

IPsec LAN-to-LAN Tunnel Between a Catalyst 6500 with the VPN Service Module and a VPN 3000 Concentrator Configuration Example

Document ID: 26285

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configuration for IPsec Using an L2 Access or Trunk Port
- Configuration for VPN 3000 Concentrator
- Configuration for IPsec Using a Routed Port

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document describes how to create an IPsec LAN-to-LAN tunnel between a Cisco Catalyst 6500 series switch with the IPsec VPN service module (W) and a Cisco VPN 3000 Concentrator.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Release 12.2.(14)SY2 for the Catalyst 6000 Supervisor Engine, with the IPsec VPN service module
- VPN 3000 Concentrator running software version 4.0.4A

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The Catalyst 6500 VPN service module has two Gigabit Ethernet (GE) ports with no externally visible connectors. These ports are addressable for configuration purposes only. Port 1 is always the inside port. This port handles all traffic from and to the inside network. The second port (port 2) handles all traffic from and to the WAN or outside networks. These two ports are always configured in 802.1Q trunking mode. The VPN service module uses a technique called Bump In The Wire (BITW) for packet flow.

Packets are processed by a pair of VLANs, one Layer 3 (L3) inside VLAN and one Layer 2 (L2) outside VLAN. The packets, from the inside to the outside, are routed through a method called Encoded Address Recognition Logic (EARL) to the inside VLAN. After encrypting the packets, the VPN service module uses the corresponding outside VLAN. In the decryption process, the packets from the outside to the inside are bridged to the VPN service module using the outside VLAN. After the VPN service module decrypts the packet and maps the VLAN to the corresponding inside VLAN, EARL routes the packet to the appropriate LAN port. The L3 inside VLAN and the L2 outside VLANs are joined together by issuing the **crypto connect vlan** command. There are three types of ports in the Catalyst 6500 series switches:

- **Routed ports** By default all Ethernet ports are routed ports. These ports have a hidden VLAN associated with them.
- **Access ports** These ports have an external or VLAN Trunk Protocol (VTP) VLAN associated with them. You can associate more than one port to a defined VLAN.
- **Trunk ports** These ports carry many external or VTP VLANs, on which all packets are encapsulated with an 802.1Q header.

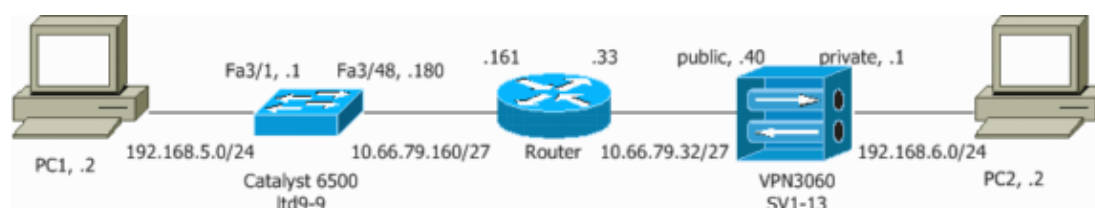
Configure

In this section, you are presented with the information to configure the features described in this document.

Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configuration for IPsec Using an L2 Access or Trunk Port

Complete these steps to configure IPsec using an L2 access or trunk port for the outside physical interface:

1. Add the inside VLANs to the inside port of the VPN service module.

Assuming that the VPN service module is on slot 4, use VLAN 100 as the inside VLAN and VLAN 209 as the outside VLAN. Configure the VPN service module GE ports as follows:

```
interface GigabitEthernet4/1
no ip address
```

```
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. Add the VLAN 100 interface and the interface where the tunnel is terminated (which, in this case, is interface Vlan 209, as shown below).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
no ip address
crypto connect vlan 100
```

