

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[IPSec NAT 透過を伴う場合の設定](#)

[IPSec NAT 透過を伴わない場合の設定](#)

[確認](#)

[IPSec NAT 透過を伴う場合の確認](#)

[IPSec NAT 透過を伴わない場合の確認](#)

[トラブルシューティング](#)

[IPSec NAT 透過を伴う場合のトラブルシューティング](#)

[IPSec NAT 透過を伴わない場合のトラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、LAN-to-LAN IPSec トンネルの確立が許可されるように Port Address Translation ( PAT ) を設定するサンプルが紹介されています。ここでは、パブリック IP アドレス ( すべてのトラフィック上で PAT を実行するために Cisco IOS® ルータで使用 ) を 1 つだけ使用し、VPN コンセントレータを使用せずに IPSec トンネルを通過するというシナリオを使用します。

12.2(13)T よりも前の Cisco IOS ソフトウェア リリースが稼働する VPN ゲートウェイでは、カプセル化セキュリティ ペイロード ( ESP ) スルーを許可するには、PAT を実行するルータで IPSec パススルー機能が必要です。

注この機能は [ソフトウェア アドバイザリー \( 登録ユーザのみ \)](#) のネットワーク アドレス変換 ( NAT ) サポートによる IPSec として知られています。

ローカル ( PAT 適用対象 ) ピアからトンネルを起動するには、設定は必要ありません。リモートピアからトンネルを起動するには、次のコマンドが必要です。

- `ip nat inside source static esp inside_ip interface interface`
- `ip nat inside` ソース スタティック UDP ( ユーザ・ データグラム・ プロトコル ) `inside_ip 500`  
インターフェイス インターフェイス 500

12.2(13)T 以降の Cisco IOS ソフトウェア リリースが稼働する VPN ゲートウェイでは、IPSec トラフィックは User Data Protocol ( UDP ) ポート 4500 のパケットにカプセル化されます。この機能は [IPSec NAT 透過](#) と呼ばれるものです。ローカル ( PAT 適用対象 ) ピアからトンネルを起動するには、設定は必要ありません。

リモートピアからトンネルを起動するには、次のコマンドが必要です。

- ip nat inside source static udp inside\_ip 4500 interface interface 4500
- ip nat inside ソース スタティック UDP ( ユーザ・ データグラム・ プロトコル ) inside\_ip 500  
インターフェイス インターフェイス 500

[IPSec NAT 透過を無効にするには、no crypto ipsec nat-transparency udp-encaps コマンドを発行します。](#)

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco IOS ソフトウェア リリース 12.3(7)T1 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### 表記法

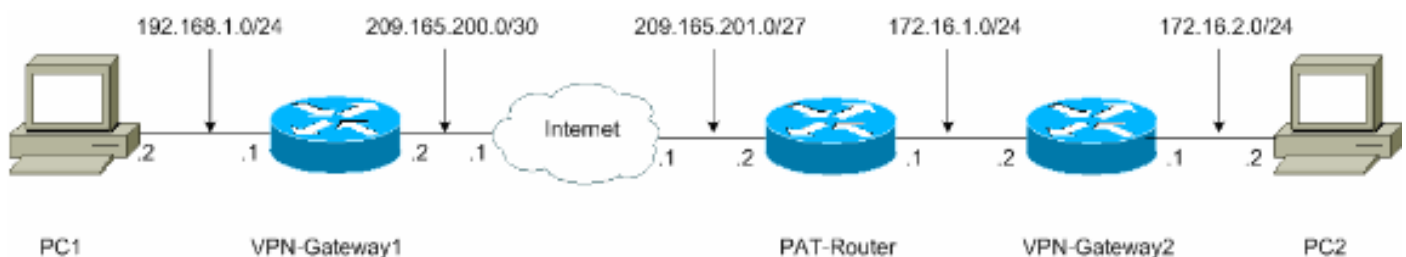
ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

### ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



### IPSec NAT 透過を伴う場合の設定

このドキュメントでは、次の設定を使用します。

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

## VPN-Gateway1

```
VPN-Gateway1#show running-config Building
configuration...Current configuration : 1017
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname VPN-Gateway1!!--- VPN
Gateway1 and VPN Gateway2 can be any devices that !---
perform IPSec. For detailed information on configuring
IPSec !--- refer to IPSec Technology Support
Information. !--- IPSec configuration between VPN
Gateway1 and VPN Gateway2 !--- is beyond the scope of
this document.boot-start-markerboot-end-marker!!clock
timezone EST 0no aaa new-modelip subnet-zero!!ip audit
po max-events 100no ftp-server write-enable!!! ! !!---
IKE policies (phase 1).crypto isakmp policy 10
authentication pre-sharecrypto 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 classlessip route 0.0.0.0 0.0.0.0
209.165.200.1no ip http serverno ip http secure-
server!!!access-list 101 permit ip 192.168.1.0 0.0.0.255
172.16.2.0 0.0.0.255access-list 101 remark Crypto
ACL!!!control-plane!!line con 0line aux 0line vty 0
4!!end
```

## PAT-Router

```
PAT-Router#show running-config Building
configuration...Current configuration : 971
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname PAT-Router!boot-start-
markerboot-end-marker!!clock timezone EST 0no aaa new-
modelip subnet-zero!!ip audit po max-events 100no 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
outsideserial restart-delay 0!ip classlessip route
0.0.0.0 0.0.0.0 209.165.201.1ip route 172.16.0.0
255.255.0.0 172.16.1.2no ip http serverno 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 address
172.16.1.2.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 address 172.16.1.2. !--- This is
required for the Internet Security Association !--- and
Key Management Protocol (ISAKMP) negotiation to be !---
initiated from VPN-Gateway1 to VPN-Gateway2.!!access-
list 1 permit 172.16.0.0 0.0.255.255!!!control-
plane!!line con 0line aux 0line vty 0 4!!end
```

## VPN-Gateway2

```
VPN-Gateway2#show running-config Building
configuration...Current configuration : 986
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname VPN-Gateway2!!--- VPN
Gateway1 and VPN Gateway2 can be any devices !--- that
perform IPSec. For detailed information on !--- IPSec
configuration refer to IPSec Technology Support
Information. !--- IPSec configuration between VPN
Gateway1 and VPN Gateway2 !--- is beyond the scope of
this document. boot-start-markerboot-end-marker!!clock
timezone EST 0no aaa new-modelip subnet-zero!!ip audit
po max-events 100no ftp-server write-enable!!! ! !---
IKE policies (phase 1).crypto isakmp policy 10
authentication pre-sharecrypto 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 classlessip
route 0.0.0.0 0.0.0.0 172.16.1.1no ip http serverno ip
http secure-server!!!access-list 101 permit ip
172.16.2.0 0.0.0.255 192.168.1.0 0.0.0.255access-list
101 remark Crypto ACL!!!control-plane!!line con 0line
aux 0line vty 0 4!!end
```

## IPSec NAT 透過を伴わない場合の設定

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

## VPN-Gateway1

```
VPN-Gateway1#show running-config Building
configuration...Current configuration : 1017
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname VPN-Gateway1!!--- VPN
Gateway1 and VPN Gateway2 can be any devices !--- that
perform IPSec. For detailed information on !--- IPSec
configuration refer to IPSec Technology Support
Information. !--- IPSec configuration between VPN
Gateway1 and VPN Gateway2 !--- is beyond the scope of
this document. boot-start-markerboot-end-marker!!clock
timezone EST 0no aaa new-modelip subnet-zero!!ip audit
po max-events 100no ftp-server write-enable!!! ! !---
IKE policies (phase 1).crypto isakmp policy 10
authentication pre-sharecrypto 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 classlessip route 0.0.0.0 0.0.0.0
```

```
209.165.200.1no ip http serverno ip http secure-
server!!!access-list 101 permit ip 192.168.1.0 0.0.0.255
172.16.2.0 0.0.0.255access-list 101 remark Crypto
ACL!!!control-plane!!line con 0line aux 0line vty 0
4!!end
```

