Revision 1.0

For Public Release 2007 May 02 1600 UTC (GMT)

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

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Cisco IOS Routers and Switches](#)
[Cisco IOS NetFlow](#)
[Cisco ASA, PIX, and FWSM Firewalls](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory "LDAP and VPN Vulnerabilities in PIX and ASA Appliances." It documents additional mitigation techniques that can be deployed on Cisco devices within the network.

Vulnerability Characteristics

Multiple vulnerabilities exist in Cisco PIX and ASA security appliances. These vulnerabilities are summarized below:

LDAP Authentication Bypass. This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may allow unauthenticated network and device access. There are two attack vectors for this vulnerability. The first attack is through the Layer 2 Tunneling Protocol (L2TP) over IPSec, which uses the Encapsulating Security Payload (ESP) protocol (protocol number 50), the Authentication Header (AH) protocol (protocol number 51), and the Internet Security Association and Key Management Protocol (ISAKMP, UDP port 500). The second attack vector is through Secure Shell (SSH) using TCP port 22, Telnet using TCP port 23, HTTP using TCP port 80, and HTTPS using TCP port 443. This vulnerability has been assigned CVE name CVE-2007-2462.

Denial of Service in VPNs with Password Expiry. This vulnerability can be exploited remotely without authentication and without user interaction. Repeated exploitation of this vulnerability could result in a sustained denial of service (DoS) condition. The attack vector used to exploit this vulnerability is through ISAKMP using UDP port 500, and HTTPS using TCP port 443. This vulnerability has been assigned CVE name CVE-2007-2463.

Denial of Service in SSL VPNs. This vulnerability can be exploited remotely without authentication and without user interaction. Repeated exploitation of this vulnerability could result in a sustained DoS condition. The attack vector used to exploit this vulnerability is through HTTPS using TCP port 443. This vulnerability has been assigned CVE name CVE-2007-2464.

This document contains information to assist Cisco customers in mitigating attempts to exploit the LDAP and VPN Vulnerabilities in PIX and ASA Appliances.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070502-asa.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the LDAP and VPN vulnerabilities described in this document. Many of these protection methods should be considered general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS can provide effective means of exploit prevention using infrastructure access control lists (iACLs). 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 using transit access control lists (tACLs).

These protection mechanisms filter and drop packets that are attempting to exploit a vulnerability described in this document. The following protocols must be filtered to prevent exploitation of all three vulnerabilities:

- ESP – IP protocol 50
- AH – IP protocol 51
- ISAKMP – UDP port 500
- SSH – TCP port 22
- Telnet – TCP port 23
- HTTP – TCP port 80
- HTTPS – TCP port 443

Visibility into these attacks can be provided by Cisco IOS NetFlow, Cisco IOS software, Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, and the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers through syslog messages and the counter values displayed in the output from **show** commands.

Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of this vulnerability. Documents that may be used to aid in risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

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

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to address space used by infrastructure devices. The construction of an iACL is accomplished 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.

In the following example, the address block 192.0.2.0/24 is the infrastructure address space. The iACL policy denies packets sent to the infrastructure address space using IP protocols 50 and 51 (ESP and AH) as well as UDP destination port 500 (ISAKMP) and TCP destination ports 22 (SSH), 23 (Telnet), 80 (HTTP), and 443 (HTTPS). Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address spaced used for user and services segments. Use of this addressing methodology will assist with the construction and deployment of iACLs.

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

```

!
ip access-list extended infrastructure-acl-policy

!-- Permit additional Layer 3 and Layer 4 traffic destined for infrastructure
!-- address space as dictated by existing security policies and configurations.
!
!-- Permit or deny traffic to infrastructure IP addresses in accordance
!-- with security policy.
!
!-- The following vulnerability-specific access control entries (ACEs) can aid
!-- in the identification of attacks.
!

deny 50 any 192.0.2.0 0.0.0.255
deny 51 any 192.0.2.0 0.0.0.255
deny udp any 192.0.2.0 0.0.0.255 eq 500
deny tcp any 192.0.2.0 0.0.0.255 eq 22
deny tcp any 192.0.2.0 0.0.0.255 eq 23
deny tcp any 192.0.2.0 0.0.0.255 eq 80
deny tcp any 192.0.2.0 0.0.0.255 eq 443

!
!-- Default deny to infrastructure IP addresses.
!

deny ip any 192.0.2.0 0.0.0.255

!
!-- Permit or deny all other IP traffic in accordance with

```

```

!-- existing security policies and configurations.
!
!-- Apply iACL to interface(s) in the ingress direction.
!

interface GigabitEthernet0/0
 ip access-group infrastructure-acl-policy in

!