3. Configure the outside physical port as an access or trunk port (which, in this case, is FastEthernet 3/48, as shown below).

```
!--- This is the configuration using an access port.
```

```
interface FastEthernet3/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration using a trunk port.
```

```
interface FastEthernet3/48
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Create the Bypass NAT. Add these entries to the no nat statement in order to exempt the nating between these network:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

5. Create your crypto configuration and the access control list (ACL) that defines the traffic to be encrypted.

- a. Create an ACL (in this case, ACL 100) that defines the traffic from the inside network 192.168.5.0/24 to the remote network 192.168.6.0/24, as follows:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

b. Define your Internet Security Association and Key Management Protocol (ISAKMP) policy proposals, as follows:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

c. Issue the following command (in this example) to use and define pre-shared keys:

```
crypto isakmp key cisco address 10.66.79.44
```

d. Define your IPsec proposals, as follows:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

e. Create your crypto map statement, as follows:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.44
set transform-set cisco
match address 100
```

6. Apply the crypto map to the VLAN 100 interface, as follows:

```
interface vlan100
crypto map cisco
```

This configuration is used:

- Catalyst 6500

Catalyst 6500

```
!--- Define the ISAKMP Phase 1 policy proposals.
crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.44
!
!

!--- Define the encryption policy for this setup.
crypto ipsec transform-set cisco esp-des esp-md5-hmac
!

!--- Define a static crypto map entry for the peer
!--- with mode ipsec-isakmp.
!--- This indicates that Internet Key Exchange (IKE)
!--- is used to establish the IPsec
!--- security associations (SAs) for protecting the traffic
!--- specified by this crypto map entry.

crypto map cisco 10 ipsec-isakmp
  set peer 10.66.79.44
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
interface FastEthernet3/1
```

```

ip address 192.168.5.1 255.255.255.0
!

!--- This is the outside L2 port that allows VLAN 209 traffic to enter.

interface FastEthernet3/48
no ip address
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q

!--- VLAN 100 is defined as the Interface VLAN (IVLAN).

switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q

!--- The Port VLAN (PVLAN) configuration is handled transparently
!--- by the VPN service module without user configuration
!--- or involvement. It also is not shown in the configuration.
!--- Note: For every IVLAN, a corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 10.66.79.180 255.255.255.224
no mop enabled

!--- Apply the crypto map to the VLAN 100 interface.
!--- This is the IVLAN that is configured to intercept the traffic
!--- destined to the secure port on which the inside port
!--- of the VPN service module is the only port present.

crypto map cisco
!

!--- This is the secure port that is a virtual L3 interface.
!--- This interface purposely does not have an L3 IP address
!--- configured, which is normal for the BITW process.
!--- The IP address was moved from this interface to the VLAN 100 to
!--- accomplish BITW, which brought the VPN service module into
!--- the packet path.

interface Vlan209
no ip address

```

```

crypto connect vlan 100
!
ip classless

!--- Configure the routing so that the device
!--- is directed to reach its destination network.

ip route 0.0.0.0 0.0.0.0 10.66.79.161
global (outside) 1 interface

!--- NAT 0 prevents NAT for networks specified in the ACL inside_nat0_outbound.

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0

!--- This access list (inside_nat0_outbound) is used with the nat zero command.
!--- This prevents traffic which matches the access list from undergoing
!--- network address translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is intentionally
!--- the same as (100).
!--- Two separate access lists should always be used in this configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
!

!--- This is the crypto ACL.

access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

Configuration for VPN 3000 Concentrator

Complete these steps to configure the VPN 3000 Concentrator:

1. In order to define your IKE proposals, choose **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Add**.

The screenshot shows the 'Add' configuration page for an IKE Proposal. The breadcrumb navigation is 'Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add'. The page title is 'Configure and add a new IKE Proposal'. The configuration fields are as follows:

Field	Value	Description
Proposal Name	LAN-TO-LAN	Specify the name of this IKE Proposal.
Authentication Mode	Preshared Keys	Select the authentication mode to use.
Authentication Algorithm	MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	DES-56	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 2 (1024-bits)	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.

At the bottom of the form are two buttons: 'Add' and 'Cancel'.

Ensure that the new IKE proposal, LAN-TO-LAN, is listed in the Active Proposals column. (To locate Active Proposals, choose **Configuration > System > Tunneling Protocol > IPSec > IKE Proposals**.)

2. In order to define the LAN-to-LAN session configuration, choose **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add**.

Configuration | System | Tunneling Protocols | IPSec | LAN to LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable <input checked="" type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name CAT-6500	Enter the name for this LAN-to-LAN connection.
Interface Ethernet 2 (Public) (10.66.79.44)	Select the interface for this LAN-to-LAN connection.
Connection Type Bi-directional	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers 10.66.79.180	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.
Digital Certificate None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key cisco	Enter the preshared key for this LAN-to-LAN connection.
Authentication ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption DES-56	Specify the encryption mechanism to use.
IKE Proposal LAN-to-LAN	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter -None-	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy -None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing None	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 192.168.6.0	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask 0.0.0.255	

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 192.168.5.0	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask 0.0.0.255	

Configuration for IPsec Using a Routed Port

Complete these steps to configure IPsec using an L3 routed port for the outside physical interface:

1. Add the inside VLANs to the inside port of the VPN service module.

Assuming that the VPN service module is on slot 4, use VLAN 100 as the inside VLAN and VLAN 209 as the outside VLAN, and configure the VPN service module GE ports as follows:

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. Add the VLAN 100 interface and the interface where the tunnel is terminated (which, in this case, is FastEthernet3/48, as shown below).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface FastEthernet3/48
no ip address
crypto connect vlan 100
```

