

# 在 IOS 路由器上通过 PAT 传递 LAN 到 LAN IPSec 隧道的配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[采用 IPSec NAT 透明模式的配置](#)

[未采用 IPSec NAT 透明模式的配置](#)

[验证](#)

[采用 IPSec NAT 透明模式的验证](#)

[未采用 IPSec NAT 透明模式的验证](#)

[故障排除](#)

[采用 IPSec NAT 透明模式的故障排除](#)

[未采用 IPSec NAT 透明模式的故障排除](#)

[相关信息](#)

## 简介

本文档提供端口地址转换(PAT)的示例配置，以允许建立LAN到LAN IPSec隧道。它适用于只有一个公用 IP 地址（在 Cisco IOS® 路由器中用于执行所有流量的 PAT）并且需要通过该地址经过 IPSec 隧道的情况。

对于运行早于12.2(13)T的Cisco IOS软件版本的VPN网关，执行PAT的路由器上需要IPSec传递功能，以允许封装安全负载(ESP)通过。

注意：此功能在[软件建议](#)中称为通过网络地址转换(NAT)的IPSec支持(仅限[注册](#)客户)。

要从本地（经过 PAT 的）对等体开始建立隧道，不需要进行任何配置。要从远程对等体开始建立隧道，则需要以下命令：

- ip nat inside source static esp inside\_ip interface interface
- ip nat inside source static udp inside\_ip 500 interface interface 500

对于运行高于12.2(13)T的Cisco IOS软件版本的VPN网关，IPSec流量将封装到用户数据协议(UDP)端口4500数据包中。此功能称为 [IPSec NAT 透明模式](#)。要从本地（经过 PAT 的）对等体开始建立隧道，不需要进行任何配置。

要从远程对等体开始建立隧道，则需要以下命令：

- ip nat inside source static udp inside\_ip 4500 interface interface 4500
- ip nat inside source static udp inside\_ip 500 interface interface 500

发出 `no crypto ipsec nat-transparency udp-encaps` 命令可禁用 [IPSec NAT 透明模式](#)。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息以 Cisco IOS 软件版本 12.3(7)T1 为基准。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

### 网络图

本文档使用以下网络设置：

#### 采用 IPSec NAT 透明模式的配置

本文档使用以下配置：

- [VPN-Gateway1](#)
- [PAT-Router](#)
- [VPN-Gateway2](#)

```
<#root>
```

```
VPN-Gateway1#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 1017 bytes
```

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname VPN-Gateway1  
!
```

```
!--- VPN Gateway1 and VPN Gateway2 can be any devices that !--- perform IPSec. For detailed information
```

```
boot-start-marker  
boot-end-marker  
!  
!  
clock timezone EST 0  
no aaa new-model  
ip subnet-zero  
!  
!  
ip audit po max-events 100  
no ftp-server write-enable  
!  
!  
!  
!
```

```
!--- IKE policies (phase 1).
```

```
crypto isakmp policy 10  
 authentication pre-share  
crypto isakmp key cisco123 address 209.165.201.2
```

```
!  
!
```

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

```
!
```

```
!--- IPSec policies (phase 1).
```

```
crypto map mymap 10 ipsec-isakmp  
 set peer 209.165.201.2  
 set transform-set basic  
 match address 101
```

```
!  
!  
!
```

```
interface Ethernet0/0  
 ip address 192.168.1.1 255.255.255.0
```

```
!  
interface Serial1/0  
 ip address 209.165.200.2 255.255.255.252  
 serial restart-delay 0  
  
crypto map mymap  
  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.200.1  
no ip http server  
no ip http secure-server  
!  
!  
!  
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255  
access-list 101 remark Crypto ACL  
  
!  
!  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

```
<#root>
```

```
PAT-Router#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 971 bytes
```

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname PAT-Router  
!  
boot-start-marker  
boot-end-marker  
!  
!  
clock timezone EST 0  
no aaa new-model
```

```
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
no crypto isakmp enable
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0

!--- This declares the interface as inside for NAT purposes.

ip nat inside
!
interface Serial1/0
 ip address 209.165.201.2 255.255.255.224

!--- This declares the interface as !--- outside for NAT purposes.

ip nat outside
 serial restart-delay 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 172.16.0.0 255.255.0.0 172.16.1.2
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface Serial1/0 overload

!--- This allows PAT to be used for regular Internet traffic.

ip nat inside source static udp 172.16.1.2 4500 interface Serial1/0 4500

!--- This permits IPSec traffic destined for the Serial1/0 !--- interface to be sent to the inside IP .

ip nat inside source static udp 172.16.1.2 500 interface Serial1/0 500

!--- This allows UDP traffic for the Serial1/0 interface to be !--- statically mapped to the inside IP .

!
!
access-list 1 permit 172.16.0.0 0.0.255.255
!
!
```

```
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

```
<#root>
```

```
VPN-Gateway2#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 986 bytes
```

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname VPN-Gateway2  
!
```

```
!--- VPN Gateway1 and VPN Gateway2 can be any devices !--- that perform IPSec. For detailed information
```

```
boot-start-marker  
boot-end-marker
```

```
!  
!  
clock timezone EST 0  
no aaa new-model  
ip subnet-zero  
!  
!  
ip audit po max-events 100  
no ftp-server write-enable  
!  
!  
!  
!
```

```
!--- IKE policies (phase 1).
```

```
crypto isakmp policy 10  
 authentication pre-share  
crypto isakmp key cisco123 address 209.165.200.2
```

```

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

!

!--- IPsec policies (phase 1).

crypto map mymap 10 ipsec-isakmp
 set peer 209.165.200.2
 set transform-set basic
 match address 101

!
!
!
interface Ethernet0/0
 ip address 172.16.1.2 255.255.255.0

crypto map mymap

!
interface Ethernet1/0
 ip address 172.16.2.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
no ip http server
no ip http secure-server
!
!
!
access-list 101 permit ip 172.16.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 101 remark Crypto ACL

!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

## 未采用 IPsec NAT 透明模式的配置

- [VPN-Gateway1](#)
- [PAT-Router](#)

- [VPN-Gateway2](#)

```
<#root>
```

```
VPN-Gateway1#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 1017 bytes
```

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname VPN-Gateway1  
!
```

```
!--- VPN Gateway1 and VPN Gateway2 can be any devices !--- that perform IPsec. For detailed information
```

```
boot-start-marker  
boot-end-marker
```

```
!  
!  
clock timezone EST 0  
no aaa new-model  
ip subnet-zero  
!  
!  
ip audit po max-events 100  
no ftp-server write-enable  
!  
!  
!  
!
```

```
!--- IKE policies (phase 1).
```

```
crypto isakmp policy 10  
 authentication pre-share  
crypto isakmp key cisco123 address 209.165.201.2
```

```
!  
!
```

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

```
!
```

```
!--- IPsec policies (phase 1).
```

```
crypto map mymap 10 ipsec-isakmp
```



```
set peer 209.165.201.2
set transform-set basic
match address 101

!
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 209.165.200.2 255.255.255.252
 serial restart-delay 0

crypto map mymap

!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
no ip http server
no ip http secure-server
!
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255
access-list 101 remark Crypto ACL

!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

```
<#root>
```

```
PAT-Router#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 971 bytes
```

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!  
hostname PAT-Router  
!  
boot-start-marker  
boot-end-marker  
!  
!  
clock timezone EST 0  
no aaa new-model  
ip subnet-zero  
!  
!  
ip audit po max-events 100  
no ftp-server write-enable  
!  
!  
!  
no crypto isakmp enable  
!  
!  
!  
interface Ethernet0/0  
 ip address 172.16.1.1 255.255.255.0  
  
!--- This declares the interface as inside for NAT purposes.  
  
ip nat inside  
!  
interface Serial1/0  
 ip address 209.165.201.2 255.255.255.224  
  
!--- This declares the interface as !--- outside for NAT purposes.  
  
ip nat outside  
 serial restart-delay 0  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.201.1  
ip route 172.16.0.0 255.255.0.0 172.16.1.2  
no ip http server  
no ip http secure-server  
!  
ip nat inside source list 1 interface Serial1/0 overload  
  
!--- This allows PAT to be used for regular Internet traffic.  
  
ip nat inside source static esp 172.16.1.2 interface Serial1/0  
  
!--- This permits the IPSec ESP tunnel mode !--- destined for the Serial1/0 interface to be sent !---  
  
ip nat inside source static udp 172.16.1.2 500 interface Serial1/0 500
```

```
!--- This allows UDP traffic for the Serial1/0 !--- interface to be statically mapped to the inside !--  
!  
!  
access-list 1 permit 172.16.0.0 0.0.255.255  
  
