

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the DLSw Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070110-dlsw.shtml>

Revision 1.0

For Public Release 2007 January 10 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

Vulnerability Characteristics

A vulnerability exists in the Data-Link Switching (DLSw) feature within Cisco IOS software where an invalid value in a DLSw capabilities exchange message may result in a crash of the affected device and repeated attempts to exploit this vulnerability could result in a sustained Denial of Service (DoS) condition. Devices running vulnerable IOS software affected by this vulnerability can be exploited remotely by an unauthenticated attacker. The threat vector used to exploit this vulnerability is through the Transmission Control Protocol (TCP) using ports TCP/2065 or TCP/2067 and requires the ability to establish a DLSw connection to the affected device. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the **DLSw Vulnerability**. The vulnerability described in this document affects devices running Cisco IOS software and having DLSw enabled.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the "DLSw Vulnerability". The most effective means of exploit prevention is provided through [Infrastructure Protection Access Control Lists \(iACLs\)](#), [Transit Access Control Lists \(tACLs\)](#), or the Control Plane Policing feature which filter TCP packets sent to addresses configured on the affected device on ports TCP/2065 and TCP/2067 or by disabling the use of DLSw promiscuous peering and configuring explicit DLSw peers using the configuration command **dlsw remote-peer** for all DLSw connections.

Device-Specific Mitigation and Identification

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

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

Cisco IOS Routers



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

Mitigation

Infrastructure Protection Access Control Lists (iACL)

The following access control list (ACL) policy denies TCP packets sent to the IP addresses configured on an affected device for TCP/2065 and TCP/2067. All other packets sent to the affected device are permitted only from known trusted source networks (ie: management networks, security operations center, network operations center). Added access list entries (ACEs) should be implemented as part of an Infrastructure Protection Access Control List (iACL) policy that is used to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic to the infrastructure equipment while permitting all other transit traffic in accordance with existing security policies and configurations.

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

```
!-- Permit TCP packets on ports TCP/2065 and TCP/2067 sent to addresses  
!-- configured on interfaces of the affected device (management, loopback,  
!-- access links and network/user segments) from known trusted DLSw peers.
```

```
ip access-list extended infrastructure-acl-policy
```

```

permit tcp host 192.168.2.2 host 192.168.1.1 eq 2065
permit tcp host 192.168.2.2 host 192.168.1.1 eq 2067
permit tcp host 192.168.3.3 host 192.168.1.1 eq 2065
permit tcp host 192.168.3.3 host 192.168.1.1 eq 2067
permit tcp host 192.168.4.4 host 192.168.1.1 eq 2065
permit tcp host 192.168.4.4 host 192.168.1.1 eq 2067
permit tcp host 192.168.5.5 host 192.168.1.1 eq 2065
permit tcp host 192.168.5.5 host 192.168.1.1 eq 2067

```

```

!-- Deny all other TCP traffic sent to addresses configured on interfaces
!-- of the affected device for ports TCP/2065 and TCP/2067.

```

```

deny tcp any any eq 2065
deny tcp any any eq 2067

```

```

!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance
!-- with existing security policies and configurations.

```

```
!
```

```
!-- Apply iACL to interface(s) in the inbound direction.
```

```

interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group infrastructure-acl-policy in
!

```

Identification

Infrastructure Protection Access Control Lists (iACL)

With an iACL, once the access list is applied, the **show access-lists** or **show ip access-lists** commands can be used to identify the number of TCP packets being filtered. Filtered packets should be investigated to determine if they are attempts to exploit this vulnerability or to verify if they are legitimate packets.

