IPSec between PIX Firewall and Cisco VPN 3000 Concentrator with Overlapping Private Networks Configuration Example

Document ID: 23193

Contents

Introduction

This document describes how to configure the Cisco Secure PIX Firewall in a site−to−site IPSec VPN with overlapping private network addresses behind VPN gateways. The enhanced Network Address Translation (NAT) feature introduced in PIX 6.2 is used in this example to translate the overlapping networks on each side of the IPSec VPN tunnel to non−overlapping address spaces.

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 Secure PIX Firewall 506 with software version 6.3(3)
- VPN 3030 Concentrator with software version 4.1(5)

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

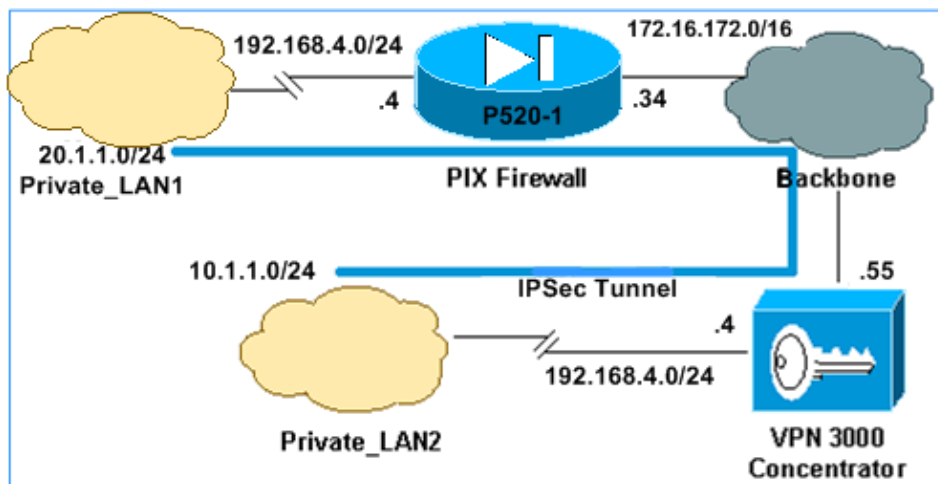For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configure

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

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in this diagram.

Both Private_LAN1 and Private_LAN2 have an IP subnet of 192.168.4.0/24. This simulates the overlapping address space behind each side of the IPSec tunnel. The VPN 3000 Concentrator is used here as one example of a concentrator which does not have the functionality of NAT over VPN traffic.

In this example, the PIX performs a bi−directional translation so that the two private LANs can communicate over the IPSec tunnel. The translation means that Private_LAN1 "sees" Private_LAN2 as 10.1.1.0/24 through the IPSec tunnel, and Private_LAN2 "sees" Private_LAN1 as 20.1.1.0/24 through the IPSec tunnel.

Configurations

PIX
| ```
P520−1(config)#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname P520−1
domain−name bru−ch.com
fixup protocol dns maximum−length 512
fixup protocol ftp 21
``` |

```
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
```

!--- Defines IPSec interesting traffic.
!--- Note that the host behind PIX communicates
!--- to Private_LAN1 using 10.1.1.0/24.
!--- When the packets arrive at the PIX, they are first
!--- translated to 192.168.4.0/24 and then encrypted by IPSec.

access-list 101 permit ip 20.1.1.0 255.255.255.0 192.168.4.0 255.255.255.0
```
pager lines 24
mtu outside 1500
mtu inside 1500
```
ip address outside 172.16.172.34 255.255.255.0
ip address inside 192.168.4.4 255.255.255.0
```
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
```

!--- Static translation defined to translate Private_LAN2
!--- from 192.168.4.0/24 to 10.1.1.0/24.

static (outside,inside) 10.1.1.0 192.168.4.0 netmask 255.255.255.0 0 0

!--- Static translation defined to translate Private_LAN1
!--- from 192.168.4.0/24 to 20.1.1.0/24.
!--- Note that this translation is used for both
!--- VPN and Internet traffic from Private_LAN1.
!--- A routable global IP address range, or an extra NAT
!--- at the ISP router (in front of PIX), is
!--- required if Private_LAN1 also needs internal access.

static (inside,outside) 20.1.1.0 192.168.4.0 netmask 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.16.172.55 1
```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
```
sysopt connection permit-ipsec

!--- Defines IPSec encryption and authentication algorithms.

crypto ipsec transform-set myset esp-des esp-md5-hmac

!--- Defines crypto map.

crypto map vpn 10 ipsec-isakmp