```

Please 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 IOS, ICMP unreachable generation is limited to one packet every 500 milliseconds. 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 of one per 500 milliseconds using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Identification: Infrastructure Access Control Lists

Once the iACL has been applied to an interface in the ingress direction, the **show ip access-lists** command can be used to identify the number of packets that have been filtered. Filtered packets should be investigated 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 deny esp any 192.0.2.0 0.0.0.255
 20 deny ahp any 192.0.2.0 0.0.0.255
 30 deny udp any 192.0.2.0 0.0.0.255 eq 500
 40 deny tcp any 192.0.2.0 0.0.0.255 eq 22 (111 matches)
 50 deny tcp any 192.0.2.0 0.0.0.255 eq telnet
 60 deny tcp any 192.0.2.0 0.0.0.255 eq www
 70 deny tcp any 192.0.2.0 0.0.0.255 eq 443
 80 deny ip any 192.0.2.0 0.0.0.255

--      Infrastructure ACL Policy Truncated      --
router#

```

In the preceding example, access list *infrastructure-acl-policy* has dropped **111 TCP port 22 (SSH)** packets for access control entry (ACE) sequence ID 40.

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

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit a vulnerability described in this document. Flows should be investigated to determine whether they are attempts to exploit this vulnerability or legitimate traffic.

```
router#show ip cache flow
IP packet size distribution (3277 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
    .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
      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
  125 active, 3971 inactive, 249 added
  3155 aged polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

Protocol          Total      Flows      Packets Bytes      Packets Active(Sec) Idle(Sec)
-----          -----
                  Flows      /Sec      /Flow  /Pkt      /Sec      /Flow      /Flow
TCP-Telnet         10         0.0        12     43         0.6        0.0        15.4
TCP-WWW             7         0.0        17     43         0.6        0.0        15.2
TCP-other          107        0.5        13     43         7.2        0.0        15.4
Total:             124        0.6        13     43         8.4        0.0        15.4

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Et0/0      192.0.2.152      Et0/1      192.0.2.126      06 53F7 0016 17
Et0/0      192.168.124.92   Et0/1      192.168.110.145  06 C7EC 76F3 10
Et0/0      192.168.114.165  Et0/1      192.168.47.163   06 DFF9 9E1B 10
Et0/0      192.168.103.248  Et0/1      192.168.21.246   06 6A33 0430 11
Et0/0      192.0.2.3        Et0/1      192.0.2.130      06 A220 0017 1
Et0/0      192.168.214.150  Et0/1      192.168.203.219  06 B2D7 DA54 10
Et0/0      192.168.155.177  Et0/1      192.168.32.46    06 D768 D151 4
Et0/0      192.168.34.125   Et0/1      192.168.77.113   06 4502 D0D0 6
Et0/0      192.0.2.170      Et0/1      192.0.2.72       06 72B2 01BB 7
Et0/0      192.0.2.163      Et0/1      192.0.2.104      06 82DA 0017 45
Et0/0      192.168.123.158  Et0/1      192.168.174.125  06 AD48 5675 5
Et0/0      192.168.229.156  Et0/1      192.168.240.237  06 C653 918D 5
Et0/0      192.0.2.35       Et0/1      192.0.2.151      06 C023 0050 24
Et0/0      192.168.123.230  Et0/1      192.168.122.120  06 2535 9AEE 6
Et0/0      192.0.2.226      Et0/1      192.0.2.146      06 7065 0050 7
Et0/0      192.168.229.216  Et0/1      192.168.83.221   06 1E7D 1FA2 5
Et0/0      192.168.43.121   Et0/1      192.168.33.62    06 E317 0797 6
Et0/0      192.0.2.31       Et0/1      192.0.2.78       06 C1F3 0050 3
Et0/0      192.168.100.226  Et0/1      192.168.150.9    06 A99F 5BE7 4
Et0/0      192.168.85.0     Et0/1      192.168.130.217  06 6DAE FD03 6
Et0/0      192.168.113.217  Et0/1      192.168.206.71   06 1D69 5A3B 5
Et0/0      192.168.53.157   Et0/1      192.168.69.6     06 B9D3 BC24 6
Et0/0      192.0.2.211      Et0/1      192.0.2.164      06 5798 0017 11
Et0/0      192.0.2.177      Et0/1      192.0.2.127      06 F7DF 0050 40
Et0/0      192.0.2.138      Et0/1      192.0.2.68       06 C615 0050 6
Et0/0      192.0.2.247      Et0/1      192.0.2.55       06 87C7 01BB 23
Et0/0      192.0.2.220      Et0/1      192.0.2.73       06 1635 0017 17
Et0/0      192.168.65.249   Et0/1      192.168.211.101  06 1BE9 701D 6
Et0/0      192.0.2.98       Et0/1      192.0.2.13       06 47BF 0017 33
Et0/0      192.0.2.184      Et0/1      192.0.2.45       06 C717 0050 7
```

