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

## Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de Rede Configurar por meio do assistente de VPN do ASDM Configurar por meio da CLI Configurar o site B para ASA versão 8.4 e posteriores Configurar o site A para ASA versão 8.2 e anteriores Política de grupo Verificar **ASDM** CLI Fase 1 Fase 2 Troubleshoot ASA versão 8.4 e posteriores ASA versão 8.3 e anteriores

## Introduction

Este documento descreve como configurar um túnel site a site IPsec (IKEv1) versão 1 do Internet Key Exchange entre um Cisco 5515-X Series Adaptive Security Appliance (ASA) que executa a versão de software 9.2.x e um Cisco 5510 Series ASA que executa a versão de software 8.2.x.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- A conectividade IP de ponta a ponta deve ser estabelecida
- Estes protocolos devem ser permitidos:

User Datagram Protocol (UDP) 500 e 4500 para o plano de controle IPsecEncapsulating Security Payload (ESP) IP Protocol 50 para o plano de dados 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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

Esta seção descreve como configurar o túnel VPN site a site por meio do assistente de VPN do ASDM (Adaptive Security Device Manager) ou por meio da CLI.

### Diagrama de Rede





### Configurar por meio do assistente de VPN do ASDM

Siga estas etapas para configurar o túnel VPN site a site por meio do assistente do ASDM:

1. Abra o ASDM e navegue até Wizards > VPN Wizards > Site-to-site VPN Wizard.

Cisco ASEM T4 tord		10 m		All of the local division of the local divis	1 miles - 10		0.0
View Toole W	erðs Window Help					We topic to search	illa altalla
HINE OF CON	Statup Weard.						CISCO
Derive List . But	VPN Waards * Sterlo sile VPN Waard.						1
or list	High Armidelity and Scalebility Woord_						
et 🛱 Celete	Unified Conversariation Weard Chevites 532 VPN Wzard		tank in the second				
	ASDM Identity Cartificate Waand. (Psec (REd) Remote Access VPN Waand.)		Enterteos Status				
20. 120. 120. 12	Pashat Capture Wisand.	14	Interface:	IP Aldress Nak	Line	LHR	vitere
1.105.131.43	Heal Fame: electrate		4504	10.105.100.100/04	0.+	0.44	
ADD. 1201.100	AGA Version: 9.115319 Device Liptime: S6d Zh 44m 0s		inside	20.2.2.2.294	<b>0</b> up	0.0	
5130100	40/mesoni 7.4(1) Jevie Troe ASA 5530, 55H-CSC-20-45		kneide2	10.4.4.1/24	0.40	0.0	
5.130.395	Pressel Mode: Readed Excitact Mode: Single		ousite	172.16.1.1(24	0.0	<b>9</b> up	1
1.130.191	Tatal Rody 256 MB Total Memory 2648 MB	Tatal Rady 256 HB Total Henroys 2848 HB					
136.122							
303-138-224	Withourse State of the A		Patron Claim				
06.44.154	Date Creating where we have a set the contract of the contract	VENUE.	Have the not carrique	in case the link to compare it.			VILLAND R
200.44.205	System-Resources Status	3	Traffic Status				
6.106.72.0	(Pit tage (servert)		- Connections Pay Sec	cond licege			214
	60 60 1% 40 30						
	(8.40-4 (0.52) (0.52) (0.52)	10-40		K9 97	+3.00	45.00	6.0
	Henory Liage (HD)		In date Departure 7	afferi sana Mani			
			in the second second	and heady frame			
			1.1				
	1000						
	500						
	UR454 0 1038 1037 1038 8030	10-00	10:58	10.07	+3.00	40.90	10-0
	Details	Povt Gps 1	OvbuctOpsi 0				
						1.000.000	
	Litest ASI/It Systep Hessages						13 - 6 - 1
	ASIZM logging a	feabled. To enable ASOM bogs	ng with informational level stogging	, dok the lautton below.			
at configuration leader	uccessfully.			100	15		A INTERESTICTION

