Configuración de túneles IPsec de IKEv1 de sitio a sitio con ASDM o la CLI en ASA

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de la red Configuración a través del Asistente de VPN ASDM Configuración a través de CLI Configuración del sitio B para ASA versiones 8.4 y posteriores Configuración del sitio A para ASA versiones 8.2 y anteriores Directiva de grupo Verificación **ASDM** CLI Fase 1 Fase 2 Troubleshoot ASA versiones 8.4 y posteriores ASA versiones 8.3 y anteriores

Introducción

Este documento describe cómo configurar un túnel IPsec de sitio a sitio de Intercambio de claves de Internet versión 1 (IKEv1) entre un Cisco 5515-X Series Adaptive Security Appliance (ASA) que ejecuta la versión 9.2.x del software y un Cisco 5510 Series ASA que ejecuta la versión 8.2.x del software.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Se debe establecer la conectividad IP de extremo a extremo
- Se deben permitir estos protocolos: Protocolo de datagramas de usuario (UDP) 500 y 4500 para el plano de control IPsecProtocolo IP 50 de carga de seguridad de encapsulación (ESP) para el plano de datos IPsec

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA serie 5510 que ejecuta la versión de software 8.2
- Cisco 5515-X ASA que ejecuta la versión de software 9.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En esta sección se describe cómo configurar el túnel VPN de sitio a sitio mediante el asistente para VPN del Administrador adaptable de dispositivos de seguridad (ASDM) o mediante la CLI.

Diagrama de la red

Esta topología se utiliza para los ejemplos de este documento:



Configuración a través del Asistente de VPN ASDM

Complete estos pasos para configurar el túnel VPN de sitio a sitio a través del asistente de ASDM:

1. Abra el ASDM y navegue hasta Wizards > VPN Wizards > Site-to-site VPN Wizard.

Cipio ASEM 74 tord	454-3031513	010	-	internal in the	a landar		Manager and	100		All shares the second	-			
View Tools W	Voerde Windo	w Help	5									Vpe topic to select-	64	aludi.
Derive Line Bas	Startup Win VDN Minard Minh August	ed.		N	Site to site VI	N Ward.	\geq							CISCO
Ace List	Grafinal Core		en Werel		Charles III	The strand								
del 👔 Celata	ASDEM Salare	ity Catili	ute Winand	2	UPper (RE-01)	Printle Access VPR	Minet.		Interface Status					
and the second	Paulot Capt	Are Wisse	4.		to ave (name) -	CONTRACTOR OF CONTRACTOR			Interface.	IP Aldress Pask	Une	108	vibos	
0.003.138.13			1000						ACON	10 105 100 100/04	0	0		
12.131.70		ACRIM	anat cas	10110					Inecke	20.2.2.2.294	0.00	0.0		
1 10 102		ACTIN 1	1901: 3.4	100107		ence opane: stor	THE CONTRACT OF		ineide2	10.4.4.1/24	0.0	0.0		
1.130.168 1.130.195		Press Tress	Marke Ra	uted c.em	-	antaot Plade: Single	1000, 5547 CSC 2014		outside	172.16.1.124	0.0	0 w	1	
31.194							5		Select an interface to v	ew nour and output Ibpo				
138.102		WN Dates							Failure Date					
31.138.294 06.44.154		Disc: 6		Clarificat	153, VPN: 0	AnyConnect	Clerk: Ø	Datala	Fallover not configure	6 Click the link to configure it.				Candiaga.
10.44.200		System-Re	NUMBER OF	iu;					TrafficStatus					
06.72.0		Primp	(permit)						Connections Pay Sec	nt isage				
		15 (14)-6	40 40 90 0	10.3H	10:37	-0.30		0.0	10.28 10.05 0 10	90 20 21:0 📕 Total 6	+1 30-		 	
	- 10	Planory Lk	lage (HE) -						· 'outside' Enterface To	effic Usage (Host)				5.0
		4598	#130 1030											
			500				****	********	10 C					10000
		0.45-8	0	10.98	10.37	10.38	80.30	10-48	8 10.98	10.07	+3.06	40.00	10-4	
		Details							Post Spall	Ovbutibesi 6				
	10	Mest Asi	in Systep)	Hessages										0.00
en om Bussien 1	d successfield a						ASDM logg	ing is deabled. To enable ASOPI by Drot	proj viti informational level, Re Leoping	dick the laution below.	64 J	80	(0)	1.0.00.00.00
vot configuration loads	c successfully.									000	10	COM Pro-	m 10300	13 10/40140 AM L

2. Haga clic en Next cuando llegue a la página de inicio del asistente.

🛅 Site-to-site VPN Connectio	m Setup Wizard
VPN Wizard	Introduction
	Use this staard 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.
	< Back Cancel Help

Nota: Las versiones más recientes de ASDM proporcionan un enlace a un video que explica esta configuración.