```

Et0/0      192.168.107.117 Et0/1      192.168.209.220 06 D825 1BA1    5
Et0/0      192.168.194.227 Et0/1      192.168.157.250 06 2747 1262    6
Et0/0      192.0.2.15      Et0/1      192.0.2.156      06 C542 01BB    9
Et0/0      192.0.2.105     Et0/1      192.0.2.215     06 84BF 01BB    8
Et0/0      192.168.234.45  Et0/1      192.168.134.179 06 2776 9354    5
Et0/0      192.0.2.68      Et0/1      192.0.2.159     06 2551 01BB    5
Et0/0      192.0.2.212     Et0/1      192.0.2.81      06 C58C 01BB   25
Et0/0      192.168.140.207 Et0/1      192.168.83.49   06 D526 1E56    5
Et0/0      192.168.22.251  Et0/1      192.168.92.50   06 124A 9204    5
Et0/0      192.0.2.32      Et0/1      192.0.2.11      06 8A75 0017    2
Et0/0      192.168.202.169 Et0/1      192.168.140.10  06 FC51 B9C6    5
Et0/0      192.0.2.127     Et0/1      192.0.2.47      06 CA89 0016   10
Et0/0      192.168.116.239 Et0/1      192.168.111.66  06 FB7F 551F    6
Et0/0      192.0.2.12      Et0/1      192.0.2.9       06 EBE8 0017   17
Et0/0      192.0.2.223     Et0/1      192.0.2.222     06 DA45 0017   12
Et0/0      192.168.236.119 Et0/1      192.168.164.216 06 EFB6 3D87    5
Et0/0      192.0.2.130     Et0/1      192.0.2.81      06 9B06 0017   10
Et0/0      192.168.44.166  Et0/1      192.168.79.139  06 A3B0 C554   11
Et0/0      192.168.57.12   Et0/1      192.168.3.105   06 F559 4B92    5
router#

```

In the preceding example, there are multiple flows for SSH using TCP port 22 (**0016 hex**), Telnet using TCP port 23 (**0017 hex**), HTTP using TCP port 80 (**0050 hex**), and HTTPS using TCP port 443 (**01BB hex**). Using the command **show ip cache flow | include string**, it is possible to filter the flows displayed.

```

router#show ip cache flow | include SrcIf|0016|0017|0050|01BB
SrcIf      SrcIPAddress    DstIf      DstIPAddress    Pr  SrcP  DstP  Pkts
Et0/0      192.0.2.152     Et0/1      192.0.2.126     06 53F7 0016  17
Et0/0      192.0.2.3       Et0/1      192.0.2.130     06 A220 0017   1
Et0/0      192.0.2.170     Et0/1      192.0.2.72      06 72B2 01BB   7
Et0/0      192.0.2.163     Et0/1      192.0.2.104     06 82DA 0017  45
Et0/0      192.0.2.35      Et0/1      192.0.2.151     06 C023 0050  24
Et0/0      192.0.2.226     Et0/1      192.0.2.146     06 7065 0050   7
Et0/0      192.0.2.31      Et0/1      192.0.2.78      06 C1F3 0050   3
Et0/0      192.0.2.211     Et0/1      192.0.2.164     06 5798 0017  11
Et0/0      192.0.2.177     Et0/1      192.0.2.127     06 F7DF 0050  40
Et0/0      192.0.2.138     Et0/1      192.0.2.68      06 C615 0050   6
Et0/0      192.0.2.247     Et0/1      192.0.2.55      06 87C7 01BB  23
Et0/0      192.0.2.220     Et0/1      192.0.2.73      06 1635 0017  17
Et0/0      192.0.2.98      Et0/1      192.0.2.13      06 47BF 0017  33
Et0/0      192.0.2.184     Et0/1      192.0.2.45      06 C717 0050   7
Et0/0      192.0.2.15      Et0/1      192.0.2.156     06 C542 01BB   9
Et0/0      192.0.2.105     Et0/1      192.0.2.215     06 84BF 01BB   8
Et0/0      192.0.2.68      Et0/1      192.0.2.159     06 2551 01BB   5
Et0/0      192.0.2.212     Et0/1      192.0.2.81      06 C58C 01BB  25
Et0/0      192.0.2.32      Et0/1      192.0.2.11      06 8A75 0017   2
Et0/0      192.0.2.127     Et0/1      192.0.2.47      06 CA89 0016  10
Et0/0      192.0.2.12      Et0/1      192.0.2.9       06 EBE8 0017  17
Et0/0      192.0.2.223     Et0/1      192.0.2.222     06 DA45 0017  12
Et0/0      192.0.2.130     Et0/1      192.0.2.81      06 9B06 0017  10
router#

```

This traffic is being sourced from and sent to addresses within the 192.0.2.0/24 address block, which is used for infrastructure devices. These flows should be compared to a traffic baseline and should be investigated to determine whether they are sourced from untrusted hosts or networks.

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 and traffic that transits the network, administrators should deploy transit access control lists (tACLs). The construction of a

tACL is accomplished 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.



Caution: Access control lists placed on an affected PIX and ASA appliance are not effective in mitigating attacks directed at that device.

In the following example, 192.168.1.66 is the IP address of an affected device. The tACL policy denies packets using IP protocols 50 and 51 (ESP and AH) as well as UDP destination port 500 (ISAKMP) and TCP destination ports 22 (SSH), 23 (Telnet), 80 (HTTP), and 443 (HTTPS). 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 tACLs.

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