## PAT-Router

```
PAT-Router#show running-config Building
configuration...Current configuration : 971
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname PAT-Router!boot-start-
markerboot-end-marker!!clock timezone EST 0no aaa new-
modelip subnet-zero!!ip audit po max-events 100no 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 classlessip route
0.0.0.0 0.0.0.0 209.165.201.1ip route 172.16.0.0
255.255.0.0 172.16.1.2no ip http serverno 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 !--- to the inside IP address
172.16.1.2. The "esp" !--- option allows a single ESP
tunnel-mode !--- VPN setup to be possible.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
address 172.16.1.2. This is required !--- for the ISAKMP
negotiation to be initiated !--- from VPN-Gateway1 to
VPN-Gateway2.!!access-list 1 permit 172.16.0.0
0.0.255.255!!!control-plane!!line con 0line aux 0line
vtty 0 4!!end
```

## VPN-Gateway2

```
VPN-Gateway2#show running-configBuilding
configuration...Current configuration : 986
bytes!version 12.3service timestamps debug datetime
msecservice timestamps log datetime msecno service
password-encryption!hostname VPN-Gateway2!--- VPN
Gateway1 and VPN Gateway2 can be any devices !--- that
perform IPSec. For detailed information on !--- IPSec
configuration refer to IPSec Technology Support
Information. !--- IPSec configuration between VPN
Gateway1 and VPN Gateway2 !--- is beyond the scope of
this document. boot-start-markerboot-end-marker!!clock
timezone EST 0no aaa new-modelip subnet-zero!!ip audit
po max-events 100no ftp-server write-enable!!! ! !!---
IKE policies (phase 1).crypto isakmp policy 10
authentication pre-sharecrypto isakmp key cisco123
address 209.165.200.2!!crypto ipsec transform-set basic
esp-des esp-md5-hmacno 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 classlessip route 0.0.0.0
0.0.0.0 172.16.1.1no ip http serverno ip http secure-
server!!!access-list 101 permit ip 172.16.2.0 0.0.0.255
192.168.1.0 0.0.0.255access-list 101 remark Crypto
ACL!!!control-plane!!line con 0line aux 0line vty 0
4!!end
```

## 確認

このセクションでは、設定が正しく動作していることを確認するための情報を提供しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- [IPSec NAT 透過を伴う場合の確認](#)
- [IPSec NAT 透過を伴わない場合の確認](#)

## IPSec NAT 透過を伴う場合の確認

- **show crypto isakmp sa** か。ピアですべての現在のインターネット キー エクスチェンジ ( IKE ) Security Associations ( SA ) を表示する。VPN-Gateway1#**show crypto isakmp sadst**  
src state conn-id slot209.165.200.2 209.165.201.2 QM\_IDLE  
1 0VPN-Gateway2#**show crypto isakmp sadst** src state conn-  
id slot209.165.200.2 172.16.1.2 QM\_IDLE 1 0
- **show crypto ipsec sa** か。ピア間で確立されたIPSec SA を表示する。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** か。アクティブ な NAT変換を表示する。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	---	---	---		

## IPSec NAT 透過を伴わない場合の確認

- **show crypto isakmp sa** か。ピアですべての電流 IKE SA を表示する。VPN-Gateway1#**show crypto isakmp sadst**

src	state	conn-id	slot	209.165.200.2		
209.165.201.2	QM_IDLE	1	0	VPN-Gateway2# <b>show crypto isakmp sadst</b>		
src	state	conn-id	slot	209.165.200.2	172.16.1.2	QM_IDLE
1	0					
- **show crypto ipsec sa** か。ピア間で確立されたIPSec SA を表示する。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 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: 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** か。アクティブ な NAT変換を表示する。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	---	---	---		