Example output for **show access-lists infrastructure-acl-policy**:

```

ios-router#
ios-router#show access-lists infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 permit tcp host 192.168.2.2 host 192.168.1.1 eq 2065 (13 matches)
 20 permit tcp host 192.168.2.2 host 192.168.1.1 eq 2067
 30 permit tcp host 192.168.3.3 host 192.168.1.1 eq 2065 (7 matches)
 40 permit tcp host 192.168.3.3 host 192.168.1.1 eq 2067
 50 permit tcp host 192.168.4.4 host 192.168.1.1 eq 2065
 60 permit tcp host 192.168.4.4 host 192.168.1.1 eq 2067 (5 matches)
 70 permit tcp host 192.168.5.5 host 192.168.1.1 eq 2065 (29 matches)
 80 permit tcp host 192.168.5.5 host 192.168.1.1 eq 2067
 90 deny tcp any any eq 2065 (130 matches)
100 deny tcp any any eq 2067 (2 matches)
--          ACL Policy Truncated          --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.            --
ios-router#

```

In the above example, access list **infrastructure-acl-policy** permitted 13 - packets on ACE sequence-id 10 for TCP/2065, 7 - packets on ACE sequence-id 30 for TCP/2065, 5 - packets on ACE sequence-id 60 for TCP/2067, 29 - packets on ACE sequence-id 70 for TCP/2065, and denied a total of 132 - packets on TCP/2065 and TCP/2067. Access control list **infrastructure-acl-policy** is applied in the inbound direction on interface GigabitEthernet0/0.

Cisco IOS Switches



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.

Mitigation

Infrastructure Protection Access Control Lists (iACL)

The following access control list (ACL) policy denies TCP packets sent to the addresses configured on an affected device for TCP/2065 and TCP/2067. All other packets sent to the affected device are permitted only from known trusted source networks (ie: management networks, security operations center, network operations center). Added access list entries (ACEs) should be implemented as part of an Infrastructure Protection Access Control List (iACL) policy that is used to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic to the infrastructure equipment while permitting all other transit traffic in accordance with existing security policies and configurations.

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

```
!-- Permit TCP packets on ports TCP/2065 and TCP/2067 sent to addresses  
!-- configured on interfaces of the affected device (management, loopback,  
!-- access links and network/user segments) from known trusted DLSw peers.  
  
ip access-list extended infrastructure-acl-policy  
  permit tcp host 192.168.2.2 host 192.168.1.1 eq 2065  
  permit tcp host 192.168.2.2 host 192.168.1.1 eq 2067  
  permit tcp host 192.168.3.3 host 192.168.1.1 eq 2065  
  permit tcp host 192.168.3.3 host 192.168.1.1 eq 2067  
  permit tcp host 192.168.4.4 host 192.168.1.1 eq 2065  
  permit tcp host 192.168.4.4 host 192.168.1.1 eq 2067  
  permit tcp host 192.168.5.5 host 192.168.1.1 eq 2065  
  permit tcp host 192.168.5.5 host 192.168.1.1 eq 2067  
  
!-- Deny all other TCP traffic sent to addresses configured on interfaces  
!-- of the affected device for ports TCP/2065 and TCP/2067.  
  
  deny tcp any any eq 2065  
  deny tcp any any eq 2067  
  
!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance  
!-- with existing security policies and configurations.
```

```

!

!-- Apply iACL to interface(s) in the inbound direction.

interface Vlan100
 ip address 192.168.1.1 255.255.255.0
 ip access-group infrastructure-acl-policy in
!

```

Identification

Infrastructure Protection Access Control Lists (iACL)

With an iACL, once the access list is applied, the **show access-lists** or **show ip access-lists** commands can be used to identify the number of TCP packets being filtered. Filtered packets should be investigated to determine if they are attempts to exploit this vulnerability or to verify if they are legitimate packets.

Example output for **show access-lists infrastructure-acl-policy**:

```

ios-switch#
ios-switch#show access-lists infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 permit tcp host 192.168.2.2 host 192.168.1.1 eq 2065 (6 matches)
 20 permit tcp host 192.168.2.2 host 192.168.1.1 eq 2067
 30 permit tcp host 192.168.3.3 host 192.168.1.1 eq 2065 (11 matches)
 40 permit tcp host 192.168.3.3 host 192.168.1.1 eq 2067
 50 permit tcp host 192.168.4.4 host 192.168.1.1 eq 2065 (14 matches)
 60 permit tcp host 192.168.4.4 host 192.168.1.1 eq 2067 (7 matches)
 70 permit tcp host 192.168.5.5 host 192.168.1.1 eq 2065
 80 permit tcp host 192.168.5.5 host 192.168.1.1 eq 2067 (1 match)
 90 deny tcp any any eq 2065 (63 matches)
100 deny tcp any any eq 2067 (1 match)
--          ACL Policy Truncated          --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.          --
ios-switch#