3. Configure la dirección IP del par. En este ejemplo, la dirección IP del par se establece en 192.168.1.1 en el Sitio B. Si configura la dirección IP par en el Sitio A, debe cambiarla a 172.16.1.1. También se especifica la interfaz a través de la cual se puede alcanzar el extremo remoto. Haga clic en Next una vez completada.

6659		1019 - Contra Cont		
eps	Peer Device Identificat	ion		
. Introduction	This step lets you iden	tify the peer VPN device by its IP address and the in	terface used to access the peer.	
Peer Device Identification	Peer 1P Address:	192.168.1.1		
Traffic to protect	187 8	· · · · · · · · · · · · · · · · · · ·		
Security	VPIN Access Interface:	outside	•	
NAT Exempt				
Summary				
	a Tanda Marsha			Transl Links

4. Configure las redes locales y remotas (origen y destino del tráfico). Esta imagen muestra la configuración del sitio B (lo contrario se aplica al sitio A).

Steps	Traffic to protect			
1. Introduction	This step lets you	dentify the local network and remote network betwe	en which the traffic is to be protected using IPsec encryption.	
3. Traffic to protect	Local Network:	10.2.2.0_24		
4. Security	Remote Network:	10.1.1.0_24	<u></u>	
5. NAT Exempt				
Summary				

5. En la página Seguridad, configure la clave previamente compartida (debe coincidir en ambos extremos). Haga clic en Next una vez completada.

iteps	Security	
 Introduction Peer Device Identification 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 ISA/MP secunty parameters 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 ASDN selected for you.	for
	<back next=""> Cancel</back>	Help

6. Configure la interfaz de origen para el tráfico en el ASA. El ASDM crea automáticamente la regla de traducción de direcciones de red (NAT) basada en la versión de ASA y la inserta con el resto de la configuración en el paso final. Nota: Para el ejemplo que se utiliza en este documento, 'inside' es el origen del

tr	á	f	İ	0	۱.
100	1	23	2.5	1.00	

Steps	NAT Exempt	
1. Introduction 2. Peer Device Identificatio 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	This step allows you to exempt the local network addresses from network translation. Exempt ASA side host/network from address translation inside	
	<back next=""></back>	Cancel

7. El asistente ahora proporciona un resumen de la configuración que se envía al ASA. Revise y compruebe los parámetros de configuración y, a continuación, haga clic en Finish.

Summary	
Brandh Here is the summary of the co	nfiguration.
Name	Value
Summary	
Peer Device IP Address	192.168.1.1
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
DE 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 Secre	cy (PFS) Disabled
E DKE v1	
DKE 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-30ES-SHA, ESP-30ES-MD5, ESP-0ES-SHA, ESP-0ES-MD5
E DKE v2	
IKE Policy	
IPsec Proposal	AES256, AES192, AES, 3DES, DES

Configuración a través de CLI

En esta sección se describe cómo configurar el túnel de sitio a sitio IPsec IKEv1 a través de la CLI.

Configuración del sitio B para ASA versiones 8.4 y posteriores

En las versiones 8.4 y posteriores de ASA, se introdujo la compatibilidad con IKEv1 y con la versión 2 de Intercambio de claves de Internet (IKEv2).

Sugerencia: para obtener más información sobre las diferencias entre las dos versiones, consulte la sección <u>Por qué migrar a IKEv2?</u> del documento Configuración del túnel L2L de migración rápida de IKEv1 a IKEv2 en código Cisco ASA 8.4.

Sugerencia: para ver un ejemplo de configuración de IKEv2 con ASA, consulte el documento <u>Ejemplos de configuración de sitio a sitio IKEv2 entre ASA y router de</u> Cisco.

