

# Configurar túneis de site para site do IPsec IKEv1 com o ASDM ou o CLI no ASA

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar através do wizard VPN ASDM](#)

[Configurar através do CLI](#)

[Configurar o local B para as versões ASA 8.4 e mais atrasado](#)

[Configurar o local A para as versões ASA 8.2 e mais adiantado](#)

[Agrupe a política](#)

[Verificar](#)

[ASDM](#)

[CLI](#)

[Fase 1](#)

[Fase 2](#)

[Troubleshooting](#)

[Versões ASA 8.4 e mais atrasado](#)

[Versões ASA 8.3 e mais adiantado](#)

## Introdução

Este documento descreve como configurar um túnel de site para site do IPsec da versão 1 do intercâmbio de chave de Internet (IKEv1) entre uma ferramenta de segurança adaptável do Cisco 5515-X Series (ASA) essa versão de software 9.2.x das corridas e um Cisco 5510 Series ASA que executa a versão de software 8.2.x.

## Pré-requisitos

### Requisitos

Cisco recomenda que estas exigências estejam cumpridas antes que você tente a configuração que está descrita neste documento:

- A conectividade IP fim-a-fim deve ser estabelecida.
- Estes protocolos devem ser permitidos:

User Datagram Protocol (UDP) 500 e 4500 para o plano do controle do IPsec

50 pés do protocolo IP do Encapsulating Security Payload (ESP) para o plano dos dados do IPsec

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5510 Series ASA que executa a versão de software 8.2
- Cisco 5515-X ASA que executa a versão de software 9.2

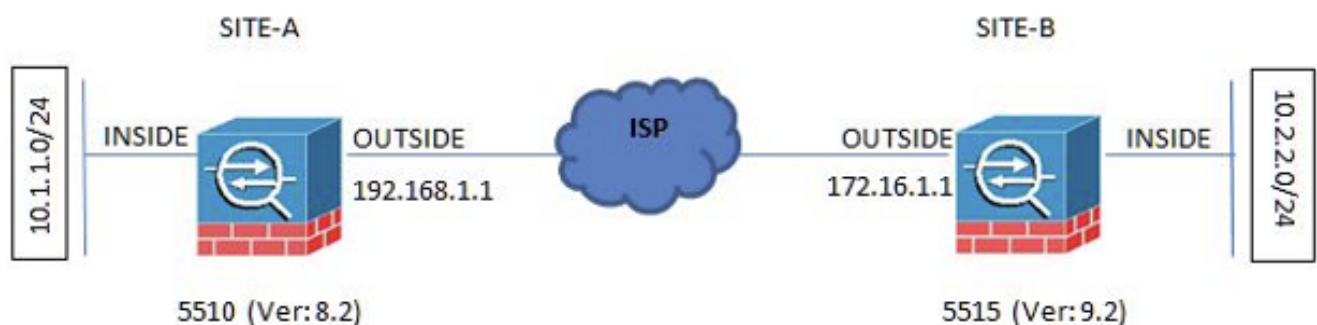
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Esta seção descreve como configurar o túnel do VPN de Site-para-Site através do wizard VPN adaptável do Security Device Manager (ASDM) ou através do CLI.

## Diagrama de Rede

Esta é a topologia que é usada para os exemplos durante todo este documento:

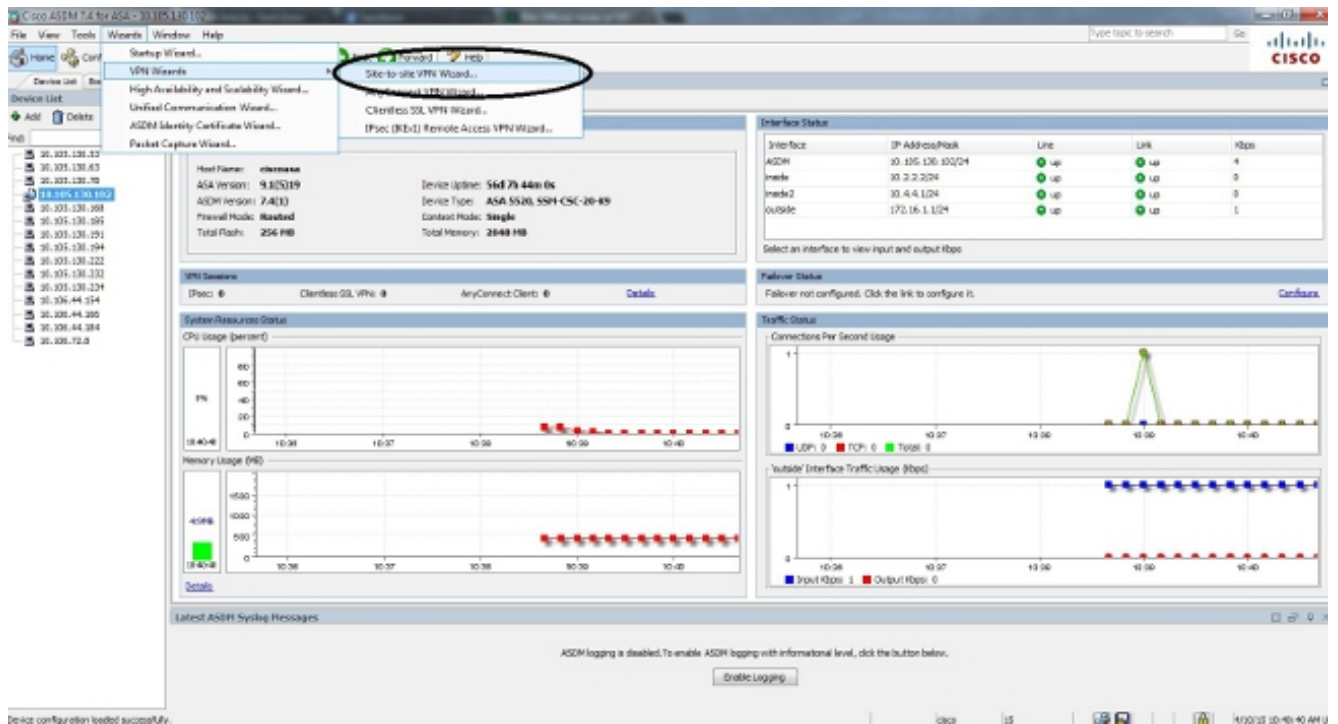


## Configurar através do wizard VPN ASDM

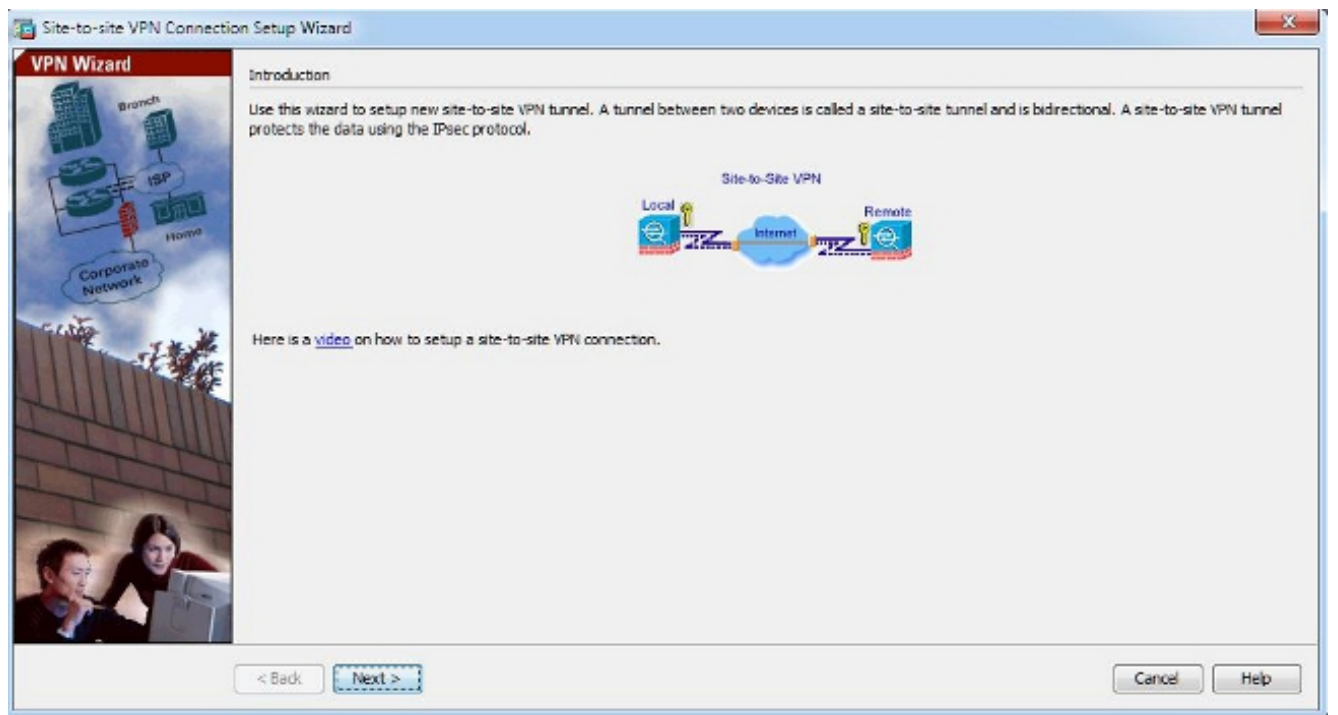
Termine estas etapas a fim estabelecer o túnel do VPN de Site-para-Site através do assistente ASDM:

1. Abra o ASDM e navegue aos **assistentes > aos wizard VPN > ao assistente do VPN de Site-**

para-Site:

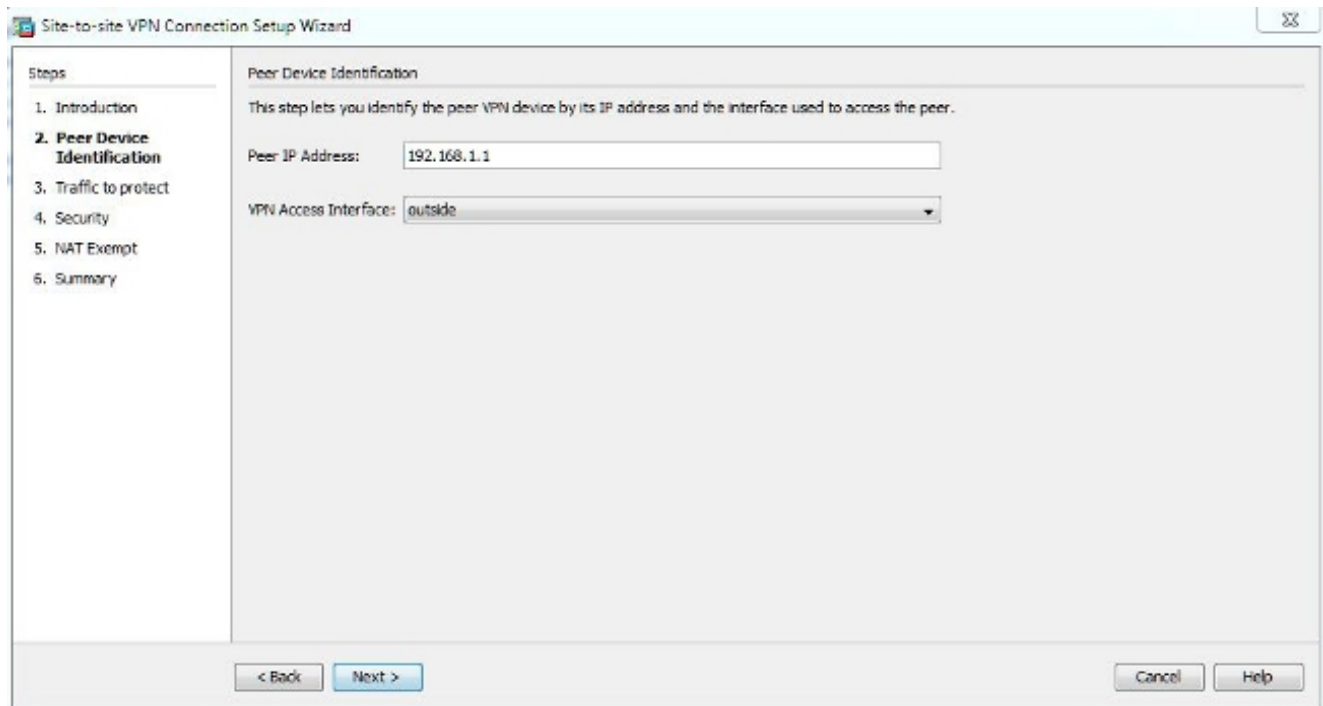


2. Clique **em seguida** uma vez que você alcança o Home Page do assistente:

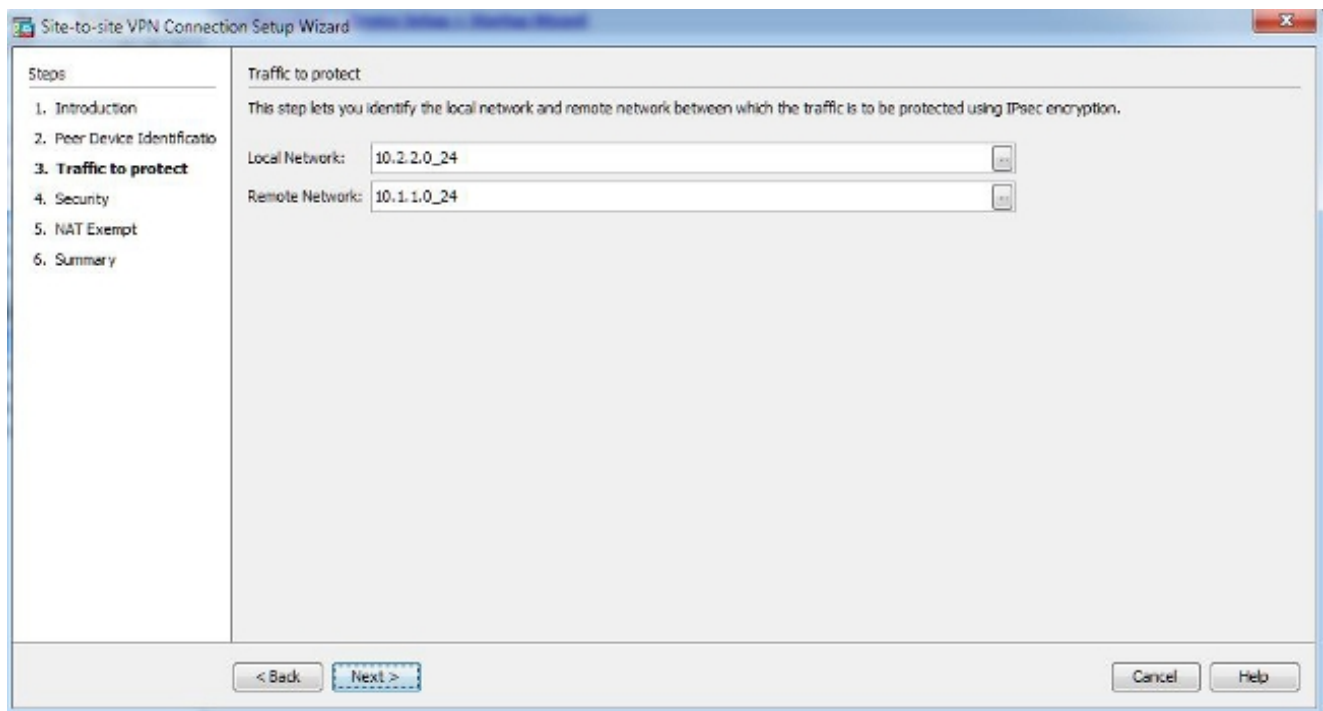


Nota: As versões as mais recentes ASDM fornecem um link a um vídeo que explique esta configuração.

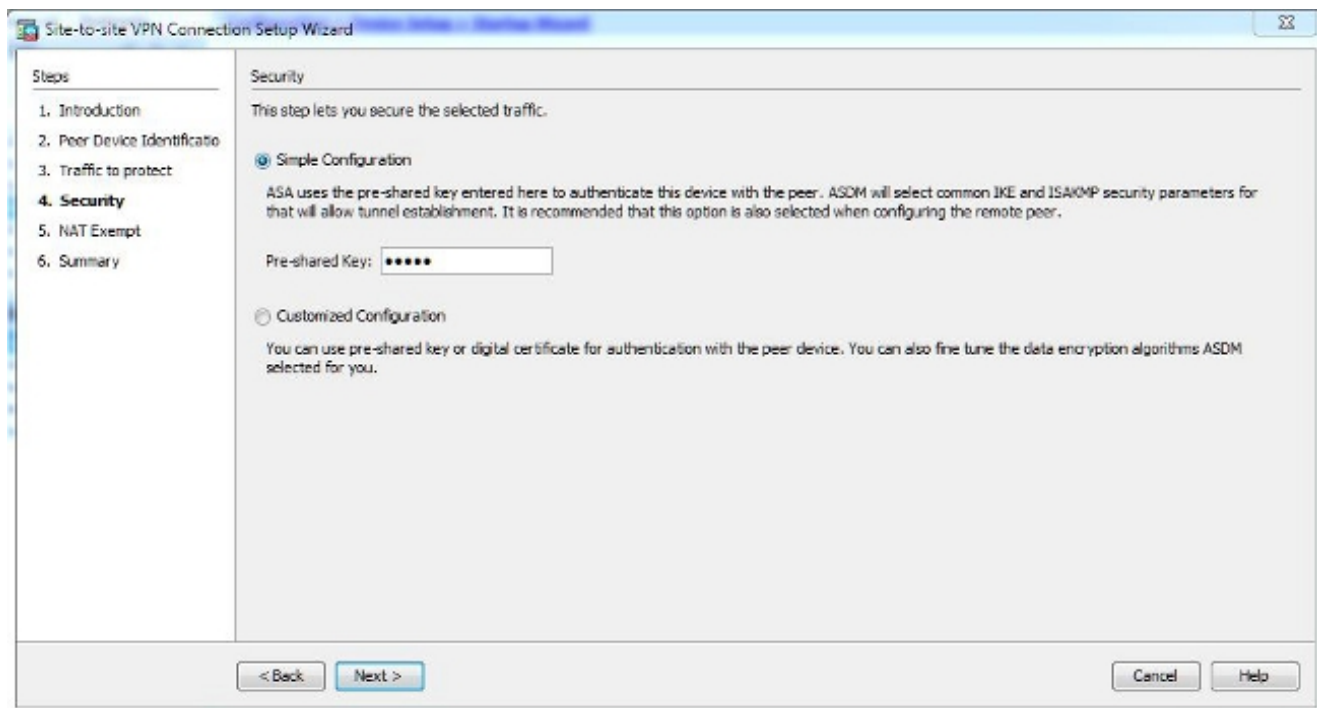
3. Configurar o endereço IP do peer. Neste exemplo, o endereço IP do peer é ajustado a 192.168.1.1 no local B. Se você configura o endereço IP do peer no local A, deve ser mudado a 172.16.1.1. A relação através de que a extremidade remota pode ser alcançada é especificada igualmente. Clique **em seguida** uma vez completo.