!  
!  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

```
<#root>
```

```
VPN-Gateway2#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 986 bytes
```

```
!
```

```
version 12.3
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname VPN-Gateway2
```

```
!
```

```
!--- VPN Gateway1 and VPN Gateway2 can be any devices !--- that perform IPSec. For detailed information
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
clock timezone EST 0
```

```
no aaa new-model
```

```
ip subnet-zero
```

```
!
```

```
!
```

```
ip audit po max-events 100
```

```
no ftp-server write-enable
```

```
!
```

```
!
```

```
!  
!  
!  
  
!--- IKE policies (phase 1).  
  
crypto isakmp policy 10  
  authentication pre-share  
crypto isakmp key cisco123 address 209.165.200.2  
  
!  
!  
  
crypto ipsec transform-set basic esp-des esp-md5-hmac  
no crypto ipsec nat-transparency udp-encaps  
  
!  
  
!--- IPSec policies (phase 1).  
  
crypto map mymap 10 ipsec-isakmp  
  set peer 209.165.200.2  
  set transform-set basic  
  match address 101  
  
!  
!  
!  
interface Ethernet0/0  
  ip address 172.16.1.2 255.255.255.0  
  
crypto map mymap  
  
!  
interface Ethernet1/0  
  ip address 172.16.2.1 255.255.255.0  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.16.1.1  
no ip http server  
no ip http secure-server  
!  
!  
!  
  
access-list 101 permit ip 172.16.2.0 0.0.0.255 192.168.1.0 0.0.0.255  
access-list 101 remark Crypto ACL  
  
!  
!  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

# 验证

以下几部分提供的信息可用于确认您的配置是否工作正常。

[命令输出解释程序工具 \(仅限注册用户\) 支持某些 show 命令](#)，使用此工具可以查看对 show 命令输出的分析。

- [采用 IPsec NAT 透明模式的验证](#)
- [未采用 IPsec NAT 透明模式的验证](#)

## 采用 IPsec NAT 透明模式的验证

- show crypto isakmp sa - 显示对等体上的所有当前 Internet 密钥交换 (IKE) 安全关联 (SA)。

```
<#root>
```

```
VPN-Gateway1#
```

```
show crypto isakmp sa
```

```
dst          src          state         conn-id slot
209.165.200.2 209.165.201.2 QM_IDLE      1      0
```

```
VPN-Gateway2#
```

```
show crypto isakmp sa
```

```
dst          src          state         conn-id slot
209.165.200.2 172.16.1.2   QM_IDLE      1      0
```

- show crypto ipsec sa - 显示对等体之间构建的 IPsec SA。

```
<#root>
```

```
VPN-Gateway1#
```

```
show crypto ipsec sa
```

*!--- This command is issued after a ping !--- is attempted from PC2 to PC1.*

```
interface: Serial1/0
```

```
  Crypto map tag: mymap, local addr. 209.165.200.2
```

```
protected vrf:
```

```
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
```

```
  remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
```

```
  current_peer: 209.165.201.2:4500
```

```
    PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
```

```
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 209.165.200.2, remote crypto endpt.: 209.165.201.2
path mtu 1500, media mtu 1500
current outbound spi: 9CCA0619
```

```
inbound esp sas:
```

```
spi: 0x4E6B990F(1315674383)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel UDP-Encaps, }
slot: 0, conn id: 2000, flow_id: 5, crypto map: mymap
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4602622/3489)
ike_cookies: 8973C578 9C7DEB45 5C9BE6DC 7F737D09
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x9CCA0619(2630485529)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel UDP-Encaps, }
slot: 0, conn id: 2001, flow_id: 6, crypto map: mymap
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4602622/3489)
ike_cookies: 8973C578 9C7DEB45 5C9BE6DC 7F737D09
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
VPN-Gateway2#
```

```
show crypto ipsec sa
```

*!--- This command is issued after a ping !--- is attempted from PC2 to PC1.*

```
interface: Ethernet0/0
```

```
Crypto map tag: mymap, local addr. 172.16.1.2
```

```
protected vrf:
```

```
local ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer: 209.165.200.2:4500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
#pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 16
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 7, #recv errors 0
```

```
local crypto endpt.: 172.16.1.2, remote crypto endpt.: 209.165.200.2
path mtu 1500, media mtu 1500
current outbound spi: 4E6B990F
```

```
inbound esp sas:
```

```
spi: 0x9CCA0619(2630485529)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel UDP-Encaps, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: mymap
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4384024/3481)
ike_cookies: 5C9BE6DC 7F737D09 8973C578 9C7DEB45
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x4E6B990F(1315674383)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel UDP-Encaps, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: mymap
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4384024/3481)
ike_cookies: 5C9BE6DC 7F737D09 8973C578 9C7DEB45
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- show ip nat translations — 显示处于活动状态的 NAT 转换。

```
<#root>
```

```
PAT-Router#
```

```
show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
udp	209.165.201.2:500	172.16.1.2:500	---	---
udp	209.165.201.2:4500	172.16.1.2:4500	---	---

## 未采用 IPsec NAT 透明模式的验证

- show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。

<#root>

VPN-Gateway1#

show crypto isakmp sa

dst	src	state	conn-id	slot
209.165.200.2	209.165.201.2	QM_IDLE	1	0

VPN-Gateway2#

show crypto isakmp sa

dst	src	state	conn-id	slot
209.165.200.2	172.16.1.2	QM_IDLE	1	0

- show crypto ipsec sa - 显示对等体之间构建的 IPsec SA。

<#root>

VPN-Gateway1#

show crypto ipsec sa

*!--- This command is issued after a ping !--- is attempted from PC2 to PC1.*

interface: Serial1/0

Crypto map tag: mymap, local addr. 209.165.200.2

protected vrf:

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)

current\_peer: 209.165.201.2:500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21

#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 4, #recv errors 0

local crypto endpt.: 209.165.200.2, remote crypto endpt.: 209.165.201.2

path mtu 1500, media mtu 1500

current outbound spi: E89A0245

inbound esp sas:

spi: 0xB5F867BC(3052955580)

transform: esp-des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow\_id: 7, crypto map: mymap

crypto engine type: Software, engine\_id: 1

sa timing: remaining key lifetime (k/sec): (4538665/3553)

ike\_cookies: 8973C578 DD91CB42 5C9BE6DC 63813771

IV size: 8 bytes

replay detection support: Y



inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xE89A0245(3902407237)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 8, crypto map: mymap
  crypto engine type: Software, engine_id: 1
  sa timing: remaining key lifetime (k/sec): (4538665/3553)
  ike_cookies: 8973C578 DD91CB42 5C9BE6DC 63813771
  IV size: 8 bytes
  replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

VPN-Gateway2#

**show crypto ipsec sa**

*!--- This command is issued after a ping !--- is attempted from PC2 to PC1.*

interface: Ethernet0/0

Crypto map tag: mymap, local addr. 172.16.1.2

protected vrf:

```
local ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer: 209.165.200.2:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

local crypto endpt.: 172.16.1.2, remote crypto endpt.: 209.165.200.2

path mtu 1500, media mtu 1500

current outbound spi: B5F867BC

inbound esp sas:

```
spi: 0xE89A0245(3902407237)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2000, flow_id: 3, crypto map: mymap
  crypto engine type: Software, engine_id: 1
  sa timing: remaining key lifetime (k/sec): (4572084/3561)
  ike_cookies: 5C9BE6DC 63813771 8973C578 DD91CB42
  IV size: 8 bytes
  replay detection support: Y
```

inbound ah sas:

```

inbound pcp sas:

outbound esp sas:
 spi: 0xB5F867BC(3052955580)
 transform: esp-des esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2001, flow_id: 4, crypto map: mymap
 crypto engine type: Software, engine_id: 1
 sa timing: remaining key lifetime (k/sec): (4572084/3561)
 ike_cookies: 5C9BE6DC 63813771 8973C578 DD91CB42
 IV size: 8 bytes
 replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

- show ip nat translations — 显示处于活动状态的 NAT 转换。

```
<#root>
```

```
PAT-Router#
```

```
show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
udp	209.165.201.2:500	172.16.1.2:500	---	---
esp	209.165.201.2:0	172.16.1.2:0	---	---

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

如果设置包含 PAT 的 LAN-to-LAN IPsec 隧道（如本文档所述）但仍然遇到问题，请收集来自每个设备的 debug output 以及 show 命令的输出，以供 Cisco 技术支持人员进行分析。

以下是与此配置相关的故障排除信息。有关故障排除的其他信息，请参阅[IP安全故障排除-了解和使用debug命令](#)和[验证NAT操作和基本NAT故障排除](#)。

以下几部分显示 debug 命令和输出示例。

- [采用 IPsec NAT 透明模式的故障排除](#)
- [未采用 IPsec NAT 透明模式的故障排除](#)

注意：在发出debug命令之前，请参阅[有关Debug命令的重要信息](#)。

### 采用 IPsec NAT 透明模式的故障排除

- debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。

- debug crypto isakmp - 显示第 1 阶段的 ISAKMP 协商。
- debug ip nat detail — 检查路由器所执行的 NAT。

下面是一个命令输出示例。

```
<#root>
```

```
VPN-Gateway1#
```

```
debug crypto ipsec
```

```
Crypto IPSEC debugging is on
VPN-Gateway1#
```

```
debug crypto isakmp
```

```
Crypto ISAKMP debugging is on
VPN-Gateway1#
```

```
show debug
```

```
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto IPSEC debugging is on
```