```

In the above example, access list **infrastructure-acl-policy** permitted 6 - packets on ACE sequence-id 10 for TCP/2065, 11 - packets on ACE sequence-id 30 for TCP/2065, 14 - packets on ACE sequence-id 50 for TCP/2065, 7 - packets on ACE sequence-id 60 for TCP/2067, 1 - packet on ACE sequence-id 80 for TCP/2067, and denied a total of 64 - packets on TCP/2065 and TCP/2067, which is applied in the inbound direction on interface Vlan100.

Note: The above hit counts displayed are for those packets processed (dropped) in software. For hardware-based IOS switches, an additional command can be used to determine if packets are being dropped in hardware.

Starting with IOS version 12.2(14)SX (for Supervisor 720) and version 12.2(17d)SXB (for Supervisor 2), the command **show tcam interface vlan <vlan-id> acl <in/out> ip** can be used to provide ACE hit counts for packets that have been processed in hardware.

```

ios-switch#show tcam interface vlan 100 acl in ip

* Global Defaults shared

Entries from Bank 0

```

Entries from Bank 1

```
permit      tcp host 192.168.2.2 host 192.168.1.1 eq 2065
permit      tcp host 192.168.2.2 host 192.168.1.1 eq 2067
permit      tcp host 192.168.3.3 host 192.168.1.1 eq 2065 (8 matches)
permit      tcp host 192.168.3.3 host 192.168.1.1 eq 2067
permit      tcp host 192.168.4.4 host 192.168.1.1 eq 2065
permit      tcp host 192.168.4.4 host 192.168.1.1 eq 2067
permit      tcp host 192.168.5.5 host 192.168.1.1 eq 2065 (35 matches)
permit      tcp host 192.168.5.5 host 192.168.1.1 eq 2067
deny        tcp any any eq 2065 (4 matches)
deny        tcp any any eq 2067 (1 match)
```

ios-switch#

In the above example, access list **infrastructure-acl-policy** permitted 43 (total) packets to host 192.168.1.1 in hardware and dropped 5 (total) - packets on TCP/2065 and TCP/2067 in hardware for packets being sent through interface Vlan 100. The **show tcam interface vlan <vlan-id> acl <in/out> ip detail** command can optionally be used to display detailed information.

Cisco IOS Security Features



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.

Mitigation

Control Plane Policing (CoPP)

Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the Control Plane Policing (CoPP) feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to the infrastructure device in accordance with existing security policies and configurations. The following example can be adapted to your network. This example assumes that DLSw (TCP/2065 and TCP/2067) packets sent to the device is to be restricted only to known trusted DLSw peers:

```
!-- Deny all TCP packets on ports TCP/2065 and TCP/2067 sent to addresses
!-- configured on interfaces of the affected device (management, loopback,
!-- access links and network/user segments) from known trusted DLSw peers
!-- so traffic is not policed by the CoPP feature.
```

```
ip access-list extended infrastructure-acl-policy
deny tcp host 192.168.2.2 host 192.168.1.1 eq 2065
deny tcp host 192.168.2.2 host 192.168.1.1 eq 2067
deny tcp host 192.168.3.3 host 192.168.1.1 eq 2065
deny tcp host 192.168.3.3 host 192.168.1.1 eq 2067
deny tcp host 192.168.4.4 host 192.168.1.1 eq 2065
deny tcp host 192.168.4.4 host 192.168.1.1 eq 2067
deny tcp host 192.168.5.5 host 192.168.1.1 eq 2065
deny tcp host 192.168.5.5 host 192.168.1.1 eq 2067
```

```
!-- Permit all other TCP traffic sent to addresses configured on interfaces
```

```

!-- of the affected device for ports TCP/2065 and TCP/2067 so that it will
!-- be policed by the CoPP feature.

permit tcp any any eq 2065
permit tcp any any eq 2067

!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance
!-- with existing security policies and configurations for traffic
!-- that is authorized to be sent to infrastructure devices.

!

!-- Create a Class-Map that will be configured under a Policy-Map for traffi.
!-- policed by the CoPP feature.

class-map match-all control-plane-class
  match access-group name infrastructure-acl-policy

!-- Create a Policy-Map that will be applied to the Control-Plane of the dev
!-- traffic to be policed by the CoPP feature.

policy-map drop-unauthorized-infra-traffic
  class control-plane-class
    drop

!-- Apply the Policy-Map to the Control-Plane of the device for traffic sent
!-- the management and control planes to be policed.

control-plane
  service-policy input drop-unauthorized-infra-traffic
!