```
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 172.16.172.55
crypto map vpn 10 set transform-set myset

!--- Apply crypto map on the outside interface.

crypto map vpn interface outside
isakmp enable outside

!--- Defines pre-shared secret (cisco123) used for IKE authentication.

isakmp key ******** address 172.16.172.55 netmask 255.255.255.255
isakmp identity address

!--- Defines ISAKMP policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:6cc25fc2fea20958dfe74c1fca45ada2
: end
```

VPN 3000 Concentrator LAN−to−LAN Tunnel Configuration

For the destination address 20.1.1.0 /24 (Private_LAN1) you need to have a static route on the VPN 3000. To do, select **Configuration > System > IP Routing > Static Routes** and choose **Add**. Once you are done filling out the fields, click **Add**.

Use the settings in these images to configure your VPN 3000 Concentrator.

Add a new IPSec LAN-to-LAN connection.

Enable	☑	Check to enable this LAN-to-LAN connection.
Name	ToPIX	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.16.172.55) ▼	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional ▼	Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.
Peers	172.16.172.34	Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* 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	○ Entire certificate chain ● Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	cisco123	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	IKE-DES-MD5 ▼	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	☐	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 [192.168.4.0]

Note: Enter a *wildcard* 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 [20.1.10]

Note: Enter a *wildcard* 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]

[Add] [Cancel]

Verify

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

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show crypto isakmp sa** – Display all current Internet Key Exchange (IKE) security associations (SAs) at a peer.
- **show crypto isakmp sa detail** – Display the details of all current IKE SAs at a peer.
- **show crypto ipsec sa** – Displays the settings used by current SAs.
- **show xlate detail** – Displays translation slot information.

PIX

```
P520-1(config)#
P520-1(config)#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst                 src          state      pending      created
   172.16.172.55    172.16.172.34    QM_IDLE          0            1

P520-1(config)#show crypto isakmp sa detail
Total     : 1
Embryonic : 0
        Local              Remote            Encr Hash    Auth  State        Lifetime
   172.16.172.34:500    172.16.172.55:500  des  md5       psk QM_IDLE        86211
P520-1(config)#

P520-1(config)#show crypto ipsec sa


interface: outside
    Crypto map tag: vpn, local addr. 172.16.172.34

    local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
```

```
   current_peer: 172.16.172.55:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

    local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.55
    path mtu 1500, ipsec overhead 56, media mtu 1500
    current outbound spi: 734575cb

    inbound esp sas:
     spi: 0xe028850d(3760751885)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4607999/28751)
        IV size: 8 bytes
        replay detection support: Y


   inbound ah sas:


    inbound pcp sas:


    outbound esp sas:
     spi: 0x734575cb(1933931979)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4607999/28751)
        IV size: 8 bytes
        replay detection support: Y


    outbound ah sas:

P520-1(config)#show xlate detail
2 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
NAT from inside:192.168.4.1 to outside:20.1.1.1 flags s
NAT from outside:192.168.4.1 to inside:10.1.1.1 flags s
```

Use ping traffic to verify the tunnel. This **debug icmp trace** output collected on the PIX illustrates how the packets are translated by NAT.