*!--- These debugs appeared after a ping !--- was attempted from PC2 to PC1.*

```
*Jun 27 09:31:36.159: ISAKMP (0:0): received packet from 209.165.201.2
                        dport 500 sport 500 Global (N) NEW SA
*Jun 27 09:31:36.159: ISAKMP: Created a peer struct for 209.165.201.2,
                        peer port 500
*Jun 27 09:31:36.159: ISAKMP: Locking peer struct 0x2C50610, IKE refcount
                        1 for crypto_isakmp_process_block
*Jun 27 09:31:36.159: ISAKMP: local port 500, remote port 500
*Jun 27 09:31:36.559: insert sa successfully sa = 290B720
*Jun 27 09:31:36.559: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
                        IKE_MM_EXCH
*Jun 27 09:31:36.559: ISAKMP:(0:1:SW:1):Old State = IKE_READY
                        New State = IKE_R_MM1

*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but
                        major 157 mismatch
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major
                        123 mismatch
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v2
*Jun 27 09:31:36.619: ISAKMP: Looking for a matching key for 209.165.201.2
                        in default : success
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1):found peer pre-shared key matching
                        209.165.201.2
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): local preshared key found
*Jun 27 09:31:36.619: ISAKMP : Scanning profiles for xauth ...
*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 1 against
                        priority 10 policy
*Jun 27 09:31:36.619: ISAKMP:          encryption DES-CBC
```

\*Jun 27 09:31:36.619: ISAKMP: hash SHA  
\*Jun 27 09:31:36.619: ISAKMP: default group 1  
\*Jun 27 09:31:36.619: ISAKMP: auth pre-share  
\*Jun 27 09:31:36.619: ISAKMP: life type in seconds  
\*Jun 27 09:31:36.619: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major  
157 mismatch  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but  
major 123 mismatch  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v2  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE  
\*Jun 27 09:31:36.619: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM1  
New State = IKE\_R\_MM1  
  
\*Jun 27 09:31:36.771: ISAKMP:(0:1:SW:1): constructed NAT-T vendor-03 ID  
\*Jun 27 09:31:36.771: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2  
my\_port 500 peer\_port 500 (R) MM\_SA\_SETUP  
\*Jun 27 09:31:36.771: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE  
\*Jun 27 09:31:36.771: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM1  
New State = IKE\_R\_MM2  
  
\*Jun 27 09:31:37.179: ISAKMP (0:134217729): received packet from  
209.165.201.2 dport 500 sport 500  
Global (R) MM\_SA\_SETUP  
\*Jun 27 09:31:37.179: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH  
\*Jun 27 09:31:37.179: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM2 New State = IKE\_R\_MM3  
  
\*Jun 27 09:31:38.199: ISAKMP:(0:1:SW:1): processing KE payload.  
message ID = 0  
\*Jun 27 09:31:38.199: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = 0  
\*Jun 27 09:31:38.759: ISAKMP: Looking for a matching key for 209.165.201.2  
in default : success  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1):found peer pre-shared key matching  
209.165.201.2  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1):SKEYID state generated  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): vendor ID is Unity  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): vendor ID is DPD  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1): speaking to another IOS box!  
\*Jun 27 09:31:38.759: ISAKMP:received payload type 17  
\*Jun 27 09:31:38.759: ISAKMP:received payload type 17  
\*Jun 27 09:31:38.759: ISAKMP (0:134217729): NAT found, the node outside NAT  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE  
\*Jun 27 09:31:38.759: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM3  
New State = IKE\_R\_MM3  
  
\*Jun 27 09:31:38.891: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2  
my\_port 500 peer\_port 500 (R) MM\_KEY\_EXCH  
\*Jun 27 09:31:38.891: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE  
\*Jun 27 09:31:38.891: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM3  
New State = IKE\_R\_MM4

\*Jun 27 09:31:40.071: ISAKMP (0:134217729): received packet from  
209.165.201.2 dport 4500 sport 4500 Global  
(R) MM\_KEY\_EXCH

\*Jun 27 09:31:40.071: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER,  
IKE\_MM\_EXCH

\*Jun 27 09:31:40.071: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM4  
New State = IKE\_R\_MM5

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0

\*Jun 27 09:31:40.199: ISAKMP (0:134217729): ID payload  
next-payload : 8  
type : 1  
address : 172.16.1.2  
protocol : 17  
port : 0  
length : 12

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1):: peer matches \*none\* of the profiles

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1): processing NOTIFY\_INITIAL\_CONTACT  
protocol 1  
spi 0, message ID = 0, sa = 290B720

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1):SA authentication status:  
authenticated

\*Jun 27 09:31:40.199: ISAKMP:(0:1:SW:1): Process initial contact,  
bring down existing phase 1 and 2 SA's with  
local 209.165.200.2  
remote 209.165.201.2 remote port 4500

\*Jun 27 09:31:40.231: IPSEC(key\_engine): got a queue event with 1 kei messages

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):SA authentication status:  
authenticated

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):SA has been authenticated  
with 209.165.201.2

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):Detected port floating to  
port = 4500

\*Jun 27 09:31:40.399: ISAKMP: Trying to insert a peer  
209.165.200.2/209.165.201.2/4500/  
and inserted successfully.

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):: peer matches \*none\* of the profiles

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE

\*Jun 27 09:31:40.399: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM5  
New State = IKE\_R\_MM5

\*Jun 27 09:31:40.459: ISAKMP:(0:1:SW:1):SA is doing pre-shared key  
authentication using id type ID\_IPV4\_ADDR

\*Jun 27 09:31:40.459: ISAKMP (0:134217729): ID payload  
next-payload : 8  
type : 1  
address : 209.165.200.2  
protocol : 17  
port : 0  
length : 12

\*Jun 27 09:31:40.459: ISAKMP:(0:1:SW:1):Total payload length: 12

\*Jun 27 09:31:40.459: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2  
my\_port 4500 peer\_port 4500 (R) MM\_KEY\_EXCH

\*Jun 27 09:31:40.459: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE

\*Jun 27 09:31:40.459: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM5  
New State = IKE\_P1\_COMPLETE

\*Jun 27 09:31:40.539: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PHASE1\_COMPLETE

\*Jun 27 09:31:40.539: ISAKMP:(0:1:SW:1):Old State = IKE\_P1\_COMPLETE  
New State = IKE\_P1\_COMPLETE

\*Jun 27 09:31:40.999: ISAKMP (0:134217729): received packet from 209.165.201.2  
dport 4500 sport 4500 Global (R) QM\_IDLE

\*Jun 27 09:31:40.999: ISAKMP: set new node 1546295295 to QM\_IDLE

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): processing HASH payload. message  
ID = 1546295295

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): processing SA payload.  
message ID = 1546295295

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1

\*Jun 27 09:31:40.999: ISAKMP: transform 1, ESP\_DES

\*Jun 27 09:31:40.999: ISAKMP: attributes in transform:

\*Jun 27 09:31:40.999: ISAKMP: encaps is 61443 (Tunnel-UDP)

\*Jun 27 09:31:40.999: ISAKMP: SA life type in seconds

\*Jun 27 09:31:40.999: ISAKMP: SA life duration (basic) of 3600

\*Jun 27 09:31:40.999: ISAKMP: SA life type in kilobytes

\*Jun 27 09:31:40.999: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

\*Jun 27 09:31:40.999: ISAKMP: authenticator is HMAC-MD5

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1):atts are acceptable.

\*Jun 27 09:31:40.999: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 209.165.200.2, remote= 209.165.201.2,  
local\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x400

\*Jun 27 09:31:40.999: IPSEC(kei\_proxy): head = mymap, map->ivrf = , kei->ivrf =

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): processing NONCE payload.  
message ID = 1546295295

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1546295295

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1546295295

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1): asking for 1 spis from ipsec

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1):Node 1546295295, Input =  
IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH

\*Jun 27 09:31:40.999: ISAKMP:(0:1:SW:1):Old State = IKE\_QM\_READY  
New State = IKE\_QM\_SPI\_STARVE

\*Jun 27 09:31:41.031: IPSEC(key\_engine): got a queue event with 1 kei messages

\*Jun 27 09:31:41.031: IPSEC(spi\_response): getting spi 1315674383 for SA  
from 209.165.200.2 to 209.165.201.2 for prot 3

\*Jun 27 09:31:41.079: ISAKMP: received ike message (2/1)

\*Jun 27 09:31:42.039: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2  
my\_port 4500 peer\_port 4500 (R) QM\_IDLE

\*Jun 27 09:31:42.039: ISAKMP:(0:1:SW:1):Node 1546295295,  
Input = IKE\_MSG\_FROM\_IPSEC, IKE\_SPI\_REPLY

\*Jun 27 09:31:42.039: ISAKMP:(0:1:SW:1):Old State = IKE\_QM\_SPI\_STARVE  
New State = IKE\_QM\_R\_QM2

\*Jun 27 09:31:42.311: ISAKMP (0:134217729): received packet from 209.165.201.2  
dport 4500 sport 4500 Global (R) QM\_IDLE

\*Jun 27 09:31:42.311: IPsec: Flow\_switching Allocated flow for flow\_id 134217733

\*Jun 27 09:31:42.311: IPsec: Flow\_switching Allocated flow for flow\_id 134217734

\*Jun 27 09:31:43.339: %CRYPTO-5-SESSION\_STATUS: Crypto tunnel is UP .  
Peer 209.165.201.2:4500 Id: 172.16.1.2

\*Jun 27 09:31:43.339: ISAKMP: Locking peer struct 0x2C50610, IPSEC refcount 1  
for for stuff\_ke