Fase 1 (IKEv1)

Complete estos pasos para la configuración de la Fase 1:

1. Ingrese este comando en la CLI para habilitar IKEv1 en la interfaz externa:

crypto ikev1 enable outside

2. Cree una política IKEv1 que defina los algoritmos/métodos que se utilizarán para el hashing, la autenticación, el grupo Diffie-Hellman, la duración y el cifrado:

```
!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
```

 Cree un grupo de túnel bajo los atributos IPSec y configure la dirección IP del par y la clave previamente compartida del túnel:

```
tunnel-group 192.168.1.1 type ipsec-12l
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.
2 (IPcoc)
```

Fase 2 (IPsec)

Complete estos pasos para la configuración de la Fase 2:

 Cree una lista de acceso que defina el tráfico que se va a cifrar y tunelizar. En este ejemplo, el tráfico de interés es el tráfico del túnel que se origina desde la subred 10.2.2.0 a 10.1.1.0. Puede contener varias entradas si hay varias subredes involucradas entre los sitios.

En las versiones 8.4 y posteriores, se pueden crear objetos o grupos de objetos que sirvan como contenedores para las redes, subredes, direcciones IP de host o varios objetos. Cree dos objetos que tengan las subredes local y remota y utilícelos tanto para la lista de control de acceso (ACL) de cifrado como para las instrucciones 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 el conjunto de transformación (TS), que debe incluir la palabra clave IKEv1. También se debe crear un TS idéntico en el extremo remoto.

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

- 3. Configure el mapa criptográfico, que contiene estos componentes: La dirección IP del parLa lista de acceso definida que contiene el tráfico de interésEl TSUn parámetro opcional de confidencialidad directa perfecta (PFS), que crea un nuevo par de claves Diffie-Hellman que se utilizan para proteger los datos (ambos extremos deben estar habilitados para PFS antes de que aparezca la fase 2)
- 4. Aplique el mapa criptográfico en la interfaz 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

Exención de NAT

Asegúrese de que el tráfico VPN no esté sujeto a ninguna otra regla NAT. Esta es la regla NAT que se utiliza:

```
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: Cuando se utilizan varias subredes, debe crear grupos de objetos con todas las subredes de origen y destino y utilizarlas en la regla 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

Ejemplo de Configuración Completo

Esta es la configuración completa del sitio 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
```

Configuración del sitio A para ASA versiones 8.2 y anteriores

Esta sección describe cómo configurar el Sitio A para las versiones 8.2 y anteriores de ASA.

Fase 1 (ISAKMP)

Complete estos pasos para la configuración de la Fase 1:

1. Ingrese este comando en la CLI para habilitar la Asociación de seguridad de Internet y el Protocolo de administración de claves (ISAKMP) en la interfaz externa:

crypto isakmp enable outside

Nota: Dado que las versiones múltiples de IKE (IKEv1 e IKEv2) ya no son compatibles, se utiliza ISAKMP para hacer referencia a la Fase 1.

2. Cree una política ISAKMP que defina los algoritmos/métodos que se utilizarán para construir la Fase 1.

Nota: En este ejemplo de configuración, la palabra clave IKEv1 de la versión 9.x se sustituye por ISAKMP.

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

3. Cree un grupo de túnel para la dirección IP del par (dirección IP externa de 5515) con la clave previamente compartida:

```
tunnel-group 172.16.1.1 type ipsec-121
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
2 (IDooc)
```

Fase 2 (IPsec)

Complete estos pasos para la configuración de la Fase 2:

1. Similar a la configuración de la versión 9.x, debe crear una lista de acceso ampliada para definir el tráfico de interés.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

2. Defina un TS que contenga todos los algoritmos de cifrado y hash disponibles (los problemas ofrecidos tienen un signo de interrogación). Asegúrese de que es idéntico al que

se configuró en el otro lado.