```

Please note that in the 12.0S, 12.2S, and 12.2SX Cisco IOS software releases, the **policy-map** syntax is different:

```

policy-map drop-unauthorized-infra-traffic
  class control-plane-class
    police cir 32000 bc 1500 be 1500 conform-action drop exceed-action drop
    violate-action drop

```

Note: In the above CoPP examples, the access control list entries (ACEs) which match the potential exploit packets with the "**permit**" action result in these packets being discarded by the policy-map "**drop**" function, while packets that match the "**deny**" action are not affected by the policy-map drop function. The 12.0S, 12.2S, and 12.2SX Cisco IOS software releases use the "**police**" keyword to drop packets that exceed a configured threshold.

Identification

Cisco IOS Router

With Control Plane Policing (CoPP), once the policy-map is applied to the **control-plane**, the **show policy-map control-plane** and **show access-lists** commands can be used to identify the number of packets that have been sent to the management and control planes and dropped by the CoPP policy.

Packets dropped by CoPP should be investigated to determine if they are attempts to exploit this vulnerability or to verify if they are legitimate packets.

Example output for **show policy-map control-plane** and **show access-list infrastructure-acl-policy**:

```
ios-router#show policy-map control-plane
Control Plane

Service-policy input: drop-unauthorized-infra-traffic

Class-map: control-plane-class (match-all)
  165 packets, 9984 bytes
  5 minute offered rate 2000 bps, drop rate 2000 bps
  Match: access-group name infrastructure-acl-policy
  drop

Class-map: class-default (match-any)
  1063 packets, 69960 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
ios-router#
ios-router#show access-list infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 deny tcp host 192.168.2.2 host 192.168.1.1 eq 2065
 20 deny tcp host 192.168.2.2 host 192.168.1.1 eq 2067
 30 deny tcp host 192.168.3.3 host 192.168.1.1 eq 2065
 40 deny tcp host 192.168.3.3 host 192.168.1.1 eq 2067
 50 deny tcp host 192.168.4.4 host 192.168.1.1 eq 2065
 60 deny tcp host 192.168.4.4 host 192.168.1.1 eq 2067
 70 deny tcp host 192.168.5.5 host 192.168.1.1 eq 2065
 80 deny tcp host 192.168.5.5 host 192.168.1.1 eq 2067
 90 permit tcp any any eq 2065 (111 matches)
100 permit tcp any any eq 2067 (54 matches)
--          ACL Policy Truncated          --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.          --
ios-router#
```

In the above example, the CoPP policy dropped 165 (total) packets by access control list (ACL) "infrastructure-acl-policy" which is associated with CoPP.

Cisco IOS Switch

With Control Plane Policing (CoPP), once the policy-map is applied to the **control-plane**, the **show policy-map control-plane** and **show access-lists** commands can be used to identify the number of packets that have been sent to the management and control planes and dropped by the CoPP policy. Packets dropped by CoPP should be investigated to determine if they are attempts to exploit this vulnerability or to verify if they are legitimate packets.