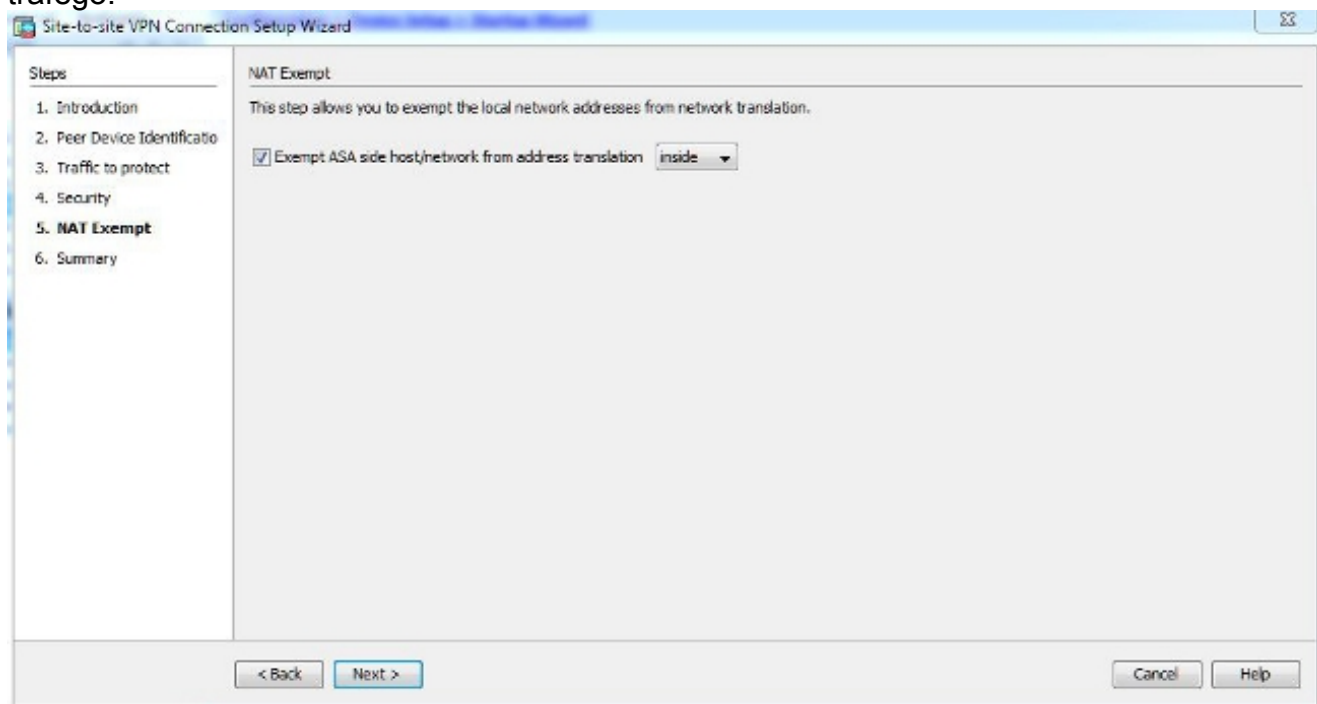
4. Configurar as redes remotas e locais (origem de tráfego e destino). Esta imagem mostra a configuração para o local B (o reverso se aplica para o local A):



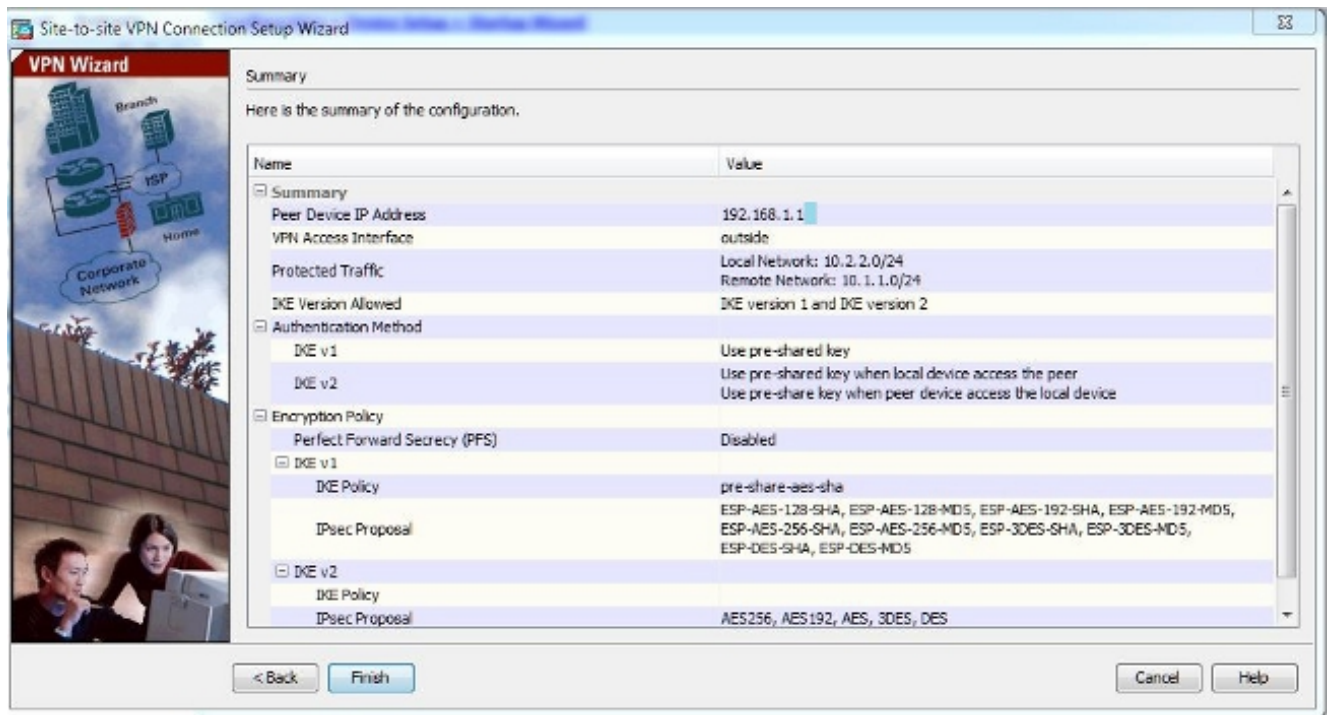
5. Na página da Segurança, configurar a chave pré-compartilhada (deve combinar em ambos as extremidades). Clique **em seguida** uma vez completo.



6. Configurar a interface de origem para o tráfego no ASA. O ASDM cria automaticamente a regra do Network Address Translation (NAT) baseada na versão ASA e empurra-a com o resto da configuração na etapa final. Nota: Para o exemplo que é usado neste documento, *dentro de* é a fonte do tráfego.



7. O assistente fornece agora um sumário da configuração que será empurrada para o ASA. Reveja e verifique os ajustes de configuração, e clique então o **revestimento**.



## Configurar através do CLI

Esta seção descreve como configurar o túnel de site para site do IPsec IKEv1 através do CLI.

### Configurar o local B para as versões ASA 8.4 e mais atrasado

Nas versões ASA 8.4 e mais atrasado, o apoio para a versão 2 IKEv1 e de intercâmbio de chave de Internet (IKEv2) foi introduzido.

Dica: Para obter mais informações sobre das diferenças entre as duas versões, refira [porque migre a IKEv2?](#) seção da *migração rápida de IKEv1 à configuração de túnel IKEv2 L2L* no documento Cisco do *código ASA 8.4*.

Dica: Para um exemplo de configuração IKEv2 com o ASA, refira o [túnel da site para site IKEv2 entre o ASA e o](#) documento Cisco dos [exemplos da configuração de roteador](#).

### Fase 1 (IKEv1)

Termine estas etapas para a configuração da fase 1:

1. Incorpore este comando no CLI a fim permitir IKEv1 na interface externa:  
`crypto ikev1 enable outside`
2. Crie uma política IKEv1 que defina os algoritmos/métodos a ser usados para picar, autenticação, grupo Diffie-Hellman, vida, e criptografia:  
`crypto ikev1 policy 1`  
!The 1 in the above command refers to the Policy suite priority  
(1 highest, 65535 lowest)  
`authentication pre-share`  
`encryption aes`  
`hash sha`  
`group 2`

```
lifetime 86400
```

3. Crie um grupo de túneis sob os atributos do IPsec e configurar o endereço IP do peer e a chave pré-compartilhada do túnel:

```
tunnel-group 192.168.1.1 type ipsec-l2l  
tunnel-group 192.168.1.1 ipsec-attributes  
ikev1 pre-shared-key cisco
```

! Note the IKEv1 keyword at the beginning of the pre-shared-key command.