3. Create the Bypass NAT. Add these entries to the no nat statement in order to exempt the nating between these networks:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

4. Create your crypto configuration and the ACL that defines the traffic to be encrypted.

- a. Create an ACL (in this case, ACL 100) that defines the traffic from the inside network 192.168.5.0/24 to the remote network 192.168.6.0/24, as follows:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

- b. Define your ISAKMP policy proposals, as follows:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

- c. Issue this command (in this example) to use and define pre-shared keys:

```
crypto isakmp key cisco address 10.66.79.44
```

- d. Define your IPsec proposals, as follows:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

- e. Create your crypto map statement, as follows:

```
crypto map cisco 10 ipsec-isakmp
```

```
set peer 10.66.79.44
set transform-set cisco
match address 100
```

5. Apply the crypto map to the VLAN 100 interface, as follows:

```
interface vlan100
crypto map cisco
```

This configuration is used:

- Catalyst 6500

Catalyst 6500

```
!--- Define the ISAKMP Phase 1 policy proposals.

crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.44
!
!

!--- Define the encryption policy for this setup.

crypto ipsec transform-set cisco esp-des esp-md5-hmac
!

!--- Define a static crypto map entry for the peer
!--- with mode ipsec-isakmp. This indicates that IKE
!--- is used to establish the IPsec
!--- SAs for protecting the traffic
!--- specified by this crypto map entry.

crypto map cisco 10 ipsec-isakmp
  set peer 10.66.79.44
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
interface FastEthernet3/1
  ip address 192.168.5.1 255.255.255.0
!

!--- This is the secure port that is configured in routed port mode.
!--- This routed port mode purposely does not have an L3 IP address
!--- configured, which is normal for the BITW process.
!--- The IP address was moved from this interface to the VLAN 100 to
!--- accomplish BITW, which brought the VPN service module into
!--- the packet path. This is the L2 port VLAN on which the
!--- outside port of the VPN service module also belongs.

interface FastEthernet3/48
  no ip address
  crypto connect vlan 100
!
interface GigabitEthernet4/1
  no ip address
  flowcontrol receive on
  flowcontrol send off
```

```

switchport
switchport trunk encapsulation dot1q

!--- VLAN 100 is defined as the IVLAN.

switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q

!--- The PVLAN configuration is handled transparently
!--- by the VPN service module without user configuration
!--- or involvement. It also is not shown in the configuration.
!--- Note: For every IVLAN, a corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 10.66.79.180 255.255.255.224
no mop enabled

!--- Apply the crypto map to the VLAN 100 interface.
!--- This is the IVLAN configured to intercept the traffic
!--- destined to the secure port on which the inside port
!--- of the VPN service module is the only port present.

crypto map cisco
!
!
ip classless

!--- Configure the routing so that the device
!--- is directed to reach its destination network.

ip route 0.0.0.0 0.0.0.0 10.66.79.161
!
global (outside) 1 interface

!--- NAT 0 prevents NAT for networks specified in the ACL inside_nat0_outbound.

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0

!--- This access list (inside_nat0_outbound) is used with the nat zero command.
!--- This prevents traffic which matches the access list from undergoing
!--- network address translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is intentionally
!--- the same as (100).
!--- Two separate access lists should always be used in this configuration.