\*Jun 27 09:31:43.339: ISAKMP:(0:1:SW:1): Creating IPsec SAs

\*Jun 27 09:31:43.339: inbound SA from 209.165.201.2 to 209.165.200.2  
(f/i) 0/ 0  
(proxy 172.16.2.0 to 192.168.1.0)

\*Jun 27 09:31:43.339: has spi 0x4E6B990F and conn\_id 2000 and flags 400

```

*Jun 27 09:31:43.339:      lifetime of 3600 seconds
*Jun 27 09:31:43.339:      lifetime of 4608000 kilobytes
*Jun 27 09:31:43.339:      has client flags 0x10
*Jun 27 09:31:43.339:      outbound SA from 209.165.200.2 to 209.165.201.2
                          (f/i) 0/0
                          (proxy 192.168.1.0 to 172.16.2.0)
*Jun 27 09:31:43.339:      has spi -1664481767 and conn_id 2001 and flags 408
*Jun 27 09:31:43.339:      lifetime of 3600 seconds
*Jun 27 09:31:43.339:      lifetime of 4608000 kilobytes
*Jun 27 09:31:43.339:      has client flags 0x10
*Jun 27 09:31:43.339: ISAKMP:(0:1:SW:1):deleting node 1546295295 error
                          FALSE reason "quick mode done (await)"
*Jun 27 09:31:43.339: ISAKMP:(0:1:SW:1):Node 1546295295, Input =
                          IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Jun 27 09:31:43.339: ISAKMP:(0:1:SW:1):Old State = IKE_QM_R_QM2
                          New State = IKE_QM_PHASE2_COMPLETE
*Jun 27 09:31:43.359: IPSEC(key_engine): got a queue event with 2 kei messages
*Jun 27 09:31:43.359: IPSEC(initialize_sas): ,
                          (key eng. msg.) INBOUND local= 209.165.200.2, remote= 209.165.201.2,
                          local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
                          remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
                          protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
                          lifedur= 3600s and 4608000kb,
                          spi= 0x4E6B990F(1315674383), conn_id= 134219728, keysize= 0, flags= 0x400
*Jun 27 09:31:43.359: IPSEC(initialize_sas): ,
                          (key eng. msg.) OUTBOUND local= 209.165.200.2, remote= 209.165.201.2,
                          local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
                          remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
                          protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
                          lifedur= 3600s and 4608000kb,
                          spi= 0x9CCA0619(2630485529), conn_id= 134219729, keysize= 0, flags= 0x408
*Jun 27 09:31:43.359: IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
*Jun 27 09:31:43.359: IPSEC(crypto_ipsec_sa_find_ident_head):
                          reconnecting with the same proxies and 209.165.201.2
*Jun 27 09:31:43.359: IPSEC(mtree_add_ident): src 192.168.1.0, dest 172.16.2.0,
                          dest_port 0

*Jun 27 09:31:43.359: IPSEC(create_sa): sa created,
                          (sa) sa_dest= 209.165.200.2, sa_prot= 50,
                          sa_spi= 0x4E6B990F(1315674383),
                          sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219728
*Jun 27 09:31:43.359: IPSEC(create_sa): sa created,
                          (sa) sa_dest= 209.165.201.2, sa_prot= 50,
                          sa_spi= 0x9CCA0619(2630485529),
                          sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219729
*Jun 27 09:32:33.359: ISAKMP:(0:1:SW:1):purging node 1546295295

```

VPN-Gateway2#

debug crypto ipsec

Crypto IPSEC debugging is on

VPN-Gateway2#

debug crypto isakmp

Crypto ISAKMP debugging is on

VPN-Gateway2#

show debug

Cryptographic Subsystem:

Crypto ISAKMP debugging is on

Crypto IPSEC debugging is on

VPN-Gateway2#

*!--- These debugs appeared after a ping !--- was attempted from PC2 to PC1.*

```
*Jun 27 09:31:35.447: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.16.1.2, remote= 209.165.200.2,
  local_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x9CCA0619(2630485529), conn_id= 0, keysize= 0, flags= 0x400A
*Jun 27 09:31:35.455: ISAKMP: received ke message (1/1)
*Jun 27 09:31:35.455: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Jun 27 09:31:35.455: ISAKMP: Created a peer struct for 209.165.200.2,
  peer port 500
*Jun 27 09:31:35.455: ISAKMP: Locking peer struct 0x2C42438, IKE refcount
  1 for isakmp_initiator
*Jun 27 09:31:35.455: ISAKMP: local port 500, remote port 500
*Jun 27 09:31:35.487: ISAKMP: set new node 0 to QM_IDLE
*Jun 27 09:31:35.487: insert sa successfully sa = 2CB1E80
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1):Can not start Aggressive mode,
  trying Main mode.
*Jun 27 09:31:35.487: ISAKMP: Looking for a matching key for 209.165.200.2
  in default : success
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1):found peer pre-shared key matching
  209.165.200.2
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1): constructed NAT-T vendor-03 ID
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1): constructed NAT-T vendor-02 ID
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_IPSEC,
  IKE_SA_REQ_MM
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1):Old State = IKE_READY
  New State = IKE_I_MM1

*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1): beginning Main Mode exchange
*Jun 27 09:31:35.487: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
  my_port 500 peer_port 500 (I) MM_NO_STATE
*Jun 27 09:31:36.607: ISAKMP (0:134217729): received packet from 209.165.200.2
  dport 500 sport 500 Global (I) MM_NO_STATE
*Jun 27 09:31:36.607: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
  IKE_MM_EXCH
*Jun 27 09:31:36.607: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM1
  New State = IKE_I_MM2

*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but
  major 157 mismatch
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3
*Jun 27 09:31:36.687: ISAKMP: Looking for a matching key for 209.165.200.2
  in default : success
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1):found peer pre-shared key
  matching 209.165.200.2
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): local preshared key found
*Jun 27 09:31:36.687: ISAKMP : Scanning profiles for xauth ...
*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 1
  against priority 10 policy
*Jun 27 09:31:36.687: ISAKMP:      encryption DES-CBC
*Jun 27 09:31:36.687: ISAKMP:      hash SHA
*Jun 27 09:31:36.687: ISAKMP:      default group 1
*Jun 27 09:31:36.687: ISAKMP:      auth pre-share
```



\*Jun 27 09:31:36.687: ISAKMP: life type in seconds  
\*Jun 27 09:31:36.687: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but  
major 157 mismatch  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE  
\*Jun 27 09:31:36.687: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM2  
New State = IKE\_I\_MM2  
  
\*Jun 27 09:31:36.795: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2  
my\_port 500 peer\_port 500 (I) MM\_SA\_SETUP  
\*Jun 27 09:31:36.795: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE  
\*Jun 27 09:31:36.795: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM2  
New State = IKE\_I\_MM3  
  
\*Jun 27 09:31:38.727: ISAKMP (0:134217729): received packet from 209.165.200.2  
dport 500 sport 500 Global (I) MM\_SA\_SETUP  
\*Jun 27 09:31:38.727: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER,  
IKE\_MM\_EXCH  
\*Jun 27 09:31:38.727: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM3  
New State = IKE\_I\_MM4  
  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): processing KE payload.  
message ID = 0  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = 0  
\*Jun 27 09:31:38.807: ISAKMP: Looking for a matching key for 209.165.200.2  
in default : success  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1):found peer pre-shared key matching  
209.165.200.2  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1):SKEYID state generated  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): vendor ID is Unity  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): vendor ID is DPD  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): processing vendor id payload  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1): speaking to another IOS box!  
\*Jun 27 09:31:38.807: ISAKMP:received payload type 17  
\*Jun 27 09:31:38.807: ISAKMP (0:134217729): NAT found, the node inside NAT  
\*Jun 27 09:31:38.807: ISAKMP:received payload type 17  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE  
\*Jun 27 09:31:38.807: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM4  
New State = IKE\_I\_MM4  
  