2. Clique em Next quando chegar à página inicial do assistente.

🚡 Site-to-site VPN Connectio	n Setup Wizard
VPN Wizard	Introduction Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.
Corporate Network	Site-to-Site VPN
	Here is a <u>video</u> on how to setup a site-to-site VPN connection.
	< Back Next > Carrel Heb
	s oaus Cance Hep

**Observação**: as versões mais recentes do ASDM fornecem um link para um vídeo que explica essa configuração.

3. Configure o endereço IP do par. Neste exemplo, o endereço IP do par é definido como 192.168.1.1 no site B. Se você configurar o endereço IP do par no site A, ele deve ser alterado para 172.16.1.1. A interface através da qual a extremidade remota pode ser alcançada também é especificada. Clique em Next após a conclusão.

eps	Peer Device Identificat	ion .		
. Introduction	This step lets you ident	tfy the peer VPN device by its IP address and the interface used t	o access the peer.	
Peer Device Identification	Peer IP Address:	192.168.1.1		
. Traffic to protect	1153	1		
Security	VPN Access Interface:	outside	<b>•</b> .	
NAT Exempt				
Summary				

4. Configure as redes locais e remotas (origem e destino do tráfego). Esta imagem mostra a configuração para o Site B (o inverso se aplica ao Site A).

Steps	Traffic to protect			
Introduction     Peer Device Identificatio     Traffic to protect     Security     NAT Exempt     Operation	This step lets you Local Network: Remote Network:	dentify the local network and remote network betwe 10.2.2.0_24 10.1.1.0_24	en which the traffic is to be protected using IPsec encryption.	
6. Summary				
	C Back D		[ Created ]	( Holo

5. Na página Segurança, configure a chave pré-compartilhada (ela deve corresponder em ambas as extremidades). Clique em Next após a conclusão.

teps	Security	
Introduction     Peer Device Identificatio     Traffic to protect     Security     NAT Exempt     Summary	This step lets you secure the selected traffic.  Simple Configuration  ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISARMP security parameter that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.  Pre-shared Key:  Customized Configuration  You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms Assessed for you.	ers for
	<back next=""> Cancel</back>	Help

6. Configure a interface de origem para o tráfego no ASA. O ASDM cria automaticamente a regra de Network Address Translation (NAT) com base na versão do ASA e a envia com o restante da configuração na etapa final. **Observação**: no exemplo usado neste documento, 'inside' é a origem do

tráfego.

Steps	NAT Exempt	
Introduction     Introduction     Peer Device Identificatio     Traffic to protect     Security     NAT Exempt     Source Summery	This step allows you to exempt the local network addresses from network translation.    Exempt ASA side host/hetwork from address translation   inside	
	< Back Next >	Cancel Help

7. O assistente agora fornece um resumo da configuração que é enviada para o ASA. Revise e verifique as definições de configuração e clique em Finish.

Summary	
Here is the summary of the configuration.	
Name	Value
G Summary	
Peer Device IP Address	192.168.1.1
Home VPN Access Interface	outside
Protected Traffic	Local Network: 10.2.2.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
DKE v1	Use pre-shared key
DKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
E DKE v1	
IXE Policy	pre-share-aes-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5 ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
E DKE v2	
IKE Policy	
IPsec Proposal	AES256, AES192, AES, 3DES, DES

### Configurar por meio da CLI

Esta seção descreve como configurar o túnel site a site IPsec IKEv1 por meio da CLI.

#### Configurar o site B para ASA versão 8.4 e posteriores

No ASA versão 8.4 e posteriores, introduziu-se o suporte para IKEv1 e Internet Key Exchange versão 2 (IKEv2).

**Dica**: para obter mais informações sobre as diferenças entre as duas versões, consulte a seção <u>Por que migrar para IKEv2?</u> da Migração rápida de IKEv1 para a Configuração de túnel L2L IKEv2 no Código ASA 8.4 do documento Cisco.

**Dica**: para obter um exemplo de configuração IKEv2 com o ASA, consulte o documento IKEv2 Tunnel entre sites do ASA e Exemplos de Configuração de Roteador da Cisco.