```
!  
!-- Permit or deny additional Layer 3 and Layer 4 traffic entering  
!-- the network at ingress access points or traffic that transits  
!-- the network in accordance with existing security policies and  
!-- configurations.  
!  
!-- The following vulnerability-specific ACEs can aid in the  
!-- identification of attacks.  
!  
access-list transit-acl-policy extended deny 50 any host 192.168.1.66  
access-list transit-acl-policy extended deny 51 any host 192.168.1.66  
access-list transit-acl-policy extended deny udp any host 192.168.1.66 eq 500  
access-list transit-acl-policy extended deny tcp any host 192.168.1.66 eq 22  
access-list transit-acl-policy extended deny tcp any host 192.168.1.66 eq 23  
access-list transit-acl-policy extended deny tcp any host 192.168.1.66 eq 80  
access-list transit-acl-policy extended deny tcp any host 192.168.1.66 eq 443  
  
!  
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance with  
!-- existing security policies and configurations.  
!  
!-- Apply tACL to interface(s) in the ingress direction.  
  
access-group transit-acl-policy in interface outside  
  
!
```

Identification: Transit Access Control Lists

Once the tACL has been applied to an interface, the **show access-list** command can be used to identify the number of packets that have been filtered. Filtered packets should be investigated 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 line 1 extended deny esp any host 192.168.1.66 (hitcnt=0) 0x  
access-list transit-acl-policy line 2 extended deny ah any host 192.168.1.66 (hitcnt=0) 0x  
access-list transit-acl-policy line 3 extended deny udp any host 192.168.1.66 eq isakmp (h  
access-list transit-acl-policy line 4 extended deny tcp any host 192.168.1.66 eq ssh (hitc  
access-list transit-acl-policy line 5 extended deny tcp any host 192.168.1.66 eq telnet (h  
access-list transit-acl-policy line 6 extended deny tcp any host 192.168.1.66 eq www (hitc  
access-list transit-acl-policy line 7 extended deny tcp any host 192.168.1.66 eq https (hi
```

```
--          Transit ACL Policy Truncated          --
firewall#
```

In the preceding example, access list *transit-acl-policy* has dropped **98 packets for TCP port 22 (SSH)** received from an untrusted host or network. This tACL is applied to interface outside in the ingress direction. 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 protocol for the denied packet.

Identification: Firewall 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 at [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 at [Configuring Logging on the Cisco Security Appliance](#). Information on configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available at [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following examples, the **show logging | grep regex** command is used to extract syslog messages from the logging buffer on the firewall. The results from this command provide additional information about denied packets that could indicate potential attempts to exploit a vulnerability described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data present within the logged messages.

Additional information about regular expression syntax is available at [Filtering show Command Output](#).

```
firewall#show logging | grep 106023
%FWSM-4-106023: Deny tcp src outside:172.16.2.100/33616 dst inside:192.168.1.66/22 by access
%FWSM-4-106023: Deny tcp src outside:172.16.2.100/33616 dst inside:192.168.1.66/22 by access
%FWSM-4-106023: Deny tcp src outside:172.16.2.100/33616 dst inside:192.168.1.66/22 by access
%FWSM-4-106023: Deny tcp src outside:172.16.2.100/33616 dst inside:192.168.1.66/22 by access
%FWSM-4-106023: Deny tcp src outside:172.16.2.100/25046 dst inside:192.168.1.66/22 by access
firewall#
```

In the preceding example, the messages logged for *transit-acl-policy* indicate that packets were destined to TCP port 22 on the affected device. The syslog output in the preceding example is representative of messages that would appear on the Cisco ASA, PIX, and FWSM firewall platforms.

Additional information about syslog messages for ASA and PIX security appliances is available at [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available at [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-May-02	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

- [Risk Triage for Security Vulnerability Announcements](#)
- [Risk Triage and Prototyping](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco Security Appliance System Log Message – 106023](#)
- [Configuring Logging on the Cisco Security Appliance](#)
- [Configuring Monitoring and Logging on the Cisco FWSM](#)
- [Cisco FWSM Regular Expression Syntax](#)
- [Filtering show Command Output](#)

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

Updated: May 02, 2007

Document ID: 91388