\*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1):Send initial contact  
\*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1):SA is doing pre-shared key  
authentication using id type ID\_IPV4\_ADDR  
\*Jun 27 09:31:38.935: ISAKMP (0:134217729): ID payload  
next-payload : 8  
type : 1  
address : 172.16.1.2  
protocol : 17  
port : 0  
length : 12  
\*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1):Total payload length: 12  
\*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2  
my\_port 4500 peer\_port 4500 (I) MM\_KEY\_EXCH  
\*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,

```
IKE_PROCESS_COMPLETE
*Jun 27 09:31:38.935: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM4
    New State = IKE_I_MM5

*Jun 27 09:31:40.307: ISAKMP (0:134217729): received packet from
    209.165.200.2 dport 4500 sport 4500 Global (I) MM_KEY_EXCH
*Jun 27 09:31:40.307: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
    IKE_MM_EXCH
*Jun 27 09:31:40.307: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM5
    New State = IKE_I_MM6

*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0
*Jun 27 09:31:40.367: ISAKMP (0:134217729): ID payload
    next-payload : 8
    type          : 1
    address       : 209.165.200.2
    protocol      : 17
    port          : 0
    length        : 12
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):SA authentication status:
    authenticated
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):SA has been authenticated with
    209.165.200.2
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):: peer matches *none* of the
    profiles
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):Setting UDP ENC peer struct
    0x2940710 sa= 0x2CB1E80
*Jun 27 09:31:40.367: ISAKMP: Trying to insert a peer
    172.16.1.2/209.165.200.2/4500/, and inserted successfully.
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
    IKE_PROCESS_MAIN_MODE
*Jun 27 09:31:40.367: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM6
    New State = IKE_I_MM6

*Jun 27 09:31:40.367: ISAKMP: sending nat keepalive packet to 209.165.200.2(4500)
*Jun 27 09:31:40.395: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
    IKE_PROCESS_COMPLETE
*Jun 27 09:31:40.395: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM6
    New State = IKE_P1_COMPLETE

*Jun 27 09:31:40.475: ISAKMP:(0:1:SW:1):beginning Quick Mode exchange,
    M-ID of 1546295295
*Jun 27 09:31:40.507: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
    my_port 4500 peer_port 4500 (I) QM_IDLE
*Jun 27 09:31:40.507: ISAKMP:(0:1:SW:1):Node 1546295295, Input = IKE_MESG_INTERNAL,
    IKE_INIT_QM
*Jun 27 09:31:40.507: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY
    New State = IKE_QM_I_QM1
*Jun 27 09:31:40.507: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
    IKE_PHASE1_COMPLETE
*Jun 27 09:31:40.507: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE
    New State = IKE_P1_COMPLETE

*Jun 27 09:31:41.887: ISAKMP (0:134217729): received packet from
    209.165.200.2 dport 4500 sport 4500 Global (I) QM_IDLE
*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1): processing HASH payload.
    message ID = 1546295295
*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1): processing SA payload.
    message ID = 1546295295
*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1):Checking IPSec proposal 1
*Jun 27 09:31:41.887: ISAKMP: transform 1, ESP_DES
```

\*Jun 27 09:31:41.887: ISAKMP: attributes in transform:  
\*Jun 27 09:31:41.887: ISAKMP: encaps is 61443 (Tunnel-UDP)  
\*Jun 27 09:31:41.887: ISAKMP: SA life type in seconds  
\*Jun 27 09:31:41.887: ISAKMP: SA life duration (basic) of 3600  
\*Jun 27 09:31:41.887: ISAKMP: SA life type in kilobytes  
\*Jun 27 09:31:41.887: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0  
\*Jun 27 09:31:41.887: ISAKMP: authenticator is HMAC-MD5  
\*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1):atts are acceptable.  
\*Jun 27 09:31:41.887: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 172.16.1.2, remote= 209.165.200.2,  
local\_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x400  
\*Jun 27 09:31:41.887: IPSEC(kei\_proxy): head = mymap, map->ivrf = , kei->ivrf =  
\*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1): processing NONCE payload.  
message ID = 1546295295  
\*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1546295295  
\*Jun 27 09:31:41.887: ISAKMP:(0:1:SW:1): processing ID payload.  
message ID = 1546295295  
\*Jun 27 09:31:41.887: IPsec: Flow\_switching Allocated flow for flow\_id 134217729  
\*Jun 27 09:31:41.887: IPsec: Flow\_switching Allocated flow for flow\_id 134217730  
\*Jun 27 09:31:41.947: %CRYPTO-5-SESSION\_STATUS: Crypto tunnel is UP .  
Peer 209.165.200.2:4500 Id: 209.165.200.2  
\*Jun 27 09:31:41.947: ISAKMP: Locking peer struct 0x2C42438, IPSEC refcount  
1 for for stuff\_ke  
\*Jun 27 09:31:41.947: ISAKMP:(0:1:SW:1): Creating IPsec SAs  
\*Jun 27 09:31:41.947: inbound SA from 209.165.200.2 to 172.16.1.2  
(f/i) 0/0  
(proxy 192.168.1.0 to 172.16.2.0)  
\*Jun 27 09:31:41.947: has spi 0x9CCA0619 and conn\_id 2000 and flags 400  
\*Jun 27 09:31:41.947: lifetime of 3600 seconds  
\*Jun 27 09:31:41.947: lifetime of 4608000 kilobytes  
\*Jun 27 09:31:41.947: has client flags 0x10  
\*Jun 27 09:31:41.947: outbound SA from 172.16.1.2 to 209.165.200.2  
(f/i) 0/0  
(proxy 172.16.2.0 to 192.168.1.0)  
\*Jun 27 09:31:41.947: has spi 1315674383 and conn\_id 2001 and flags 408  
\*Jun 27 09:31:41.947: lifetime of 3600 seconds  
\*Jun 27 09:31:41.947: lifetime of 4608000 kilobytes  
\*Jun 27 09:31:41.947: has client flags 0x10  
\*Jun 27 09:31:41.947: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2  
my\_port 4500 peer\_port 4500 (I) QM\_IDLE  
\*Jun 27 09:31:41.947: ISAKMP:(0:1:SW:1):deleting node 1546295295 error  
FALSE reason ""  
\*Jun 27 09:31:41.947: ISAKMP:(0:1:SW:1):Node 1546295295, Input =  
IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH  
\*Jun 27 09:31:41.947: ISAKMP:(0:1:SW:1):Old State = IKE\_QM\_I\_QM1  
New State = IKE\_QM\_PHASE2\_COMPLETE  
\*Jun 27 09:31:41.955: IPSEC(key\_engine): got a queue event with 2 kei messages  
\*Jun 27 09:31:41.955: IPSEC(initialize\_sas): ,  
(key eng. msg.) INBOUND local= 172.16.1.2, remote= 209.165.200.2,  
local\_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),  
lifedur= 3600s and 4608000kb,  
spi= 0x9CCA0619(2630485529), conn\_id= 134219728, keysize= 0, flags= 0x400  
\*Jun 27 09:31:41.955: IPSEC(initialize\_sas): ,  
(key eng. msg.) OUTBOUND local= 172.16.1.2, remote= 209.165.200.2,  
local\_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),

```
remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
lifedur= 3600s and 4608000kb,
spi= 0x4E6B990F(1315674383), conn_id= 134219729, keysize= 0, flags= 0x408
*Jun 27 09:31:41.955: IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
*Jun 27 09:31:41.955: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting
with the same proxies and 209.165.200.2
*Jun 27 09:31:41.955: IPSEC(mtree_add_ident): src 172.16.2.0, dest 192.168.1.0,
dest_port 0
```

```
*Jun 27 09:31:41.955: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.1.2, sa_prot= 50,
sa_spi= 0x9CCA0619(2630485529),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219728
*Jun 27 09:31:41.955: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.200.2, sa_prot= 50,
sa_spi= 0x4E6B990F(1315674383),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219729
```

VPN-Gateway2#

```
*Jun 27 09:32:31.979: ISAKMP:(0:1:SW:1):purging node 1546295295
```

PAT-Router#

```
debug ip nat detail
```

```
IP NAT detailed debugging is on
PAT-Router#
```

```
show debug
```

Generic IP:

```
IP NAT detailed debugging is on
PAT-Router#
```

*!--- The "i" in this line indicates the packet is traveling from the !--- inside to the outside (from a*

```
*Jun 27 09:31:35.375: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [66]
```

*!--- The "s" in this next line shows the source address of the packet and how it is !--- being translat*

```
*Jun 27 09:31:35.375: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [66]
*Jun 27 09:31:36.475: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [66]
*Jun 27 09:31:36.475: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [66]
*Jun 27 09:31:36.683: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [67]
*Jun 27 09:31:36.683: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [67]
*Jun 27 09:31:38.595: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [67]
*Jun 27 09:31:38.595: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [67]
*Jun 27 09:31:38.823: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [68]
*Jun 27 09:31:38.823: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [68]
*Jun 27 09:31:40.163: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [68]
*Jun 27 09:31:40.163: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [68]
*Jun 27 09:31:40.255: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [69]
*Jun 27 09:31:40.255: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [69]
*Jun 27 09:31:40.395: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [70]
*Jun 27 09:31:40.395: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [70]
*Jun 27 09:31:41.747: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [69]
*Jun 27 09:31:41.747: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [69]
*Jun 27 09:31:41.839: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [71]
*Jun 27 09:31:41.839: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [71]
*Jun 27 09:31:43.463: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [72]
*Jun 27 09:31:43.463: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [72]
*Jun 27 09:31:43.523: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [70]
```

```

*Jun 27 09:31:43.523: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [70]
*Jun 27 09:33:27.975: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [73]
*Jun 27 09:33:27.975: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [73]
*Jun 27 09:33:28.067: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [71]
*Jun 27 09:33:28.067: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [71]
*Jun 27 09:33:28.115: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [74]
*Jun 27 09:33:28.115: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [74]
*Jun 27 09:33:28.167: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [72]
*Jun 27 09:33:28.167: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [72]
*Jun 27 09:33:28.227: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [75]
*Jun 27 09:33:28.227: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [75]
*Jun 27 09:33:28.283: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [73]
*Jun 27 09:33:28.283: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [73]
*Jun 27 09:33:28.355: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [76]
*Jun 27 09:33:28.355: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [76]
*Jun 27 09:33:28.407: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [74]
*Jun 27 09:33:28.407: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [74]
*Jun 27 09:33:28.455: NAT*: i: udp (172.16.1.2, 4500) -> (209.165.200.2, 4500) [77]
*Jun 27 09:33:28.455: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [77]
*Jun 27 09:33:28.487: NAT*: o: udp (209.165.200.2, 4500) -> (209.165.201.2, 4500) [75]
*Jun 27 09:33:28.487: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [75]