## **Fase 2 (IPsec)**

Termine estas etapas para a configuração da fase 2:

1. Crie uma lista de acessos que defina o tráfego a ser cifrado e escavado um túnel. Neste exemplo, o tráfego do interesse é o tráfego do túnel que é originado da sub-rede de 10.2.2.0 a 10.1.1.0. Pode conter entradas múltiplas se há uns sub-rede múltipla envolvidos entre os locais.

Nas versões 8.4 e mais recente, os objetos ou os grupos de objetos podem ser criados que servem como recipientes para as redes, as sub-redes, os endereços IP de Um ou Mais Servidores Cisco ICM NT do host, ou os objetos múltiplos. Crie dois objetos que têm o local e as sub-redes remotas e use-os para o Access Control List cripto (ACL) e as declarações NAT.

```
object network 10.2.2.0_24  
subnet 10.2.2.0 255.255.255.0  
object network 10.1.1.0_24  
subnet 10.1.1.0 255.255.255.0
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

2. Configurar o grupo da transformação (TS), que deve envolver a palavra-chave **IKEv1**. Um TS idêntico deve ser criado na extremidade remota também.  

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```
3. Configurar o crypto map, que contém estes componentes:

O endereço IP do peer

A lista de acessos definida que contém o tráfego do interesse

O TS

Um ajuste opcional do discrição perfeita adiante (PFS), que crie um par novo de chaves diffie-hellman que são usadas a fim proteger os dados (ambos os lados deve PFS-ser permitido antes da fase 2 vem acima)

4. Aplique o crypto map na interface externa:

```
crypto map outside_map 20 match address 100  
crypto map outside_map 20 set peer 192.168.1.1  
crypto map outside_map 20 set ikev1 transform-set myset  
crypto map outside_map 20 set pfs  
crypto map outside_map interface outside
```

## **Isenção de NAT**

Assegure-se de que o tráfego VPN não esteja sujeitado a nenhuma outra regra NAT. Esta é a regra NAT que é usada:

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

**Nota:** Quando os sub-rede múltipla são usados, você deve criar grupos de objetos com toda a fonte e sub-rede de destino e usá-los na regra NAT.

```
object-group network 10.x.x.x_SOURCE
network-object 10.4.4.0 255.255.255.0
network-object 10.2.2.0 255.255.255.0
```

```
object network 10.x.x.x_DESTINATION
network-object 10.3.3.0 255.255.255.0
network-object 10.1.1.0 255.255.255.0
```

```
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination
static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

### ***Termine a configuração de exemplo***

Está aqui a configuração completa para o local B:

#### **crypto ikev1 enable outside**

```
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
!Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.10_24
subnet 10.1.1.0 255.255.255.0
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.254.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

## **Configurar o local A para as versões ASA 8.2 e mais adiantado**

Esta seção descreve como configurar o local A para as versões ASA 8.2 e mais adiantado.

### ***Fase 1 (ISAKMP)***

Termine estas etapas para a configuração da fase 1:



1. Incorpore este comando no CLI a fim permitir o Internet Security Association and Key Management Protocol (ISAKMP) na interface externa:  

```
crypto isakmp enable outside
```

Nota: Porque as versões múltiplas do IKE (IKEv1 e IKEv2) não são apoiadas mais por muito tempo, o ISAKMP é usado a fim referir a fase 1.
2. Crie uma política de ISAKMP que defina os algoritmos/métodos a ser usados a fim construir a fase 1. Nota: Neste exemplo de configuração, a palavra-chave *IKEv1* da versão 9.x é substituída com o *ISAKMP*.  

```
crypto isakmp policy 1
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```
3. Crie um grupo de túneis para o endereço IP do peer (endereço IP externo de 5515) com a chave pré-compartilhada:  

```
tunnel-group 172.16.1.1 type ipsec-l2l
 tunnel-group 172.16.1.1 ipsec-attributes
 pre-shared-key cisco
```

## **Fase 2 (IPsec)**

Termine estas etapas para a configuração da fase 2:

1. Similar à configuração na versão 9.x, você deve criar uma lista de acesso estendida a fim definir o tráfego do interesse.  

```
access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
```
2. Defina um TS que contenha toda a criptografia e algoritmos de hashing disponíveis (oferecidos edições tenha um ponto de interrogação). Assegure-se de que esteja idêntico àquele que foi configurado no outro lado.  

```
crypto ipsec transform-set myset esp-aes esp-sha-hmac
```
3. Configurar um crypto map, que contenha estes componentes:

O endereço IP do peer

A lista de acessos definida que contém o tráfego do interesse

O TS

Uns pF opcional que ajustam-se, que criam um par novo de chaves diffie-hellman que são usadas a fim proteger os dados (ambos os lados devem PFS-ser permitidos de modo que a fase 2 venha acima)

4. Aplique o crypto map na interface externa:  

```
crypto map outside_map 20 set peer 172.16.1.1
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

## **Isenção de NAT**

Crie uma lista de acessos que defina o tráfego a ser isentado das verificações NAT. Nesta versão, parece similar à lista de acessos que você definiu para o tráfego do interesse:

```
access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
```

```
10.2.2.0 255.255.255.0
```

Quando os sub-rede múltipla são usados, adicionar uma outra linha à mesma lista de acessos:

```
access-list nonat line 1 extended permit ip 10.3.3.0 255.255.255.0
10.4.4.0 255.255.255.0
```

A lista de acessos é usada com o NAT, como mostrado aqui:

```
nat (inside) 0 access-list nonat
```

*Nota: O interior aqui refere o nome da interface interna em que o ASA recebe o tráfego que combina a lista de acessos.*

### ***Termine a configuração de exemplo***

Está aqui a configuração completa para o local A:

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha group 2
lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat
```

### **Política do grupo**

As políticas do grupo são usadas a fim definir os ajustes específicos que se aplicam ao túnel. Estas políticas são usadas conjuntamente com o grupo de túneis.