#### Fase 1 (IKEv1)

Siga estas etapas para a configuração da Fase 1:

1. Digite este comando na CLI para ativar o IKEv1 na interface externa:

crypto ikev1 enable outside

2. Crie uma política de IKEv1 que defina os algoritmos/métodos a serem usados para hash, autenticação, grupo Diffie-Hellman, vida útil e criptografia:

```
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. Crie um grupo de túneis nos atributos de IPsec e configure o endereço IP do par e a chave pré-compartilhada do túnel:

```
tunnel-group 192.168.1.1 type ipsec-121
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)
```

Siga estas etapas para a configuração da Fase 2:

 Crie uma lista de acesso que defina o tráfego a ser criptografado e encapsulado. Neste exemplo, o tráfego de interesse é o tráfego do túnel originado da sub-rede 10.2.2.0 para 10.1.1.0. Ele pode conter várias entradas, se houver várias sub-redes envolvidas entre os sites.

Na versão 8.4 e posteriores, podem ser criados objetos ou grupos de objetos que servem de contêineres para redes, sub-redes, endereços IP de host ou vários objetos. Crie dois objetos que tenham as sub-redes locais e remotas e os use para as instruções da lista de controle de acesso (ACL) e 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. Configure o Transform Set (TS), que deve envolver a palavra-chave IKEv1. Um TS idêntico também deve ser criado na extremidade remota.

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

- 3. Configure um mapa de criptografia que contenha estes componentes: O endereço IP do parA lista de acesso definida que contenha o tráfego de interesseO TSUma configuração opcional de PFS (Perfect Forward Secrecy), que cria um novo par de chaves Diffie-Hellman usadas para proteger os dados (ambos os lados devem ser habilitados para PFS, antes que a Fase 2 seja iniciada)
- 4. Aplique o mapa de criptografia 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

Verifique se o tráfego de VPN não está sujeito a outras regras de NAT. Esta é a regra de NAT 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
```

**Observação**: quando várias sub-redes são usadas, você deve criar grupos de objetos com todas as sub-redes de origem e de destino e usá-las 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

#### Exemplo de configuração completa

Esta é a configuração completa do site 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-121
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 10.1.1.0_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
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 192.168.1.1
```

crypto map outside\_map 20 set ikev1 transform-set myset crypto map outside\_map 20 set pfs crypto map outside\_map interface outside

```
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 site A para ASA versão 8.2 e anteriores

Esta seção descreve como configurar o site A para o ASA versão 8.2 e anteriores.

#### Fase 1 (ISAKMP)

Siga estas etapas para a configuração da Fase 1:

1. Digite este comando na CLI para ativar o Internet Security Association and Key Management Protocol (ISAKMP) na interface externa:

crypto isakmp enable outside

**Observação**: como várias versões de IKE (IKEv1 e IKEv2) não são mais suportadas, o ISAKMP é usado para se referir à Fase 1.

2. Crie uma política de ISAKMP que defina os algoritmos/métodos a serem usados para criar a Fase 1.

**Observação**: neste exemplo de configuração, a palavra-chave IKEv1 da versão 9.x é substituído por ISAKMP.

crypto isakmp policy 1 authentication pre-share encryption aes hash sha group 2 lifetime 86400

 Crie um grupo de túneis para o endereço IP do par (endereço IP externo de 5515) com a chave pré-compartilhada:

```
tunnel-group 172.16.1.1 type ipsec-12l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
2 (IDece)
```

#### Fase 2 (IPsec)

Siga estas etapas para a configuração da Fase 2:

 Semelhante à configuração na versão 9.x, você deve criar uma lista de acesso estendida para definir o tráfego de interesse.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

 Defina um TS que contenha todos os algoritmos de criptografia e hash disponíveis (os problemas oferecidos têm um ponto de interrogação). Verifique se é idêntico ao que foi configurado do outro lado.