```
P520-1(config)# debug icmp trace
ICMP trace on
Warning: this may cause problems on busy networks
P520-1(config)#
1: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3060 seq=4391 length=80
2: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
3: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
4: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3060 seq=4391 length=80
5: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
6: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
7: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3061 seq=4391 length=80
8: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
9: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
10: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3061 seq=4391 length=80
11: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
```

```
12: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
13: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3062 seq=4391 length=80
14: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
15: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
16: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3062 seq=4391 length=80
17: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
18: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
19: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3063 seq=4391 length=80
20: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
21: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
22: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3063 seq=4391 length=80
23: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
24: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
25: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3064 seq=4391 length=80
26: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
27: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
28: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3064 seq=4391 length=80
29: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
30: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
P520-1(config)#
```

VPN Concentrator

Select **Monitoring > Sessions > Detail** to verify your VPN 3000 Concentrator configuration.

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
ToPIX	172.16.172.34	IPSec/LAN-to-LAN	DES-56	Jul 07 18:09:20	0:08:13	416	416

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	20.1.1.0/0.0.0.255
Local Address	192.168.4.0/0.0.0.255	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Rekey Data Interval	4608000 KBytes		
Bytes Received	416	Bytes Transmitted	416

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Additional information on troubleshooting can be found in the following documents:

- Troubleshooting Connection Problems on the VPN 3000 Concentrator
- IP Security Troubleshooting – Understanding and Using debug Commands
- Troubleshooting the PIX to Pass Data Traffic on an Established IPSec Tunnel

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

This output demonstrates a working debug of the IKE negotiation. Shown here are the outputs of the **debug crypto isakmp** and **debug crypto ipsec** commands.

```
P520-1(config)#show debug
debug crypto ipsec 1
debug crypto isakmp 1
P520-1(config)#
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:       encryption DES-CBC
ISAKMP:       hash MD5
ISAKMP:       default group 1
ISAKMP:       auth pre-share
ISAKMP:       life type in seconds
ISAKMP:       life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): received xauth v6 vendor id
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to another IOS box!
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to a VPN3000 concentrator
ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of -995061605:c4b0909bIPSEC
(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xe028850d(3760751885) for SA
        from   172.16.172.55 to   172.16.172.34 for prot 3
```

```
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.16.172.55/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.16.172.55/500 Ref cnt incremented to:1 Total
VPN Peers:1
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3299905691
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:    attributes in transform:
ISAKMP:       SA life type in seconds
ISAKMP:       SA life duration (basic) of 28800
ISAKMP:       SA life type in kilobytes
ISAKMP:       SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:       encaps is 1
ISAKMP:       authenticator is HMAC-MD5
```
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
```
  (key eng. msg.) dest= 172.16.172.55, src= 172.16.172.34,
    dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
   src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 3299905691
ISAKMP (0): processing ID payload. message ID = 3299905691
ISAKMP (0): processing ID payload. message ID = 3299905691
```
ISAKMP (0): Creating IPSec SAs
```
        inbound SA from   172.16.172.55 to   172.16.172.34
        (proxy 192.168.4.0 to   20.1.1.0)
        has spi 3760751885 and conn_id 1 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.16.172.34 to   172.16.172.55
       (proxy         20.1.1.0 to      192.168.4.0)
        has spi 1933931979 and conn_id 2 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.172.34, src= 172.16.172.55,
    dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xe028850d(3760751885), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.172.34, dest= 172.16.172.55,
    src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x734575cb(1933931979), conn_id= 2, keysize= 0, flags= 0x4
```
VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:3 Total VPN Peers:1
```
return status is IKMP_NO_ERROR
P520-1(config)#
P520-1(config)#
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 1690390088
ISAMKP (0): received DPD_R_U_THERE from peer 172.16.172.55
```

```
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
P520-1(config)#
```

Related Information

- **Security and VPN Product Support Pages**
- **Security and VPN Technology Support Pages**
- **IPSec Support Page**
- **Technical Support – Cisco Systems**

Updated: Jan 18, 2008   Document ID: 23193