A política do grupo pode ser definida como qualquer um interno, assim que significa que os atributos estão puxados daquele que é definido no ASA, ou pode ser definido como externo, onde os atributos são perguntados de um servidor interno. Este é o comando que é usado a fim definir a política do grupo:

```
group-policy SITE_A internal
```

*Nota: Você pode definir atributos múltiplos na política do grupo. Para uma lista de todos os atributos possíveis, refira a seção [configurando das políticas do grupo dos procedimentos de configuração de VPN selecionados ASDM para o 5500 Series de Cisco ASA, versão 5.2.](#)*

## ***Agrupe atributos opcionais da política***

O atributo do VPN-túnel-protocolo determina o tipo de túnel a que estes ajustes devem ser aplicados. Neste exemplo, o *IPsec* é usado:

```
vpn-tunnel-protocol ?
group-policy mode commands/options:
IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
svc SSL VPN Client
webvpn WebVPN
```

```
vpn-tunnel-protocol ipsec - Versions 8.2 and prior
vpn-tunnel-protocol ikev1 - Version 8.4 and later
```

Você tem a opção para configurar o o túnel de modo que fique a quietude (sem tráfego) e não vá para baixo. A fim configurar esta opção, o valor de atributo do VPN-quietude-intervalo deve usar minutos, ou você pode ajustar o valor a **nenhuns**, assim que significa que o túnel nunca vai para baixo.

Aqui está um exemplo:

```
group-policy SITE_A attributes
vpn-idle-timeout ?
group-policy mode commands/options:
<1-35791394> Number of minutes
none IPSec VPN: Disable timeout and allow an unlimited idle period;
```

O comando da padrão-grupo-**política** sob os atributos gerais do grupo de túneis define a política do grupo que é usada a fim empurrar determinados ajustes da política para o túnel que é estabelecido. As configurações padrão para as opções que você não definiu na política do grupo são tomadas de uma política do grupo padrão global:

```
tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE_A
```

## **Verificar**

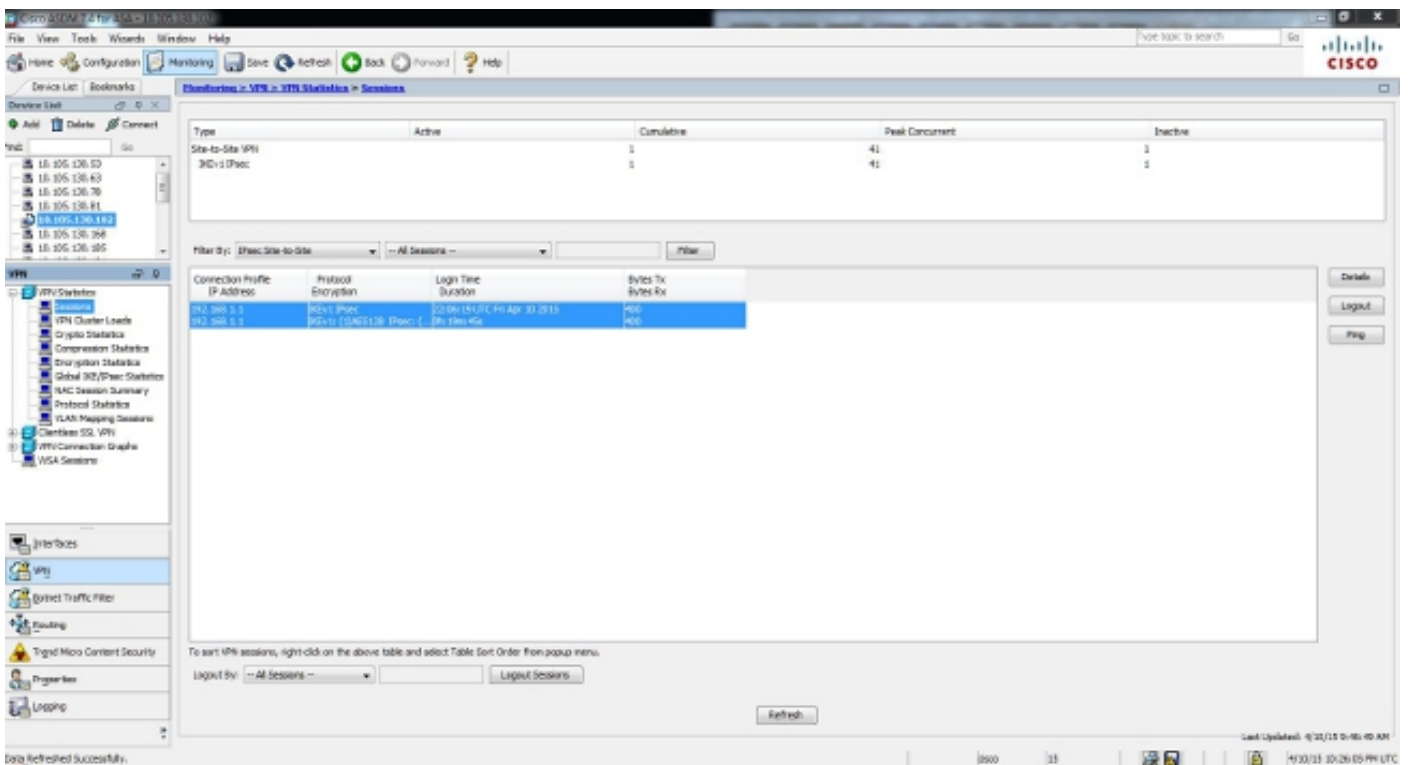
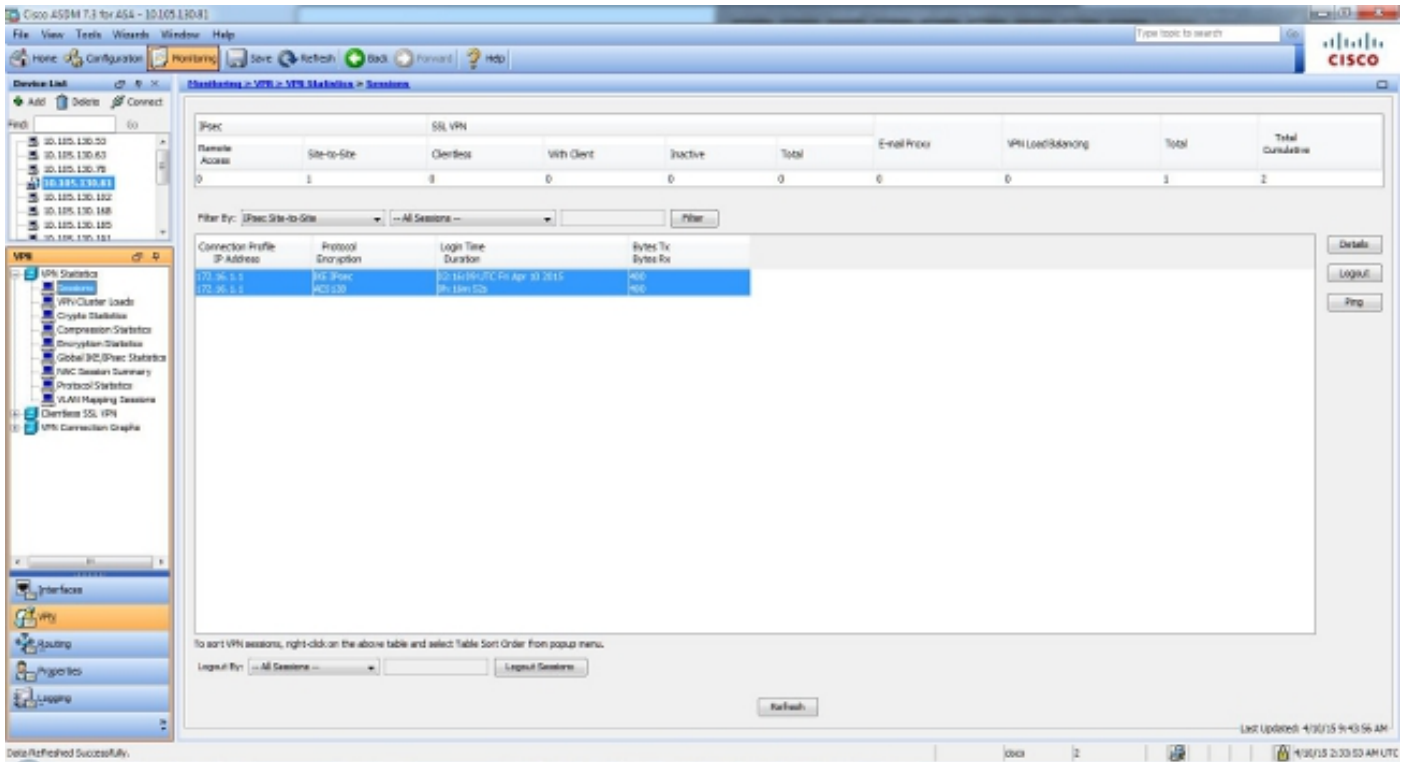
Use a informação que é fornecida nesta seção a fim verificar que sua configuração trabalha corretamente.