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

- 3. Configure um mapa de criptografia que contenha estes componentes: O endereço IP do parA lista de acesso definida que contenha o tráfego de interesseO TSUma configuração opcional de PFS, que cria um novo par de chaves Diffie-Hellman usadas para proteger os dados (ambos os lados devem ser habilitados para PFS, para que a Fase 2 seja iniciada)
- 4. Aplique o mapa de criptografia 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 acesso que defina o tráfego a ser isento das verificações de NAT. Nesta versão, ela parece semelhante à lista de acesso definida para o tráfego de 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 várias sub-redes forem usadas, adicione outra linha à mesma lista de acesso:

```
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 acesso é usada com o NAT, como mostrado aqui:

nat (inside) 0 access-list nonat

**Observação**: aqui, 'inside' se refere ao nome da interface interna na qual o ASA recebe o tráfego que corresponde à lista de acesso.

#### Exemplo de configuração completa

Esta é a configuração completa do site 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-121 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 set peer crypto map outside\_map 20 set transform-set myset crypto map outside\_map 20 set pfs 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 de grupo

As políticas de grupo são usadas para definir configurações específicas aplicáveis ao túnel. Essas políticas são usadas juntamente com o grupo de túneis.

A política de grupo pode ser definida como interna, o que significa que os atributos são extraídos do que é definido no ASA, ou pode ser definida como externa, na qual os atributos são consultados em um servidor externo. Este é o comando usado para definir a política de grupo:

group-policy SITE\_A internal

**Observação**: Você pode definir vários atributos na política de grupo. Para obter uma lista de todos os atributos possíveis, consulte a seção Configuração de políticas de grupo dos Procedimentos selecionados da configuração de VPN do ASDM para o Cisco ASA 5500 Series, versão 5.2.

#### Atributos opcionais da política de grupo

O vpn-tunnel-protocol determina o tipo de túnel ao qual essas configurações devem ser aplicadas. 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 de configurar o túnel para que ele permaneça ocioso (sem tráfego) e não seja desativado. Para configurar essa opção, o comando vpn-idle-timeout o valor do atributo deve usar

minutos ou você pode definir o valor para none, o que significa que o túnel nunca cai.

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 default-group-policy sob os atributos gerais do grupo de túneis define a política de grupo que é usada para enviar determinadas configurações de política para o túnel que é estabelecido. As configurações padrão das opções definidas na política de grupo são derivadas de uma política de grupo geral padrão:

tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE\_A

## Verificar

Use as informações fornecidas nesta seção para verificar se a configuração funciona corretamente.

### ASDM

Para visualizar o status do túnel a partir do ASDM, navegue até Monitoring > VPN. Estas informações são fornecidas:

- O endereço IP do par
- O protocolo usado para criar o túnel
- O algoritmo de criptografia usado
- A hora em que o túnel foi criado e o tempo de atividade
- O número de pacotes recebidos e transferidos

**Dica**: clique em Refresh para exibir os valores mais recentes, pois os dados não são atualizados em tempo real.

ing Store (	Careten Obsi	Deviati 🦉 Hdb							
	Charles and the second s								
odhadaq 2 VPR.2	. MR Stateline > Sensi								
Post.		SSL VPN				A DEPOSIS	wassesses.	1997	
Tamette Access	Site-to-Site	Gertless	With Client	Inactive	Total	Ereimon	1PH Loed Balancing	Total	
	1		0	0	0	. 0	0	1	1
the Roy Hour One	in the	Al Cambres -		L Alex 1					
the sy. practice		- He province -		Lowes .	-				
PAddress	Encryption	Duration		Bytter Ro					
2014-11 2014-11	405-250 405-230	12114354732 A	Apr 10 2015						
o sort VPN assessme	, right-click on the above to	die and select Table Sort O	inder from popular menu.						
agent for - Al Se	•		Logical Geneticity						
					talah				
									-Legi
							000 1		
							iana it	8	
Help							(060) (1	Trite Nor. 1: 1:070	
Help Tall Sever (C	Netes O tax	Orward ? He		_			josa ji	for tox b servi	
Help Try Date ( Storing & VIII & 1	🕽 tetest 🧿 Sax I	Ormed ? the		_			joses ji	The Nor. & Servit	
Help Frag Store (	🔾 ketesk 🔘 bas 1711 Sketalika – Second	Oriveral ? He					joea ji	Trie Kox & servi	
Help Tyl (a) Sert ( Alforden 2 VTS 2 ) Alforden 2 VTS 2 )	🤉 lettesi 🧿 tasi i	O forward 🦻 mbe Sectore		Grubber		Paid Decorrect 41	jone  ]	Frieton to servit	