```

## 未采用 IPsec NAT 透明模式的故障排除

- debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。
- debug crypto isakmp - 显示第 1 阶段的 ISAKMP 协商。
- debug ip nat detail — 检查路由器所执行的 NAT。

下面是一个命令输出示例。

```
<#root>
```

```
VPN-Gateway1#
```

```
debug crypto ipsec
```

```
Crypto IPSEC debugging is on
```

```
VPN-Gateway1#
```

```
debug crypto isakmp
```

```
Crypto ISAKMP debugging is on
```

```
VPN-Gateway1#
```

```
show debug
```

```
Cryptographic Subsystem:
```

```
  Crypto ISAKMP debugging is on
```

```
  Crypto IPSEC debugging is on
```

*!--- These debugs appeared after a ping !--- was attempted from PC2 to PC1.*

```

*Jun 27 09:49:58.351: ISAKMP (0:0): received packet from 209.165.201.2
                        dport 500 sport 500 Global (N) NEW SA

```

\*Jun 27 09:49:58.351: ISAKMP: Created a peer struct for 209.165.201.2,  
peer port 500

\*Jun 27 09:49:58.351: ISAKMP: Locking peer struct 0x2C50328, IKE refcount 1  
for crypto\_isakmp\_process\_block

\*Jun 27 09:49:58.351: ISAKMP: local port 500, remote port 500

\*Jun 27 09:49:58.991: insert sa successfully sa = 29D2E80

\*Jun 27 09:49:58.991: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH

\*Jun 27 09:49:58.991: ISAKMP:(0:1:SW:1):Old State = IKE\_READY New State =  
IKE\_R\_MM1

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0

\*Jun 27 09:49:59.151: ISAKMP: Looking for a matching key for 209.165.201.2  
in default : success

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1):found peer pre-shared key matching  
209.165.201.2

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1): local preshared key found

\*Jun 27 09:49:59.151: ISAKMP : Scanning profiles for xauth ...

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 1 against  
priority 10 policy

\*Jun 27 09:49:59.151: ISAKMP: encryption DES-CBC

\*Jun 27 09:49:59.151: ISAKMP: hash SHA

\*Jun 27 09:49:59.151: ISAKMP: default group 1

\*Jun 27 09:49:59.151: ISAKMP: auth pre-share

\*Jun 27 09:49:59.151: ISAKMP: life type in seconds

\*Jun 27 09:49:59.151: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE

\*Jun 27 09:49:59.151: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM1  
New State = IKE\_R\_MM1

\*Jun 27 09:49:59.223: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2  
my\_port 500 peer\_port 500 (R) MM\_SA\_SETUP

\*Jun 27 09:49:59.223: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE

\*Jun 27 09:49:59.223: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM1 New State =  
IKE\_R\_MM2

\*Jun 27 09:49:59.711: ISAKMP (0:134217729): received packet from 209.165.201.2  
dport 500 sport 500 Global (R) MM\_SA\_SETUP

\*Jun 27 09:49:59.711: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_FROM\_PEER,  
IKE\_MM\_EXCH

\*Jun 27 09:49:59.711: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM2  
New State = IKE\_R\_MM3

\*Jun 27 09:49:59.763: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0

\*Jun 27 09:49:59.763: ISAKMP:(0:1:SW:1): processing NONCE payload.  
message ID = 0

\*Jun 27 09:49:59.911: ISAKMP: Looking for a matching key for 209.165.201.2  
in default : success

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1):found peer pre-shared key matching  
209.165.201.2

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1):SKEYID state generated

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): processing vendor id payload

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): vendor ID is Unity

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): processing vendor id payload

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): vendor ID is DPD

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): processing vendor id payload

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1): speaking to another IOS box!

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
IKE\_PROCESS\_MAIN\_MODE

\*Jun 27 09:49:59.911: ISAKMP:(0:1:SW:1):Old State = IKE\_R\_MM3

New State = IKE\_R\_MM3

```
*Jun 27 09:50:00.051: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2
my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Jun 27 09:50:00.051: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 27 09:50:00.051: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM3 New State =
IKE_R_MM4

*Jun 27 09:50:00.743: ISAKMP (0:134217729): received packet from 209.165.201.2
dport 500 sport 500 Global (R) MM_KEY_EXCH
*Jun 27 09:50:00.743: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 27 09:50:00.743: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM4
New State = IKE_R_MM5

*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0
*Jun 27 09:50:00.811: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 172.16.1.2
protocol : 17
port : 500
length : 12
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1): processing NOTIFY_INITIAL_CONTACT
protocol 1
spi 0, message ID = 0, sa = 29D2E80
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local
209.165.200.2 remote
209.165.201.2 remote port 500
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):SA has been authenticated with
209.165.201.2
*Jun 27 09:50:00.811: ISAKMP: Trying to insert a peer
209.165.200.2/209.165.201.2/500/, and inserted successfully.
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 27 09:50:00.811: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM5
New State = IKE_R_MM5

*Jun 27 09:50:00.851: IPSEC(key_engine): got a queue event with 1 kei messages
*Jun 27 09:50:00.963: ISAKMP:(0:1:SW:1):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 27 09:50:00.963: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 209.165.200.2
protocol : 17
port : 500
length : 12
*Jun 27 09:50:00.963: ISAKMP:(0:1:SW:1):Total payload length: 12
*Jun 27 09:50:00.963: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2
my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Jun 27 09:50:00.963: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
```

```

*Jun 27 09:50:00.963: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM5 New State =
IKE_P1_COMPLETE

*Jun 27 09:50:01.043: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Jun 27 09:50:01.043: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

*Jun 27 09:50:01.403: ISAKMP (0:134217729): received packet from 209.165.201.2
dport 500 sport 500 Global (R) QM_IDLE
*Jun 27 09:50:01.403: ISAKMP: set new node 1689610294 to QM_IDLE
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): processing HASH payload. message
ID = 1689610294
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): processing SA payload. message
ID = 1689610294
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1):Checking IPSec proposal 1
*Jun 27 09:50:01.403: ISAKMP: transform 1, ESP_DES
*Jun 27 09:50:01.403: ISAKMP: attributes in transform:
*Jun 27 09:50:01.403: ISAKMP: encaps is 1 (Tunnel)
*Jun 27 09:50:01.403: ISAKMP: SA life type in seconds
*Jun 27 09:50:01.403: ISAKMP: SA life duration (basic) of 3600
*Jun 27 09:50:01.403: ISAKMP: SA life type in kilobytes
*Jun 27 09:50:01.403: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Jun 27 09:50:01.403: ISAKMP: authenticator is HMAC-MD5
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1):atts are acceptable.
*Jun 27 09:50:01.403: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.200.2, remote= 209.165.201.2,
local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Jun 27 09:50:01.403: IPSEC(kei_proxy): head = mymap, map->ivrf = ,
kei->ivrf =
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): processing NONCE payload.
message ID = 1689610294
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): processing ID payload.
message ID = 1689610294
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): processing ID payload.
message ID = 1689610294
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1): asking for 1 spis from ipsec
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1):Node 1689610294, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Jun 27 09:50:01.403: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY
New State = IKE_QM_SPI_STARVE
*Jun 27 09:50:01.443: IPSEC(key_engine): got a queue event with 1 kei messages
*Jun 27 09:50:01.443: IPSEC(spi_response): getting spi 3052955580 for SA
from 209.165.200.2 to 209.165.201.2 for prot 3
*Jun 27 09:50:01.463: ISAKMP: received ke message (2/1)
*Jun 27 09:50:01.971: ISAKMP:(0:1:SW:1): sending packet to 209.165.201.2
my_port 500 peer_port 500 (R) QM_IDLE
*Jun 27 09:50:01.971: ISAKMP:(0:1:SW:1):Node 1689610294, Input =
IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
*Jun 27 09:50:01.971: ISAKMP:(0:1:SW:1):Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
*Jun 27 09:50:02.303: ISAKMP (0:134217729): received packet from 209.165.201.2
dport 500 sport 500 Global (R) QM_IDLE
*Jun 27 09:50:02.303: IPSec: Flow_switching Allocated flow for flow_id
134217735
*Jun 27 09:50:02.303: IPSec: Flow_switching Allocated flow for flow_id 134217736
*Jun 27 09:50:03.203: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP .
Peer 209.165.201.2:500 Id: 172.16.1.2