## **ASDM**

A fim ver o status de túnel do ASDM, navegue à **monitoração > VPN**. Esta informação é fornecida:

- O endereço IP do peer
- O protocolo que é usado a fim construir o túnel
- O algoritmo de criptografia que é usado
- O tempo em que o túnel veio acima e o acima-tempo
- O número de pacotes que são recebidos e transferidos

Dica: O clique **refresca** a fim ver os valores os mais atrasados, porque os dados não atualizam no tempo real.



## CLI

Esta seção descreve como verificar sua configuração através do CLI.

## Fase 1

Incorpore este comando no CLI a fim verificar a configuração da fase 1 nos 5515) lados do local B (:

```
show crypto ikev1 sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

Incorpore este comando no CLI a fim verificar a configuração da fase 1 nos 5510) lados do local A (:

```
show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

## Fase 2

O comando **show crypto ipsec sa** mostra o sas de IPsec que é construído entre os pares. O túnel criptografado é construído entre endereços IP 192.168.1.1 e 172.16.1.1 para o tráfego que flui entre as redes 10.1.1.0 e 10.2.2.0. Você pode ver o dois ESP SA construído para o tráfego de entrada e de saída. O Authentication Header (AH) não é usado porque não há nenhum AH SA.

Incorpore este comando no CLI a fim verificar a configuração da fase 2 nos 5515) lados do local B (:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
  local ident (addr/mask/prot/port): (10.2.2.0/255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x3D3(979)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

Incorpore este comando no CLI a fim verificar a configuração da fase 2 nos 5510) lados do local A (:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

## Troubleshooting

Use a informação que é fornecida nesta seção a fim pesquisar defeitos problemas de configuração.

## Versões ASA 8.4 e mais atrasado

Inscreva estes comandos debug a fim determinar o lugar da falha do túnel:

- debug crypto ikev1 127 (fase 1)

- IPsec 127 do debug crypto (fase 2)

Está aqui um resultado do debug completo do exemplo:

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
```

(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA\_KE payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload  
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing  
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco  
VPN3000/Cisco ASA GW VID  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload  
!  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, **Connection landed on tunnel\_group  
192.168.1.1**  
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating  
keys for Initiator...  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing  
ID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing  
hash payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing  
hash for ISAKMP  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive  
payload: proposal=32767/32767 sec.  
!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms  
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
constructing dpd vid payload  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 96  
**Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT  
Detection Status: Remote end is NOT behind a NAT device This end is NOT behind  
a NAT device**  
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500  
from 192.168.1.1:500  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE RECEIVED Message (msgid=0)  
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 96  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing  
ID payload  
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,  
ID\_IPV4\_ADDR ID received 192.168.1.1  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
processing hash payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing  
hash for ISAKMP  
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload:  
proposal=32767/32767 sec.  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing  
VID payload  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received  
DPD VID  
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel\_group  
192.168.1.1  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley  
begin quick mode



Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21

**Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED**

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds.

IPSEC: New embryonic SA created @ 0x75298588,  
SCB: 0x75C34F18,  
Direction: inbound  
SPI : 0x03FC9DB7  
Session ID: 0x00004000  
VPIF num : 0x00000002  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got SPI from key engine: SPI = 0x03fc9db7

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing quick mode

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPsec SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPsec nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing proxy ID

**Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Transmitting Proxy Id:**

**Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0**

**Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0**

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending Initial Contact

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing qm hash payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200

Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.2.2.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID\_IPV4\_ADDR\_SUBNET ID received--10.1.1.0--255.255.255.0

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, loading all IPSEC SAs

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key!

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

NP encrypt rule look up for crypto map outside\_map 20 matching ACL  
100: returned cs\_id=6ef246d0; encrypt\_rule=752972d0;  
tunnelFlow\_rule=75ac8020  
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,  
Generating Quick Mode Key!  
IPSEC: New embryonic SA created @ 0x6f0e03f0,  
SCB: 0x75B6DD00,  
Direction: outbound  
SPI : 0x1BA0C55C  
Session ID: 0x00004000  
VPIF num : 0x00000002  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds  
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C  
IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C  
Flags: 0x00000005  
SA : 0x6f0e03f0  
SPI : 0x1BA0C55C  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x0B47D387  
Channel: 0x6ef0a5c0  
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C  
VPN handle: 0x0000f614  
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C  
Src addr: 10.2.2.0  
Src mask: 255.255.255.0  
Dst addr: 10.1.1.0  
Dst mask: 255.255.255.0  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 0  
Use protocol: false  
SPI: 0x00000000  
Use SPI: false  
IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C  
Rule ID: 0x74e1c558  
IPSEC: New outbound permit rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255  
Dst addr: 192.168.1.1  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C  
Rule ID: 0x6f0dec80

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule  
look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=6ef246d0;  
encrypt\_rule=752972d0; tunnelFlow\_rule=75ac8020

Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation  
complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7,  
Outbound SPI = 0x1ba0c55c

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley  
constructing final quick mode

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator  
sending 3rd QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21)  
with payloads : HDR + HASH (8) + NONE (0) total length : 76

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY\_ADD  
msg for SA: SPI = 0x1ba0c55c

IPSEC: New embryonic SA created @ 0x75298588,  
SCB: 0x75C34F18,  
Direction: inbound  
SPI : 0x03FC9DB7  
Session ID: 0x00004000  
VPIF num : 0x00000002  
Tunnel type: 121  
Protocol : esp  
Lifetime : 240 seconds

IPSEC: Completed host IBSA update, SPI 0x03FC9DB7  
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7  
Flags: 0x00000006  
SA : 0x75298588  
SPI : 0x03FC9DB7  
MTU : 0 bytes  
VCID : 0x00000000  
Peer : 0x0000F614  
SCB : 0x0B4707C7  
Channel: 0x6ef0a5c0

IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7  
VPN handle: 0x00011f6c

IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C  
Flags: 0x00000005  
SA : 0x6f0e03f0  
SPI : 0x1BA0C55C  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00011F6C  
SCB : 0x0B47D387  
Channel: 0x6ef0a5c0

IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C  
VPN handle: 0x0000f614

IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C  
Rule ID: 0x74e1c558

IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C  
Rule ID: 0x6f0dec80

IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7  
Src addr: 10.1.1.0  
Src mask: 255.255.255.0  
Dst addr: 10.2.2.0  
Dst mask: 255.255.255.0  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 0