Example output for **show policy-map control-plane** and **show access-list infrastructure-acl-policy**:

```
ios-switch#show policy-map control-plan
Control Plane Interface

Service-policy input: drop-unauthorized-infra-traffic

Hardware Counters:
```

```

class-map: control-plane-class (match-all)
  Match: access-group name infrastructure-acl-policy
  police :
    32000 bps 1000 limit 1000 extended limit

Software Counters:

Class-map: control-plane-class (match-all)
  157 packets, 10604 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name infrastructure-acl-policy
  police:
    cir 32000 bps, bc 1500 bytes, be 1500 bytes
    conformed 56 packets, 4182 bytes; action: drop
    exceeded 0 packets, 0 bytes; action: drop
    violated 0 packets, 0 bytes; action: drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
  117 packets, 11088 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
ios-switch#
ios-switch#show access-list infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 deny tcp host 192.168.2.2 host 192.168.1.1 eq 2065
 20 deny tcp host 192.168.2.2 host 192.168.1.1 eq 2067
 30 deny tcp host 192.168.3.3 host 192.168.1.1 eq 2065
 40 deny tcp host 192.168.3.3 host 192.168.1.1 eq 2067
 50 deny tcp host 192.168.4.4 host 192.168.1.1 eq 2065
 60 deny tcp host 192.168.4.4 host 192.168.1.1 eq 2067
 70 deny tcp host 192.168.5.5 host 192.168.1.1 eq 2065
 80 deny tcp host 192.168.5.5 host 192.168.1.1 eq 2067
 90 permit tcp any any eq 2065 (43 matches)
100 permit tcp any any eq 2067 (13 matches)
--          ACL Policy Truncated          --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.          --
ios-switch#

```

In the above example, the CoPP policy dropped 56 (total) packets by access control list (ACL) "**infrastructure-acl-policy**" which is associated with CoPP.

NetFlow

NetFlow can be configured on Cisco IOS routers and switches to determine if attempts are in progress to exploit this vulnerability. Packets should be investigated to determine if they are attempts to exploit this vulnerability or to verify if they are legitimate packets.

Identification

```

ios-router#show ip cache flow
IP packet size distribution (587929 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
 .000 .530 .089 .001 .030 .040 .005 .027 .000 .000 .026 .000 .000 .000 .00
      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .028 .000 .217 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes

```

```

3 active, 65533 inactive, 48473 added
585328 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(Se
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	127	0.0	1406	40	0.7	20.6	13.5
TCP-FTP	18	0.0	7	60	0.0	4.8	8.5
TCP-WWW	400	0.0	7	606	0.0	0.8	3.9
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-other	16357	0.0	21	547	1.5	0.9	2.0
UDP-DNS	32	0.0	4	71	0.0	2.9	15.4
UDP-NTP	15796	0.0	1	76	0.0	0.0	15.4
UDP-other	15249	0.0	2	163	0.1	0.6	15.4
ICMP	490	0.0	2	59	0.0	13.5	15.4
Total:	48470	0.2	12	359	2.4	0.7	10.8

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pk
Gi0/8    192.168.8.8      Local     192.168.1.1     06 900D 0811
Gi0/1     192.168.208.63   Gi0/0     192.168.208.20   06 2A76 0050   1
Gi0/9    192.168.9.9      Local     192.168.1.1     06 900D 0813
Gi0/1     192.168.1.21    Gi0/0     192.168.255.21  06 1A9C 0015
Gi0/7    192.168.7.7      Local     192.168.1.1     06 900D 0811
Gi0/1     10.10.11.22    Gi0/0     192.168.1.11    06 0016 1280
Gi0/6    192.168.6.6      Local     192.168.1.1     06 900D 0813
Gi0/0     192.168.255.10 Gi0/1     192.168.1.79    11 0035 A8FC
Gi0/6    192.168.6.6      Local     192.168.1.1     06 900D 0811   1
Gi0/0     10.10.10.22    Gi0/1     192.168.1.10    06 0016 9A32
Gi0/0     192.168.255.10 Gi0/1     192.168.1.44    11 0035 A8EB
ios-router#

```

In the above example, there are several flows on TCP/2065 (Hex value 0811) and TCP/2067 (Hex value 0813) from non-trusted IP addresses destined to the affected DLSw enabled device (192.168.1.1). This may indicate an attempt to exploit this vulnerability and should be compared to baseline utilization for traffic sent to the DLSw enabled device on ports TCP/2065 and TCP/2067.