```



```

*Jun 27 09:50:03.203: ISAKMP: Locking peer struct 0x2C50328, IPSEC refcount
      1 for for stuff_ke
*Jun 27 09:50:03.203: ISAKMP:(0:1:SW:1): Creating IPsec SAs
*Jun 27 09:50:03.203:      inbound SA from 209.165.201.2 to 209.165.200.2
      (f/i) 0/0
      (proxy 172.16.2.0 to 192.168.1.0)
*Jun 27 09:50:03.203:      has spi 0xB5F867BC and conn_id 2000 and flags 2
*Jun 27 09:50:03.203:      lifetime of 3600 seconds
*Jun 27 09:50:03.203:      lifetime of 4608000 kilobytes
*Jun 27 09:50:03.203:      has client flags 0x0
*Jun 27 09:50:03.203:      outbound SA from 209.165.200.2 to 209.165.201.2
      (f/i) 0/0
      (proxy 192.168.1.0 to 172.16.2.0)
*Jun 27 09:50:03.203:      has spi -392560059 and conn_id 2001 and flags A
*Jun 27 09:50:03.203:      lifetime of 3600 seconds
*Jun 27 09:50:03.203:      lifetime of 4608000 kilobytes
*Jun 27 09:50:03.203:      has client flags 0x0
*Jun 27 09:50:03.203: ISAKMP:(0:1:SW:1):deleting node 1689610294 error
      FALSE reason "quick mode done (await)"
*Jun 27 09:50:03.203: ISAKMP:(0:1:SW:1):Node 1689610294, Input =
      IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Jun 27 09:50:03.203: ISAKMP:(0:1:SW:1):Old State = IKE_QM_R_QM2
      New State = IKE_QM_PHASE2_COMPLETE
*Jun 27 09:50:03.231: IPSEC(key_engine): got a queue event with 2 kei messages
*Jun 27 09:50:03.231: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 209.165.200.2, remote= 209.165.201.2,
      local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
      remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
      protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
      lifedur= 3600s and 4608000kb,
      spi= 0xB5F867BC(3052955580), conn_id= 134219728, keysize= 0, flags= 0x2
*Jun 27 09:50:03.231: IPSEC(initialize_sas): ,
      (key eng. msg.) OUTBOUND local= 209.165.200.2, remote= 209.165.201.2,
      local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
      remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
      protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
      lifedur= 3600s and 4608000kb,
      spi= 0xE89A0245(3902407237), conn_id= 134219729, keysize= 0, flags= 0xA
*Jun 27 09:50:03.231: IPSEC(kei_proxy): head = mymap, map->ivrfl = , kei->ivrfl =
*Jun 27 09:50:03.231: IPSEC(crypto_ipsec_sa_find_ident_head):
      reconnecting with the same proxies and 209.165.201.2
*Jun 27 09:50:03.231: IPSEC(mtree_add_ident): src 192.168.1.0,
      dest 172.16.2.0, dest_port 0

*Jun 27 09:50:03.231: IPSEC(create_sa): sa created,
      (sa) sa_dest= 209.165.200.2, sa_prot= 50,
      sa_spi= 0xB5F867BC(3052955580),
      sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219728
*Jun 27 09:50:03.231: IPSEC(create_sa): sa created,
      (sa) sa_dest= 209.165.201.2, sa_prot= 50,
      sa_spi= 0xE89A0245(3902407237),
      sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219729

*Jun 27 09:50:53.231: ISAKMP:(0:1:SW:1):purging node 1689610294

```

VPN-Gateway2#

```
debug crypto ipsec
```

```
Crypto IPSEC debugging is on
VPN-Gateway2#
```

```
debug crypto isakmp
```

Crypto ISAKMP debugging is on  
VPN-Gateway2#

show debug

Cryptographic Subsystem:  
Crypto ISAKMP debugging is on  
Crypto IPSEC debugging is on  
VPN-Gateway2#

*!--- These debugs appeared after a ping !--- was attempted from PC2 to PC1.*

```
*Jun 27 09:49:57.799: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.16.1.2, remote= 209.165.200.2,
  local_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0xE89A0245(3902407237), conn_id= 0, keysize= 0, flags= 0x400A
*Jun 27 09:49:57.807: ISAKMP: received ke message (1/1)
*Jun 27 09:49:57.807: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Jun 27 09:49:57.807: ISAKMP: Created a peer struct for 209.165.200.2,
  peer port 500
*Jun 27 09:49:57.807: ISAKMP: Locking peer struct 0x2BEDC78, IKE refcount
  1 for isakmp_initiator
*Jun 27 09:49:57.807: ISAKMP: local port 500, remote port 500
*Jun 27 09:49:57.839: ISAKMP: set new node 0 to QM_IDLE
*Jun 27 09:49:57.839: insert sa successfully sa = 2CB1E80
*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1):Can not start Aggressive mode,
  trying Main mode.
*Jun 27 09:49:57.839: ISAKMP: Looking for a matching key for 209.165.200.2
  in default : success
*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1):found peer pre-shared key matching
  209.165.200.2
*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_IPSEC,
  IKE_SA_REQ_MM
*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1):Old State = IKE_READY
  New State = IKE_I_MM1

*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1): beginning Main Mode exchange
*Jun 27 09:49:57.839: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
  my_port 500 peer_port 500 (I) MM_NO_STATE
*Jun 27 09:49:59.099: ISAKMP (0:134217729): received packet from 209.165.200.2
  dport 500 sport 500 Global (I) MM_NO_STATE
*Jun 27 09:49:59.099: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Jun 27 09:49:59.099: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM1 New State =
  IKE_I_MM2

*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0
*Jun 27 09:49:59.139: ISAKMP: Looking for a matching key for 209.165.200.2
  in default : success
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1):found peer pre-shared key matching
  209.165.200.2
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1): local preshared key found
*Jun 27 09:49:59.139: ISAKMP : Scanning profiles for xauth ...
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 1 against
  priority 10 policy
*Jun 27 09:49:59.139: ISAKMP:      encryption DES-CBC
*Jun 27 09:49:59.139: ISAKMP:      hash SHA
*Jun 27 09:49:59.139: ISAKMP:      default group 1
*Jun 27 09:49:59.139: ISAKMP:      auth pre-share
```

```

*Jun 27 09:49:59.139: ISAKMP:      life type in seconds
*Jun 27 09:49:59.139: ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
*Jun 27 09:49:59.139: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM2  New State =
      IKE_I_MM2

*Jun 27 09:49:59.259: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
      my_port 500 peer_port 500 (I) MM_SA_SETUP
*Jun 27 09:49:59.259: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_COMPLETE
*Jun 27 09:49:59.259: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM2  New State =
      IKE_I_MM3

*Jun 27 09:49:59.919: ISAKMP (0:134217729): received packet from 209.165.200.2
      dport 500 sport 500 Global (I) MM_SA_SETUP
*Jun 27 09:49:59.919: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 27 09:49:59.919: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM3
      New State = IKE_I_MM4

*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = 0
*Jun 27 09:49:59.947: ISAKMP: Looking for a matching key for 209.165.200.2
      in default : success
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1):found peer pre-shared key matching
      209.165.200.2
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1):SKEYID state generated
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): vendor ID is Unity
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): vendor ID is DPD
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): processing vendor id payload
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1): speaking to another IOS box!
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
*Jun 27 09:49:59.947: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM4
      New State = IKE_I_MM4

*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1):Send initial contact
*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1):SA is doing pre-shared key
      authentication using id type ID_IPV4_ADDR
*Jun 27 09:50:00.059: ISAKMP (0:134217729): ID payload
      next-payload : 8
      type          : 1
      address       : 172.16.1.2
      protocol      : 17
      port          : 500
      length        : 12
*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1):Total payload length: 12
*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
      my_port 500 peer_port 500 (I) MM_KEY_EXCH
*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_COMPLETE
*Jun 27 09:50:00.059: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM4
      New State = IKE_I_MM5

*Jun 27 09:50:00.827: ISAKMP (0:134217729): received packet from 209.165.200.2
      dport 500 sport 500 Global (I) MM_KEY_EXCH
*Jun 27 09:50:00.827: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 27 09:50:00.827: ISAKMP:(0:1:SW:1):Old State = IKE_I_MM5
      New State = IKE_I_MM6

```

\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0  
\*Jun 27 09:50:00.859: ISAKMP (0:134217729): ID payload  
    next-payload : 8  
    type : 1  
    address : 209.165.200.2  
    protocol : 17  
    port : 500  
    length : 12  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1):SA authentication status:  
    authenticated  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1):SA has been authenticated  
    with 209.165.200.2  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1):: peer matches \*none\* of the profiles  
\*Jun 27 09:50:00.859: ISAKMP: Trying to insert a peer 172.16.1.2/209.165.200.2/500/,  
    and inserted successfully.  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
    IKE\_PROCESS\_MAIN\_MODE  
\*Jun 27 09:50:00.859: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM6  
    New State = IKE\_I\_MM6  
  
\*Jun 27 09:50:00.919: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
    IKE\_PROCESS\_COMPLETE  
\*Jun 27 09:50:00.919: ISAKMP:(0:1:SW:1):Old State = IKE\_I\_MM6  
    New State = IKE\_P1\_COMPLETE  
  
\*Jun 27 09:50:00.959: ISAKMP:(0:1:SW:1):beginning Quick Mode exchange,  
    M-ID of 1689610294  
\*Jun 27 09:50:01.007: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2  
    my\_port 500 peer\_port 500 (I) QM\_IDLE  
\*Jun 27 09:50:01.007: ISAKMP:(0:1:SW:1):Node 1689610294, Input =  
    IKE\_MESG\_INTERNAL, IKE\_INIT\_QM  
\*Jun 27 09:50:01.007: ISAKMP:(0:1:SW:1):Old State = IKE\_QM\_READY  
    New State = IKE\_QM\_I\_QM1  
\*Jun 27 09:50:01.007: ISAKMP:(0:1:SW:1):Input = IKE\_MESG\_INTERNAL,  
    IKE\_PHASE1\_COMPLETE  
\*Jun 27 09:50:01.007: ISAKMP:(0:1:SW:1):Old State = IKE\_P1\_COMPLETE  
    New State = IKE\_P1\_COMPLETE  
  