Help Help Martine - VIN - 1 Martine - VIN - 1 Martine - Sta VIN HErri Date	3 lettes 0 tox 1	O forward 🦻 Hole as		Canadrane 1		Pack Concernent 41 41	jone  2	Viet Kort & Servit	
Help Help Marine 2 VIII 2 V Marine 2 V Ma	3 lettes   0 los   TH Statistics - Secula	Orward 🦻 Hole an Active		Canadese 2 3		Paik Concernet 41 41	3000 J	Frie toor is servit	
Help Tag Dave ( Anorea 2 178 2 ) per a-to-Sia 1991 HC+1 (Pec) her Sy: - Prec. Sian	Stetest State	Athen		Candidate 1		Paik Dincentert 41 41	jone  2	For tax, b servi	
Help Help Boot C Boot C Bo	Sector State	Ather		Caralder 1 1 Mar		Park Concentre 41 41	jone j	Port tax, b servi	
Help Help and Love ( Andrew 2, VIC 2, 2) Andrew 2, 1996 Her Opt (Proc.Care Direction Huffe (P. Admission)	Actron      tock      This Standards      Sociale     This Standards	Active		Carninker 1 1		Paik Dincentert 41 41	jone  2	Port tax: b servi	
Help Help and Long (1990) And Annu (1990) Annu (1990)	Actron      Action     Actio	Active Active Active Active Upgit The Disatory Active Logit The Disatory Active		Carninkee 1 1 Mass To Mass To Mass To Mass To		Pail Decenter 41 41	jone  2	Port tax: b servi	
Help Help and Line ( direction 2, MSL 2) and the solution 2, MSL 2) protection 2, MSL 2) protection 2, MSL 2) har Syst. Effect direction protection 1, MFC (2) Address protection 2, MSL 2) protection 2, MSL 2)	Active	Active Active Active Active Upp The Doctor	AP: 70 2011	Canaletere 1 3 Detes The Britte The Britte The		Paik Dincartett 41 41	jone j	Prot tax: b servi	
Help Help and Line ( dention 2, MS 2) per ten 5-543 (9) NC-1 (Prec. har 5p; Prec. State per colour Huffe (P Address per colour Huffe (P Address per colour State per colour State	A Referit O Book I THE Statistics - Secure Sociale Protocol Encryphon Protocol Encryphon Protocol Encryphon	Active Active Active Active Upgin The Building Active Logit The Building Active	AV: 17.2011	Canaletee 1 3 Dette To Brites To Brites To		Pail Decenter 41 41	3000 J	Prot tax: b serving	
Help Help and Line ( dention 2, 1/2, 2) per per ten Spin ( Per Construction per Color Huffe (P Actives) per Color Huffe (P Actives) per Color Spin ( Per Color Sp	Sociale	Active Active -Al Security - Logit The Busides Free ( ) is the used	A9' 82.2016	Curniètre 1 1 Mais Tix Room Rix Room Rix		Pail Concent 41 41	000 J	Prot tax: b servi	
Help Help and Line ( Andrew 2, MC 2) Andrew 2, MC 2)	A fetteri O tox i TTS Statution - Second Soldte Protocol Proto	Active Active Active Active Upgn The Design of the Design		Conditions 2 3 Most Tix Break Rx		Pail Concentre 41 41	0000 J	Inclus	
Help Help and Line ( Andrew 2, MCR 2) Andrew	Anterest Status - Secure Solate Protocol Entrophon Entrophon E	Active Active Active Active Upgn Three Disation Disation Contents		Conditions 1 1 1 1 1 1 1 1 1 1 1 1 1		Paik Concernent 41 41	0000 J	I we take to send	
Help Help and Help Andrew 2, MAR 2 Her Ty: Prescher Dar Ty: P	Sociale	Active Active Active Active Upgin The Building Contents Active Ac	A9' (7 2011-	Curniètre 1 1 1 Maria Roma Ro Roma Ro		Pail Concentre 41 41	000 2	Profe Nor, Ib year/o	
Hele Hele Hele Hele VIII at 1 Hele VIIII at 1 Hele VIIII at 1 Hele VIIII at 1 Hele VIIII at 1 Hele VIIIII at 1 Hele VIIII at 1 Hele VIIII at 1 Hele VIIII at 1 Hel	Anterest O box   The Second S	Active	AP 102011	Considere 1 1 Protes Te Protes Te		Peek Concernent 41 41		Print for it south	
Hele Hele Hele Hele Hele Hele Hele Hele	Anterest O toos )	Active	AP 10 2011	Considere 3 3 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		Peek Concernent 44 91		Print face: B search	
Hag Hag Hag Hardens 2 VIX 2 1 Hardens 2 VIX 2	Anterest O toos a	Active	AP 10 2011	Considere 3 1 Moto Rx Moto Rx		Peek Cincurset 44 11		Print face is sourch	

tara hereshed successfully.

A Trend Micro Content Security

To said UPN as

sieris, right club or

Logout By: -- All Sessions --

## CLI

S. nyura

Esta seção descreve como verificar a configuração por meio da CLI.

nd adject Table Dort Order From papage

Light Sessins

#### Fase 1

Digite este comando na CLI para verificar a configuração da Fase 1 no lado do site B (5515):

Refesh

😹 🖬 🕴 👔 🖓 autor to can ta martic

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** 

Digite este comando na CLI para verificar a configuração da Fase 1 no lado do site A (5510):

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 show crypto ipsec sa mostra as SAs IPsec que são criadas entre os correspondentes. O túnel criptografado é criado entre os 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 as duas SAs de ESP criadas para o tráfego de entrada e de saída. O cabeçalho de autenticação (AH) não é usado porque não há SAs de AH.

Digite este comando na CLI para verificar a configuração da Fase 2 no lado do site B (5515):

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
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:
```