To only view DLSw flows (TCP/2065 - Hex 0811 or TCP/2067 - Hex 0813), the command **show ip cache flow | include SrcIf|0811|0813** may be used as shown here:

```

ios-router#show ip cache flow | include SrcIf|0811|0813
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pk
Gi0/8     192.168.8.8      Local      192.168.1.1      06 900D 0811
Gi0/9     192.168.9.9      Local      192.168.1.1      06 900D 0813
Gi0/7     192.168.7.7      Local      192.168.1.1      06 900D 0811
Gi0/6     192.168.6.6      Local      192.168.1.1      06 900D 0813
Gi0/6     192.168.6.6      Local      192.168.1.1      06 900D 0811   1
ios-router#

```

Cisco ASA, PIX, and FWSM Firewalls

 **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.

Mitigation

ASA and PIX 7.x - Transit Access Control Lists (tACL)

The following access control list (ACL) policy only permits packets sent to the affected device from known trusted DLSw peers and source networks (ie: management networks, security operations center, network operations center). Added access list entries (ACEs) should be implemented as part of a Transit Access Control List (tACL) policy which is used for filtering transit and edge traffic at network ingress points in accordance with existing security policies and configurations.

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

```
!-- Permit traffic to affected device on TCP/2065 and TCP/2067 for DLSw peer
!-- from known trusted host(s)
.

access-list transit-policy remark -- Permit TCP/2065 and TCP/2067 from trust
  hosts for DLSw peering --
access-list transit-policy permit tcp host 192.168.2.2 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.2.2 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.3.3 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.3.3 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.4.4 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.4.4 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.5.5 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.5.5 host 192.168.1.1 eq 2
access-list transit-policy deny tcp any any eq 2065
access-list transit-policy deny tcp any any eq 2067

!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance
!-- with existing security policies and configurations.

!

!-- Apply tACL to outside interface in the inbound direction.

access-group transit-policy in interface outside
!
```

FWSM - Transit Access Control Lists (tACL)

The following access control list (ACL) policy only permits packets sent to the affected device from known trusted DLSw peers and source networks (ie: management networks, security operations center, network operations center). Added access list entries (ACEs) should be implemented as part of a Transit Access Control List (tACL) policy which is used for filtering transit and edge traffic at network ingress points in accordance with existing security policies and configurations.

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

```
!-- Permit traffic to affected device on TCP/2065 and TCP/2067 for DLSw peer
!-- from known trusted host(s).
```

```

access-list transit-policy remark -- Permit TCP/2065 and TCP/2067 from trust
  hosts for DLSw peering --
access-list transit-policy permit tcp host 192.168.2.2 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.2.2 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.3.3 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.3.3 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.4.4 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.4.4 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.5.5 host 192.168.1.1 eq 2
access-list transit-policy permit tcp host 192.168.5.5 host 192.168.1.1 eq 2
access-list transit-policy deny tcp any any eq 2065
access-list transit-policy deny tcp any any eq 2067

!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance
!-- with existing security policies and configurations.

!

!-- Apply tACL to outside interface in the inbound direction.

access-group transit-policy in interface outside
!
```

Identification

ASA and PIX 7.x - Transit Access Control Lists (tACL)

```

cisco-asa#show access-list transit-policy
access-list transit-policy line 7 remark -- Permit TCP/2065 and
  TCP/2067 from trusted hosts for DLSw peering --
access-list transit-policy line 8 extended permit tcp host
  192.168.2.2 host 192.168.1.1 eq 2065 (hitcnt=8)
access-list transit-policy line 9 extended permit tcp host
  192.168.2.2 host 192.168.1.1 eq 2067 (hitcnt=0)
access-list transit-policy line 10 extended permit tcp host
  192.168.3.3 host 192.168.1.1 eq 2065 (hitcnt=71)
access-list transit-policy line 11 extended permit tcp host
  192.168.3.3 host 192.168.1.1 eq 2067 (hitcnt=0)
access-list transit-policy line 12 extended permit tcp host
  192.168.4.4 host 192.168.1.1 eq 2065 (hitcnt=0)
access-list transit-policy line 13 extended permit tcp host
  192.168.4.4 host 192.168.1.1 eq 2067 (hitcnt=0)
access-list transit-policy line 14 extended permit tcp host
  192.168.5.5 host 192.168.1.1 eq 2065 (hitcnt=39)
access-list transit-policy line 15 extended permit tcp host
  192.168.5.5 host 192.168.1.1 eq 2067 (hitcnt=0)
access-list transit-policy line 16 extended deny tcp any any eq 2065 (hitcnt
access-list transit-policy line 17 extended deny tcp any any eq 2067 (hitcnt
--      ACL Policy Truncated      --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.      --
cisco-asa#
```