\*Jun 27 09:50:01.839: ISAKMP (0:134217729): received packet from  
    209.165.200.2 dport 500 sport 500 Global (I) QM\_IDLE  
\*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1): processing HASH payload.  
    message ID = 1689610294  
\*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1): processing SA payload.  
    message ID = 1689610294  
\*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1  
\*Jun 27 09:50:01.839: ISAKMP: transform 1, ESP\_DES  
\*Jun 27 09:50:01.839: ISAKMP: attributes in transform:  
\*Jun 27 09:50:01.839: ISAKMP: encaps is 1 (Tunnel)  
\*Jun 27 09:50:01.839: ISAKMP: SA life type in seconds  
\*Jun 27 09:50:01.839: ISAKMP: SA life duration (basic) of 3600  
\*Jun 27 09:50:01.839: ISAKMP: SA life type in kilobytes  
\*Jun 27 09:50:01.839: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0  
\*Jun 27 09:50:01.839: ISAKMP: authenticator is HMAC-MD5  
\*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1):atts are acceptable.  
\*Jun 27 09:50:01.839: IPSEC(validate\_proposal\_request): proposal part #1,  
    (key eng. msg.) INBOUND local= 172.16.1.2, remote= 209.165.200.2,  
    local\_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),  
    remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),  
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),  
    lifedur= 0s and 0kb,

```
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Jun 27 09:50:01.839: IPSEC(kei_proxy): head = mymap, map->ivrf = ,
    kei->ivrf =
*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1): processing NONCE payload.
    message ID = 1689610294
*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1): processing ID payload.
    message ID = 1689610294
*Jun 27 09:50:01.839: ISAKMP:(0:1:SW:1): processing ID payload.
    message ID = 1689610294
*Jun 27 09:50:01.839: IPSec: Flow_switching Allocated flow for flow_id 134217731
*Jun 27 09:50:01.839: IPSec: Flow_switching Allocated flow for flow_id 134217732
*Jun 27 09:50:01.899: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP .
    Peer 209.165.200.2:500      Id: 209.165.200.2
*Jun 27 09:50:01.899: ISAKMP: Locking peer struct 0x2BEDC78, IPSEC
    refcount 1 for for stuff_ke
*Jun 27 09:50:01.899: ISAKMP:(0:1:SW:1): Creating IPSec SAs
*Jun 27 09:50:01.899:      inbound SA from 209.165.200.2 to 172.16.1.2
    (f/i) 0/0
    (proxy 192.168.1.0 to 172.16.2.0)
*Jun 27 09:50:01.899:      has spi 0xE89A0245 and conn_id 2000 and flags 2
*Jun 27 09:50:01.899:      lifetime of 3600 seconds
*Jun 27 09:50:01.899:      lifetime of 4608000 kilobytes
*Jun 27 09:50:01.899:      has client flags 0x0
*Jun 27 09:50:01.899:      outbound SA from 172.16.1.2 to 209.165.200.2
    (f/i) 0/0
    (proxy 172.16.2.0 to 192.168.1.0)
*Jun 27 09:50:01.899:      has spi -1242011716 and conn_id 2001 and flags A
*Jun 27 09:50:01.899:      lifetime of 3600 seconds
*Jun 27 09:50:01.899:      lifetime of 4608000 kilobytes
*Jun 27 09:50:01.899:      has client flags 0x0
*Jun 27 09:50:01.899: ISAKMP:(0:1:SW:1): sending packet to 209.165.200.2
    my_port 500 peer_port 500 (I) QM_IDLE
*Jun 27 09:50:01.899: ISAKMP:(0:1:SW:1):deleting node 1689610294 error
    FALSE reason ""
*Jun 27 09:50:01.899: ISAKMP:(0:1:SW:1):Node 1689610294, Input =
    IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Jun 27 09:50:01.899: ISAKMP:(0:1:SW:1):Old State = IKE_QM_I_QM1
    New State = IKE_QM_PHASE2_COMPLETE
*Jun 27 09:50:01.907: IPSEC(key_engine): got a queue event with 2 kei messages
*Jun 27 09:50:01.907: IPSEC(initialize_sas): ,
    (key eng. msg.) INBOUND local= 172.16.1.2, remote= 209.165.200.2,
    local_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0xE89A0245(3902407237), conn_id= 134219728, keysize= 0, flags= 0x2
*Jun 27 09:50:01.907: IPSEC(initialize_sas): ,
    (key eng. msg.) OUTBOUND local= 172.16.1.2, remote= 209.165.200.2,
    local_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0xB5F867BC(3052955580), conn_id= 134219729, keysize= 0, flags= 0xA
*Jun 27 09:50:01.907: IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
*Jun 27 09:50:01.907: IPSEC(crypto_ipsec_sa_find_ident_head):
    reconnecting with the same proxies and 209.165.200.2
*Jun 27 09:50:01.907: IPSEC(mtree_add_ident): src 172.16.2.0, dest
    192.168.1.0, dest_port 0
*Jun 27 09:50:01.907: IPSEC(create_sa): sa created,
    (sa) sa_dest= 172.16.1.2, sa_prot= 50,
    sa_spi= 0xE89A0245(3902407237),
```

```
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219728
*Jun 27 09:50:01.907: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.200.2, sa_prot= 50,
sa_spi= 0xB5F867BC(3052955580),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 134219729

*Jun 27 09:50:51.927: ISAKMP:(0:1:SW:1):purging node 1689610294
```

PAT-Router#

```
debug ip nat detail
```

```
IP NAT detailed debugging is on
PAT-Router#
```

```
show debug
```

Generic IP:

```
IP NAT detailed debugging is on
PAT-Router#
```

*!--- The "i" in this line indicates the packet is traveling from the !--- inside to the outside (from a*

```
*Jun 27 09:49:57.727: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [94]
```

*!--- The "s" in this line shows the source address of the packet and how it is !--- being translated.*

```
*Jun 27 09:49:57.727: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [94]
*Jun 27 09:49:58.927: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [100]
*Jun 27 09:49:58.927: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [100]
*Jun 27 09:49:59.147: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [95]
*Jun 27 09:49:59.147: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [95]
*Jun 27 09:49:59.755: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [101]
*Jun 27 09:49:59.755: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [101]
*Jun 27 09:49:59.947: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [96]
*Jun 27 09:49:59.947: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [96]
*Jun 27 09:50:00.667: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [102]
*Jun 27 09:50:00.667: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [102]
*Jun 27 09:50:00.895: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [97]
*Jun 27 09:50:00.895: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [97]
*Jun 27 09:50:01.679: NAT*: o: udp (209.165.200.2, 500) -> (209.165.201.2, 500) [103]
*Jun 27 09:50:01.679: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [103]
*Jun 27 09:50:01.787: NAT*: i: udp (172.16.1.2, 500) -> (209.165.200.2, 500) [98]
*Jun 27 09:50:01.787: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [98]
*Jun 27 09:50:23.667: NAT*: i: esp (172.16.1.2, 26556) -> (209.165.200.2, 0) [99]
*Jun 27 09:50:23.667: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [99]
*Jun 27 09:50:23.715: NAT*: o: esp (209.165.200.2, -392560059) -> (209.165.201.2, 0) [104]
*Jun 27 09:50:23.715: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [104]
*Jun 27 09:50:23.787: NAT*: i: esp (172.16.1.2, 26556) -> (209.165.200.2, 0) [100]
*Jun 27 09:50:23.787: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [100]
*Jun 27 09:50:23.847: NAT*: o: esp (209.165.200.2, 581) -> (209.165.201.2, 0) [105]
*Jun 27 09:50:23.847: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [105]
*Jun 27 09:50:23.915: NAT*: i: esp (172.16.1.2, 26556) -> (209.165.200.2, 0) [101]
*Jun 27 09:50:23.915: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [101]
*Jun 27 09:50:23.967: NAT*: o: esp (209.165.200.2, 581) -> (209.165.201.2, 0) [106]
*Jun 27 09:50:23.967: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [106]
*Jun 27 09:50:24.047: NAT*: i: esp (172.16.1.2, 26556) -> (209.165.200.2, 0) [102]
*Jun 27 09:50:24.047: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [102]
*Jun 27 09:50:24.095: NAT*: o: esp (209.165.200.2, 581) -> (209.165.201.2, 0) [107]
*Jun 27 09:50:24.095: NAT*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [107]
*Jun 27 09:50:24.207: NAT*: i: esp (172.16.1.2, 26556) -> (209.165.200.2, 0) [103]
*Jun 27 09:50:24.207: NAT*: s=172.16.1.2->209.165.201.2, d=209.165.200.2 [103]
```

\*Jun 27 09:50:24.267: NAT\*: o: esp (209.165.200.2, 581) -> (209.165.201.2, 0) [108]  
\*Jun 27 09:50:24.267: NAT\*: s=209.165.200.2, d=209.165.201.2->172.16.1.2 [108]

## 相关信息

- [IPSec 支持页面](#)
- [技术支持 - Cisco Systems](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。