```

```

access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL.

access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

Verify

This section provides information you can use to confirm your configuration is working properly.

For additional information on verifying and troubleshooting IPsec, refer to IP Security Troubleshooting – Understanding and Using debug Commands.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto ipsec sa** Shows the settings used by the current IPsec SAs.
- **show crypto isakmp sa** Shows all current IKE SAs at a peer.
- **show crypto vlan** Shows the VLAN associated with the crypto configuration.
- **show crypto eli** Shows the VPN service module statistics.

In the VPN 3000 Concentrator, choose **Monitoring > Sessions**, and click the **CAT-6500** connection. Verify that the packets are being encrypted and decrypted, and verify other information about this session.

Monitoring | Sessions | Detail
Monday, 22 December 2003 19:57:47

[Reset](#)

[Back to Sessions](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
CAT-6500	10.66.79.180	IPSec/LAN-to-LAN	DES-56	Dec 22 19:02:20	0:55:27	936	936

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	192.168.5.0/0.0.0.255
Local Address	192.168.6.0/0.0.0.255	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	3600 seconds
Rekey Data Interval	4608000 KBytes		
Bytes Received	936	Bytes Transmitted	936

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

For additional information on verifying and troubleshooting IPsec, refer to IP Security Troubleshooting – Understanding and Using debug Commands.

Troubleshooting Commands

Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Shows the IPsec negotiations of Phase 2.
- **debug crypto isakmp** Shows the ISAKMP negotiations of Phase 1.
- **debug crypto engine** Shows the traffic that is encrypted.
- **clear crypto isakmp** Clears the SAs related to Phase 1.
- **clear crypto sa** Clears the SAs related to Phase 2.

In order to enable several debugs, choose **Configuration > System > Events > Classes** in the VPN 3000 Concentrator, then add or modify the following "Class Names" Events to Log with Severities 1™3:

- IKE
- IKEDBG
- IPSEC
- IPSECDBG

These are the debugs for this session:

```
1 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=1 10.66.79.180
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 124

3 12/22/2003 20:12:25.950 SEV=9 IKEDBG/0 RPT=2 10.66.79.180
processing SA payload

4 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=3
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

9 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=4
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

12 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=5
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

15 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=6
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