Digite este comando na CLI para verificar a configuração da Fase 2 no lado do site A (5510):

```
interface: FastEthernet()
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
```

## Troubleshoot

Use as informações fornecidas nesta seção para solucionar problemas de configuração.

#### ASA versão 8.4 e posteriores

Digite estes comandos debug para determinar o local da falha de túnel:

- debug crypto ikev1 127 (Fase 1)
- debug crypto ipsec 127 (Fase 2)

Aqui está um exemplo completo de saída de depuração:

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 pavload 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 1 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 pavload 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. 1 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 guick 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 : 0x0000002 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 constucting 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 : 0x0000002 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x1BA0C55C IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C Flags: 0x0000005 SA : 0x6f0e03f0 SPI : 0x1BA0C55C MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 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: 0x0000000 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 : 0x0000002
Tunnel type: 121
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x0000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x0000000
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: 0x0000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x0000000
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: 0x0000000 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)

#### ASA versão 8.3 e anteriores

Digite estes comandos debug para determinar o local da falha de túnel:

```
• debug crypto isakmp 127 (Fase 1)
```

#### • debug crypto ipsec 127 (Fase 2)

Aqui está um exemplo completo de saída de depuração:

```
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 pavload 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 pavload 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 : 0x0000001 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 constucting guick 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 pavload 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 : 0x0000001 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x03FC9DB7 IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7 Flags: 0x0000005 SA : 0xAB570B58 SPI : 0x03FC9DB7 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 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: 0x0000000 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 = 0x03fc9db7Feb 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: 0x0000006 SA : 0xAB5C63A8 SPI : 0x1BA0C55C MTU : 0 bytes VCID : 0x0000000 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: 0x0000005 SA : 0xAB570B58 SPI : 0x03FC9DB7 MTU : 1500 bytes VCID : 0x0000000 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: 0x0000000 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)

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.