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

PAT を取り込んだ LAN-to-LAN IPsec トンネルをこのドキュメントの説明どおりに設定しても問題が起こる場合は、Cisco テクニカル サポート による分析用に、各デバイスの **debug** 出力と **show** コマンドの出力を収集してください。

この設定に関連するトラブルシューティング情報を次に示します。トラブルシューティングのその他の情報に関しては、[IP Security Troubleshooting - Understanding and Using debug Commands](#) および [NAT の動作確認と NAT の基本的なトラブルシューティング](#)を参照して下さい。

**debug** コマンドとサンプル出力が、このセクションで示されています。

- [IPsec NAT 透過を伴う場合のトラブルシューティング](#)
- [IPsec NAT 透過を伴わない場合のトラブルシューティング](#)

注 コマンドを使用する前に、[『debug コマンドの重要な情報』](#)を参照してください。

## [IPsec NAT 透過を伴う場合のトラブルシューティング](#)

- **debug crypto ipsec** が、フェーズ2 の IPsec ネゴシエーションを表示する。
- **debug crypto isakmp** が、フェーズ1 の ISAKMP ネゴシエーションを表示する。
- **debug ip nat detail** が、ルータによって実行された NAT を検査します。

次に、サンプルのコマンド出力を示します。

```
VPN-Gateway1#debug crypto ipsecCrypto IPSEC debugging is onVPN-Gateway1#debug crypto isakmpCrypto ISAKMP debugging is onVPN-Gateway1#show debugCryptographic 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_MSG_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_MSG_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MESG\_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\_MESG\_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\_MESG\_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 onVPN-Gateway2#**debug crypto isakmp**Crypto ISAKMP debugging is onVPN-  
Gateway2#**show debug**Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto IPSEC  
debugging is onVPN-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\_MESG\_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= 134219729VPN-Gateway2#\*Jun 27 09:32:31.979: ISAKMP:(0:1:SW:1):purging node 1546295295PAT-Router#debug ip nat detailIP NAT detailed debugging is onPAT-Router#show debugGeneric IP: IP NAT detailed debugging is onPAT-Router#!--- The "i" in this line indicates the packet is traveling from the !--- inside to the outside (from a NAT perspective) interface. The number in !--- the brackets is the identification number in the IP packet. This is !--- useful when correlating information with sniffer traces taken with a !--- network analyzer while troubleshooting problems.\*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 translated. \*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]

```

## IPSec NAT 透過を伴わない場合のトラブルシューティング

- `debug crypto ipsec` が。フェーズ2 の IPSec ネゴシエーションを表示する。
- `debug crypto isakmp` が。フェーズ1 の ISAKMP ネゴシエーションを表示する。
- `debug ip nat detail` が。ルータによって実行された NAT を検査します。

次に、サンプルのコマンド出力を示します。

```

VPN-Gateway1#debug crypto ipsecCrypto IPSEC debugging is onVPN-Gateway1#debug crypto
isakmpCrypto ISAKMP debugging is onVPN-Gateway1#show debugCryptographic 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_MSG_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\_MESG\_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->ivrf = , kei->ivrf = \*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 1689610294VPN-Gateway2#**debug crypto ipsec**Crypto IPSEC debugging is onVPN-Gateway2#**debug crypto isakmp**Crypto ISAKMP debugging is onVPN-Gateway2#**show debug**Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto IPSEC debugging is onVPN-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\_MESG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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 1689610294PAT-Router#**debug ip nat detail**IP NAT detailed debugging is onPAT-Router#**show debug**Generic IP: IP NAT detailed debugging is onPAT-Router#*!--- The "i" in this line indicates the packet is traveling from the !--- inside to the outside (from a NAT perspective) interface. The number in !--- the brackets is the identification number in the IP packet. This is !--- useful when correlating information with sniffer traces taken with a !--- network analyzer while troubleshooting problems.*\*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]

## [関連情報](#)

- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)