18 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=7
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
```

Cfg'd: Oakley Group 7

21 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=8
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

24 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=9
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 5

27 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=10
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: AES

30 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=11
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: AES

33 12/22/2003 20:12:25.950 SEV=7 IKEDBG/0 RPT=12 10.66.79.180
Oakley proposal is acceptable

34 12/22/2003 20:12:25.950 SEV=9 IKEDBG/47 RPT=1 10.66.79.180
processing VID payload

35 12/22/2003 20:12:25.950 SEV=9 IKEDBG/49 RPT=1 10.66.79.180
Received NAT-Traversal ver 03 VID

36 12/22/2003 20:12:25.950 SEV=9 IKEDBG/47 RPT=2 10.66.79.180
processing VID payload

37 12/22/2003 20:12:25.950 SEV=9 IKEDBG/49 RPT=2 10.66.79.180
Received NAT-Traversal ver 02 VID

38 12/22/2003 20:12:25.950 SEV=9 IKEDBG/0 RPT=13 10.66.79.180
processing IKE SA

39 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=14
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

44 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=15
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

47 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=16
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

50 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=17
Phase 1 failure against global IKE proposal # 4:

Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

53 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=18
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7

56 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=19
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

59 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=20
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 5

62 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=21
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: AES

65 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=22
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: AES

68 12/22/2003 20:12:25.950 SEV=7 IKEDBG/28 RPT=1 10.66.79.180
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 10 Proposal (LAN-to-LAN)

70 12/22/2003 20:12:25.950 SEV=9 IKEDBG/0 RPT=23 10.66.79.180
constructing ISA_SA for isakmp

71 12/22/2003 20:12:25.950 SEV=9 IKEDBG/46 RPT=1 10.66.79.180
constructing Fragmentation VID + extended capabilities payload

72 12/22/2003 20:12:25.950 SEV=8 IKEDBG/0 RPT=24 10.66.79.180
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13)
total length : 108

74 12/22/2003 20:12:25.960 SEV=8 IKEDBG/0 RPT=25 10.66.79.180
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ NONE (0)
total length : 256

77 12/22/2003 20:12:25.960 SEV=8 IKEDBG/0 RPT=26 10.66.79.180
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ NONE (0)
total length : 256

80 12/22/2003 20:12:25.960 SEV=9 IKEDBG/0 RPT=27 10.66.79.180
processing ke payload

81 12/22/2003 20:12:25.960 SEV=9 IKEDBG/0 RPT=28 10.66.79.180
processing ISA_KE

82 12/22/2003 20:12:25.960 SEV=9 IKEDBG/1 RPT=1 10.66.79.180
processing nonce payload

83 12/22/2003 20:12:25.960 SEV=9 IKEDBG/47 RPT=3 10.66.79.180
processing VID payload

84 12/22/2003 20:12:25.960 SEV=9 IKEDBG/49 RPT=3 10.66.79.180
Received Cisco Unity client VID

85 12/22/2003 20:12:25.960 SEV=9 IKEDBG/47 RPT=4 10.66.79.180
processing VID payload

86 12/22/2003 20:12:25.960 SEV=9 IKEDBG/49 RPT=4 10.66.79.180
Received DPD VID

87 12/22/2003 20:12:25.960 SEV=9 IKEDBG/47 RPT=5 10.66.79.180
processing VID payload

88 12/22/2003 20:12:25.960 SEV=9 IKEDBG/38 RPT=1 10.66.79.180
Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 0000037f)

89 12/22/2003 20:12:25.960 SEV=9 IKEDBG/47 RPT=6 10.66.79.180
processing VID payload

90 12/22/2003 20:12:25.960 SEV=9 IKEDBG/49 RPT=5 10.66.79.180
Received xauth V6 VID

91 12/22/2003 20:12:25.990 SEV=9 IKEDBG/0 RPT=29 10.66.79.180
constructing ke payload

92 12/22/2003 20:12:25.990 SEV=9 IKEDBG/1 RPT=2 10.66.79.180
constructing nonce payload

93 12/22/2003 20:12:25.990 SEV=9 IKEDBG/46 RPT=2 10.66.79.180
constructing Cisco Unity VID payload

94 12/22/2003 20:12:25.990 SEV=9 IKEDBG/46 RPT=3 10.66.79.180
constructing xauth V6 VID payload

95 12/22/2003 20:12:25.990 SEV=9 IKEDBG/48 RPT=1 10.66.79.180
Send IOS VID

96 12/22/2003 20:12:25.990 SEV=9 IKEDBG/38 RPT=2 10.66.79.180
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000409)

98 12/22/2003 20:12:25.990 SEV=9 IKEDBG/46 RPT=4 10.66.79.180
constructing VID payload

99 12/22/2003 20:12:25.990 SEV=9 IKEDBG/48 RPT=2 10.66.79.180
Send Altiga GW VID

100 12/22/2003 20:12:25.990 SEV=9 IKEDBG/0 RPT=30 10.66.79.180
Generating keys for Responder...

101 12/22/2003 20:12:26.000 SEV=8 IKEDBG/0 RPT=31 10.66.79.180
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10)
total length : 256

103 12/22/2003 20:12:26.000 SEV=8 IKEDBG/0 RPT=32 10.66.79.180
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NOTIFY (11) + NONE (0)
total length : 88

105 12/22/2003 20:12:26.000 SEV=9 IKEDBG/1 RPT=3 10.66.79.180
Group [10.66.79.180]
Processing ID

106 12/22/2003 20:12:26.000 SEV=9 IKEDBG/0 RPT=33 10.66.79.180
Group [10.66.79.180]
processing hash

107 12/22/2003 20:12:26.000 SEV=9 IKEDBG/0 RPT=34 10.66.79.180
Group [10.66.79.180]
computing hash

108 12/22/2003 20:12:26.000 SEV=9 IKEDBG/0 RPT=35 10.66.79.180
Group [10.66.79.180]
Processing Notify payload

109 12/22/2003 20:12:26.000 SEV=9 IKEDBG/23 RPT=1 10.66.79.180
Group [10.66.79.180]
Starting group lookup for peer 10.66.79.180

110 12/22/2003 20:12:26.100 SEV=7 IKEDBG/0 RPT=36 10.66.79.180
Group [10.66.79.180]
Found Phase 1 Group (10.66.79.180)

111 12/22/2003 20:12:26.100 SEV=7 IKEDBG/14 RPT=1 10.66.79.180
Group [10.66.79.180]
Authentication configured for Internal

112 12/22/2003 20:12:26.100 SEV=9 IKEDBG/19 RPT=1 10.66.79.180
Group [10.66.79.180]
IKEGetUserAttributes: IP Compression = disabled

113 12/22/2003 20:12:26.100 SEV=9 IKEDBG/19 RPT=2 10.66.79.180
Group [10.66.79.180]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

114 12/22/2003 20:12:26.100 SEV=9 IKEDBG/1 RPT=4 10.66.79.180
Group [10.66.79.180]
constructing ID

115 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=37
Group [10.66.79.180]
construct hash payload

116 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=38 10.66.79.180
Group [10.66.79.180]
computing hash

117 12/22/2003 20:12:26.100 SEV=9 IKEDBG/34 RPT=1 10.66.79.180
Constructing IOS keep alive payload: proposal=32767/32767 sec.

118 12/22/2003 20:12:26.100 SEV=9 IKEDBG/46 RPT=5 10.66.79.180
Group [10.66.79.180]
constructing dpd vid payload

119 12/22/2003 20:12:26.100 SEV=8 IKEDBG/0 RPT=39 10.66.79.180
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8)
total length : 92

121 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=40
Delete with reason code capability is negotiated

122 12/22/2003 20:12:26.100 SEV=4 IKE/119 RPT=5 10.66.79.180
Group [10.66.79.180]
PHASE 1 COMPLETED

123 12/22/2003 20:12:26.100 SEV=6 IKE/121 RPT=5 10.66.79.180
Keep-alive type for this connection: DPD

124 12/22/2003 20:12:26.100 SEV=7 IKEDBG/0 RPT=41 10.66.79.180
Group [10.66.79.180]
Starting phase 1 rekey timer: 82080000 (ms)

125 12/22/2003 20:12:26.100 SEV=4 AUTH/22 RPT=5
User [10.66.79.180] Group [10.66.79.180] connected, Session Type: IPSec/LAN-to-LAN

127 12/22/2003 20:12:26.100 SEV=4 AUTH/84 RPT=2
LAN-to-LAN tunnel to headend device 10.66.79.180 connected