In the above example, 97 (total) - TCP packets sent to ports TCP/2065 and TCP/2067 have been received from a non-trusted host or network and denied. In addition, the following syslog message will be logged for any attempts that are denied by access list **transit-policy**:

```

Jan 08 2007 10:39:38: %ASA-4-106023: Deny tcp src outside:192.168.66.6/39174
  dst inside:192.168.1.1/2065 by access-group "transit-policy"
```

Additional information about SYSLOG messages is available at [Cisco Security Appliance System Log Messages - 106023](#).

FWSM - Transit Access Control Lists (tACL)

```
cisco-fwsm#show access-list transit-policy
access-list transit-policy line 7 remark -- Permit TCP/2065 and TCP/2067
    from trusted hosts for DLSw peering --
access-list transit-policy line 8 extended permit tcp host 192.168.2.2 host
    192.168.1.1 eq 2065 (hitcnt=0)
access-list transit-policy line 9 extended permit tcp host 192.168.2.2 host
    192.168.1.1 eq 2067 (hitcnt=1)
access-list transit-policy line 10 extended permit tcp host 192.168.3.3 host
    192.168.1.1 eq 2065 (hitcnt=39)
access-list transit-policy line 11 extended permit tcp host 192.168.3.3 host
    192.168.1.1 eq 2067 (hitcnt=8)
access-list transit-policy line 12 extended permit tcp host 192.168.4.4 host
    192.168.1.1 eq 2065 (hitcnt=53)
access-list transit-policy line 13 extended permit tcp host 192.168.4.4 host
    192.168.1.1 eq 2067 (hitcnt=19)
access-list transit-policy line 14 extended permit tcp host 192.168.5.5 host
    192.168.1.1 eq 2065 (hitcnt=72)
access-list transit-policy line 15 extended permit tcp host 192.168.5.5 host
    192.168.1.1 eq 2067 (hitcnt=0)
access-list transit-policy line 16 extended deny tcp any any eq 2065 (hitcnt
access-list transit-policy line 17 extended deny tcp any any eq 2067 (hitcnt
--          ACL Policy Truncated          --
-- Permit or Deny all other Layer3 and Layer4 --
-- traffic in accordance with existing security --
-- policies and configurations.          --
cisco-fwsm#
```

In the above example, 139 (total) - TCP packets sent to ports TCP/2065 and TCP/2066 have been received from a non-trusted host or network and denied. In addition, the following syslog message will be logged for any attempts that are denied by access list **transit-policy**:

```
Jan 08 2007 09:45:12: %FWSM-4-106023: Deny tcp src outside:192.168.66.6/3910
dst inside:192.168.1.1/2065 by access-group "transit-policy"
```

Additional information about SYSLOG messages is available at [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Message 106023](#).

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-January-10	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

- [IBM Networking: Data-Link Switching \(DLSw\) and Data-Link Switching Plus \(DLSw+\)](#)
- [Data-Link Switching \(DLSw\)](#)
- [Data-Link Switching Plus \(DLSw+\)](#)
- [RFC 1434 - Data Link Switching: Switch-to-Switch Protocol](#) 
- [RFC 1795 - Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1.0](#) 
- [RFC 2166 - APPN Implementer's Workshop Closed Pages Document / DLSw v2.0 Enhancements](#) 
- [Control Plane Policing \(CoPP\)](#)
- [Deploying Control Plane Policing \(CoPP\)](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection \(NFP\) White Papers](#)

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.](#)