```
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

## Versões ASA 8.3 e mais adiantado

Inscreva estes comandos debug a fim determinar o lugar da falha do túnel:

- **isakmp 127 do debug crypto (fase 1)**
- **IPsec 127 do debug crypto (fase 2)**

Está aqui um resultado do debug completo do exemplo:

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
```

NONE (0) total length : 172  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation  
capability flags: Main Mode: True Aggressive Mode: True  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload  
**Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1  
acceptable Matches global IKE entry # 1**  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver  
02 payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID +  
extended capabilities payload  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=0) with  
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message (msgid=0) with  
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +  
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA\_KE payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS  
Vendor ID payload (version: 1.0.0, capabilities: 20000001)  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco  
ASA GW VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor  
ID payload (version: 1.0.0, capabilities: 20000001)  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco  
ASA GW VID  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash  
**Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel\_group 172.16.1.1**  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys  
for Responder...  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=0) with  
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +  
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message (msgid=0) with

payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)  
total length : 96  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing  
ID payload  
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID\_IPV4\_ADDR  
ID received 172.16.1.1  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing  
hash payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing  
hash for ISAKMP  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload:  
proposal=32767/32767 sec.  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing  
VID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection  
Status: Remote end is NOT behind a NAT device This end is NOT behind  
a NAT device**  
**Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel\_group 172.16.1.1**  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
constructing ID payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
constructing hash payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
Computing hash for ISAKMP  
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload:  
proposal=32767/32767 sec.  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
constructing dpd vid payload  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=0) with  
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)  
total length : 96  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED**  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1  
rekey timer: 82080 seconds.  
Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id =  
4c073b21  
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message  
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +  
ID (5) + NOTIFY (11) + NONE (0) total length : 200  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
processing hash payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
processing SA payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
processing nonce payload  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
processing ID payload  
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,  
ID\_IPV4\_ADDR\_SUBNET ID received--10.2.2.0--255.255.255.0  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP  
Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0,  
Protocol 0, Port 0  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,  
processing ID payload  
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,  
ID\_IPV4\_ADDR\_SUBNET ID received--10.1.1.0--255.255.255.0  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP  
Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,  
Protocol 0, Port 0  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing  
notify payload  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa

not found by addr

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside\_map, seq = 20...

**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside\_map, seq = 20 is a successful match**

**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside\_map**

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPsec SA payload

**Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPsec SA Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 20**

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!  
IPSEC: New embryonic SA created @ 0xAB5C63A8,  
SCB: 0xABD54E98,

Direction: inbound

SPI : 0x1BA0C55C

Session ID: 0x00004000

VPIF num : 0x00000001

Tunnel type: 121

Protocol : esp

Lifetime : 240 seconds

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI from key engine: SPI = 0x1ba0c55c

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley constructing quick mode

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing blank hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPsec SA payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPsec nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing proxy ID

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting Proxy Id:

Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0

Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing qm hash payload

Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder sending 2nd QM pkt: msg id = 4c073b21

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE\_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all IPSEC SAs

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=ab9302f0; rule=ab9309b0

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!

IPSEC: New embryonic SA created @ 0xAB570B58,  
SCB: 0xABD55378,

Direction: outbound

SPI : 0x03FC9DB7

Session ID: 0x00004000

VPIF num : 0x00000001

Tunnel type: 121

Protocol : esp  
Lifetime : 240 seconds  
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7  
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7  
Flags: 0x00000005  
SA : 0xAB570B58  
SPI : 0x03FC9DB7  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x01512E71  
Channel: 0xA7A98400  
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7  
VPN handle: 0x0000F99C  
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7  
Src addr: 10.1.1.0  
Src mask: 255.255.255.0  
Dst addr: 10.2.2.0  
Dst mask: 255.255.255.0  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 0  
Use protocol: false  
SPI: 0x00000000  
Use SPI: false  
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7  
Rule ID: 0xABD557B0  
IPSEC: New outbound permit rule, SPI 0x03FC9DB7  
Src addr: 192.168.1.1  
Src mask: 255.255.255.255  
Dst addr: 172.16.1.1  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x03FC9DB7  
Use SPI: true  
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7  
Rule ID: 0xABD55848  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule  
look up for crypto map outside\_map 20 matching ACL 100: returned cs\_id=ab9302f0;  
rule=ab9309b0  
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation  
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,  
Outbound SPI = 0x03fc9db7  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a  
KEY\_ADD msg for SA: SPI = 0x03fc9db7  
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C  
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C  
Flags: 0x00000006  
SA : 0xAB5C63A8



SPI : 0x1BA0C55C  
MTU : 0 bytes  
VCID : 0x00000000  
Peer : 0x0000F99C  
SCB : 0x0150B419  
Channel: 0xA7A98400  
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C  
VPN handle: 0x0001169C  
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7  
Flags: 0x00000005  
SA : 0xAB570B58  
SPI : 0x03FC9DB7  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x0001169C  
SCB : 0x01512E71  
Channel: 0xA7A98400  
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7  
VPN handle: 0x0000F99C  
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7  
Rule ID: 0xABD557B0  
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7  
Rule ID: 0xABD55848  
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C  
Src addr: 10.2.2.0  
Src mask: 255.255.255.0  
Dst addr: 10.1.1.0  
Dst mask: 255.255.255.0  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 0  
Use protocol: false  
SPI: 0x00000000  
Use SPI: false  
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C  
Rule ID: 0xAB8D98A8  
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255  
Dst addr: 192.168.1.1  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C  
Rule ID: 0xABD55CB0  
IPSEC: New inbound permit rule, SPI 0x1BA0C55C  
Src addr: 172.16.1.1  
Src mask: 255.255.255.255

Dst addr: 192.168.1.1  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x1BA0C55C  
Use SPI: true  
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C  
Rule ID: 0xABD55D48  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received  
KEY\_UPDATE, spi 0x1ba0c55c  
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey  
timer: 27360 seconds.  
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED  
(msgid=4c073b21)**