128 12/22/2003 20:12:26.100 SEV=8 IKEDBG/0 RPT=42 10.66.79.180
RECEIVED Message (msgid=7adf63fe) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
total length : 164

131 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=43 10.66.79.180
Group [10.66.79.180]
processing hash

132 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=44 10.66.79.180
Group [10.66.79.180]
processing SA payload

133 12/22/2003 20:12:26.100 SEV=9 IKEDBG/1 RPT=5 10.66.79.180
Group [10.66.79.180]
processing nonce payload

134 12/22/2003 20:12:26.100 SEV=9 IKEDBG/1 RPT=6 10.66.79.180
Group [10.66.79.180]
Processing ID

135 12/22/2003 20:12:26.100 SEV=5 IKE/35 RPT=2 10.66.79.180
Group [10.66.79.180]
Received remote IP Proxy Subnet data in ID Payload:
Address 192.168.5.0, Mask 255.255.255.0, Protocol 0, Port 0

138 12/22/2003 20:12:26.100 SEV=9 IKEDBG/1 RPT=7 10.66.79.180
Group [10.66.79.180]
Processing ID

139 12/22/2003 20:12:26.100 SEV=5 IKE/34 RPT=4 10.66.79.180
Group [10.66.79.180]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.6.0, Mask 255.255.255.0, Protocol 0, Port 0

142 12/22/2003 20:12:26.100 SEV=8 IKEDBG/0 RPT=45
QM IsRekeyed old sa not found by addr

143 12/22/2003 20:12:26.100 SEV=5 IKE/66 RPT=7 10.66.79.180
Group [10.66.79.180]
IKE Remote Peer configured for SA: L2L: CAT-6500

144 12/22/2003 20:12:26.100 SEV=9 IKEDBG/0 RPT=46 10.66.79.180
Group [10.66.79.180]
processing IPSEC SA

145 12/22/2003 20:12:26.100 SEV=7 IKEDBG/27 RPT=1 10.66.79.180
Group [10.66.79.180]
IPSec SA Proposal # 1, Transform # 1 acceptable
Matches global IPSec SA entry # 10 Proposal (L2L: CAT-6500)

148 12/22/2003 20:12:26.100 SEV=7 IKEDBG/0 RPT=47 10.66.79.180
Group [10.66.79.180]
IKE: requesting SPI!

149 12/22/2003 20:12:26.100 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 208, vers 1, pid 00000000, seq 8, err 0
, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyL
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 636852, lifetime2 0, dsId
300

153 12/22/2003 20:12:26.100 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

154 12/22/2003 20:12:26.110 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 713229868

155 12/22/2003 20:12:26.110 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x2a83062c

156 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=48 10.66.79.180
Group [10.66.79.180]
oakley constucting quick mode

157 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=49 10.66.79.180
Group [10.66.79.180]
constructing blank hash

158 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=50 10.66.79.180
Group [10.66.79.180]
constructing ISA_SA for ipsec

159 12/22/2003 20:12:26.110 SEV=9 IKEDBG/1 RPT=8 10.66.79.180
Group [10.66.79.180]
constructing ipsec nonce payload

160 12/22/2003 20:12:26.110 SEV=9 IKEDBG/1 RPT=9 10.66.79.180
Group [10.66.79.180]
constructing proxy ID

161 12/22/2003 20:12:26.110 SEV=7 IKEDBG/0 RPT=51 10.66.79.180
Group [10.66.79.180]
Transmitting Proxy Id:
Remote subnet: 192.168.5.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 192.168.6.0 mask 255.255.255.0 Protocol 0 Port 0

165 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=52 10.66.79.180
Group [10.66.79.180]
constructing qm hash

166 12/22/2003 20:12:26.110 SEV=8 IKEDBG/0 RPT=53 10.66.79.180
SENDING Message (msgid=7adf63fe) with payloads :
HDR + HASH (8) + SA (1)
total length : 164

168 12/22/2003 20:12:26.110 SEV=8 IKEDBG/0 RPT=54 10.66.79.180
RECEIVED Message (msgid=7adf63fe) with payloads :
HDR + HASH (8) + NONE (0)
total length : 48

170 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=55 10.66.79.180
Group [10.66.79.180]
processing hash

171 12/22/2003 20:12:26.110 SEV=9 IKEDBG/0 RPT=56 10.66.79.180
Group [10.66.79.180]
loading all IPSEC SAs

172 12/22/2003 20:12:26.110 SEV=9 IKEDBG/1 RPT=10 10.66.79.180
Group [10.66.79.180]
Generating Quick Mode Key!

173 12/22/2003 20:12:26.120 SEV=9 IKEDBG/1 RPT=11 10.66.79.180
Group [10.66.79.180]
Generating Quick Mode Key!

174 12/22/2003 20:12:26.120 SEV=7 IKEDBG/0 RPT=57 10.66.79.180
Group [10.66.79.180]
Loading subnet:
 Dst: 192.168.6.0 mask: 255.255.255.0
 Src: 192.168.5.0 mask: 255.255.255.0

177 12/22/2003 20:12:26.120 SEV=4 IKE/49 RPT=8 10.66.79.180
Group [10.66.79.180]
Security negotiation complete for LAN-to-LAN Group (10.66.79.180)
Responder, Inbound SPI = 0x2a83062c, Outbound SPI = 0x1f18e9ee

180 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, len 317, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 8256, label 0, pad 0, spi 1f18e9ee, encrKeyLen 8, hashKe
yLen 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 636852, lifetime2 0, d
sId -378167296

184 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD msg!

185 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

186 12/22/2003 20:12:26.120 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

187 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter

188 12/22/2003 20:12:26.120 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

189 12/22/2003 20:12:26.120 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 192.168.6.0 mask 0.0.0.255, dst 192.168.5.0 mask 0.0.0.255

190 12/22/2003 20:12:26.120 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpssecAddIkeSa success

191 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, len 317, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 8224, label 0, pad 0, spi 2a83062c, encrKeyLen 8, hashKe
yLen 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 636852, lifetime2 0, d
sId -378167296

195 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE msg!

196 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

197 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

198 12/22/2003 20:12:26.120 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

199 12/22/2003 20:12:26.120 SEV=9 IPSECDBG/1 RPT=13

KeyProcessUpdate: Enter

200 12/22/2003 20:12:26.120 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

201 12/22/2003 20:12:26.120 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD msg for SA: SPI = 0x1f18e9ee

202 12/22/2003 20:12:26.120 SEV=8 IKEDBG/0 RPT=58
pitcher: rcv KEY_UPDATE, spi 0x2a83062c

203 12/22/2003 20:12:26.120 SEV=4 IKE/120 RPT=8 10.66.79.180
Group [10.66.79.180]
PHASE 2 COMPLETED (msgid=7adf63fe)

204 12/22/2003 20:12:27.940 SEV=7 IPSECDBG/1 RPT=15
IPSec Inbound SA has received data!

205 12/22/2003 20:12:27.940 SEV=8 IKEDBG/0 RPT=59
pitcher: recv KEY_SA_ACTIVE spi 0x2a83062c

206 12/22/2003 20:12:27.940 SEV=8 IKEDBG/0 RPT=60
KEY_SA_ACTIVE no old rekey centry found with new spi 0x2a83062c, mess_id 0x0

207 12/22/2003 20:12:44.390 SEV=9 IKEDBG/36 RPT=1 10.66.79.180
Group [10.66.79.180]
Sending keep-alive of type DPD R-U-THERE (seq number 0x10ecefbb)

209 12/22/2003 20:12:44.390 SEV=9 IKEDBG/0 RPT=61 10.66.79.180
Group [10.66.79.180]
constructing blank hash

210 12/22/2003 20:12:44.390 SEV=9 IKEDBG/0 RPT=62 10.66.79.180
Group [10.66.79.180]
constructing qm hash

211 12/22/2003 20:12:44.390 SEV=8 IKEDBG/0 RPT=63 10.66.79.180
SENDING Message (msgid=50760703) with payloads :
HDR + HASH (8) + NOTIFY (11)
total length : 80

213 12/22/2003 20:12:44.400 SEV=8 IKEDBG/0 RPT=64 10.66.79.180
RECEIVED Message (msgid=7dd8f884) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0)
total length : 80

215 12/22/2003 20:12:44.400 SEV=9 IKEDBG/0 RPT=65 10.66.79.180
Group [10.66.79.180]
processing hash

216 12/22/2003 20:12:44.400 SEV=9 IKEDBG/0 RPT=66 10.66.79.180
Group [10.66.79.180]
Processing Notify payload

Related Information

- [IPSec Support Page](#)
- [Configuring IPSec Network Security](#)
- [Configuring Internet Key Exchange Security Protocol](#)
- [Technical Support & Documentation – Cisco Systems](#)