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

- Configure un mapa criptográfico que contenga estos componentes: La dirección IP del parLa lista de acceso definida que contiene el tráfico de interésEl TSUn parámetro PFS opcional, que crea un nuevo par de claves Diffie-Hellman que se utilizan para proteger los datos (ambos extremos deben estar habilitados para PFS para que aparezca la fase 2)
- 4. Aplique el mapa criptográfico en la interfaz 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
```

Exención de NAT

Cree una lista de acceso que defina el tráfico que se va a eximir de las comprobaciones de NAT. En esta versión, parece similar a la lista de acceso que definió para el tráfico de interés:

```
access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
Cuando se utilizan varias subredes, agregue otra línea a la misma lista de acceso:
```

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

La lista de acceso se utiliza con NAT, como se muestra aquí:

nat (inside) 0 access-list nonat

Nota: El 'interior' aquí se refiere al nombre de la interfaz interior en la que el ASA recibe el tráfico que coincide con la lista de acceso.

Ejemplo de Configuración Completo

Esta es la configuración completa del sitio 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 10 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

Directiva de grupo

Las políticas de grupo se utilizan para definir las configuraciones específicas que se aplican al túnel. Estas políticas se utilizan junto con el grupo de túnel.

La política de grupo se puede definir como interna, lo que significa que los atributos se extraen de lo que se define en el ASA, o se puede definir como externa, donde los atributos se consultan desde un servidor externo. Este es el comando que se utiliza para definir la política de grupo:

group-policy SITE_A internal

Nota: Puede definir varios atributos en la política de grupo. Para obtener una lista de todos los atributos posibles, refiérase a la sección <u>Configuración de las Políticas de Grupo</u> de los Procedimientos de Configuración de VPN ASDM Seleccionados para Cisco ASA 5500 Series, versión 5.2.

Atributos opcionales de directiva de grupo

vpn-tunnel-protocol determina el tipo de túnel al que se debe aplicar esta configuración. En este ejemplo, se utiliza IPSec:

```
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
```

Tiene la opción de configurar el túnel para que permanezca inactivo (sin tráfico) y no se desactive. Para configurar esta opción, el vpn-idle-timeout valor del atributo debe utilizar minutos, o puede establecer el valor en none, lo que significa que el túnel nunca se desactiva.

Aquí tiene un ejemplo:

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;

default-group-policy bajo los atributos generales del grupo de túnel define la política de grupo que se utiliza para presionar ciertas configuraciones de política para el túnel que se establece. La configuración predeterminada de las opciones que no definió en la directiva de grupo se toma de una directiva de grupo predeterminada global:

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

Verificación

Utilice la información que se proporciona en esta sección para verificar que su configuración funcione correctamente.

ASDM

Para ver el estado del túnel desde el ASDM, navegue hasta Monitoring > VPN. Esta información se proporciona:

- La dirección IP del par
- El protocolo que se utiliza para construir el túnel
- Algoritmo de cifrado que se utiliza
- · La hora a la que se activó el túnel y el tiempo de actividad
- El número de paquetes que se reciben y se transfieren

Sugerencia: haga clic en Refresh para ver los últimos valores, ya que los datos no se actualizan en tiempo real.

and the second second		and the second							-
arris 🔄 Sire i	Acton Obsi	Chanter 3 400							_
indiating is VIII.a	MR Stateline > Serie	lers.							
For		SSL VPN				A Constants	i a company a	1.22	
Ramatia	Site-to-Site	Gertless	Vith Clert	Institut	Total	E-mail Proce	VPII Loed Balancing	Total	Cursula
0	1		0	0	0	0	0	1	2
-				(Lawson)					
Friter By: [JFast Set	1-ID-SINE •	- Al Sesione -		[LODELA]					
P Address	Engraption	Duration		Bytes Ra					
22.411	401000	in the Sta	140-01311	-					
to port UPN assessme	which the second second	while and aslant Table Story ()	inder from popular menu.						
	The second se		a second s						
Lagent By: All S	anima - +	16	Legeul Gentere						
Legent for (All S			Legent Senters						
laged for (mALS) (J	Legisl Genters		falsah				
Lagast Byr Landi S			Legent Services		_tabat.		6100 E	1.2.199	-Les Upday
Logist for Looks	antera — •		Legnal Sentern		. talah		joses ji	9	Last Updat
ingent for and b	amora — •]]		Legent Services		. talah		0000 [2		Let Upder
Help	andera		.goul Bostern	_	. Rafaat		jones ja	Trate taok its sourch	Last Update
High the sales	Anteresk Q local	Ofreed 2 Ho	.goul Bostern	_	. Forback		jana ji	Vere Now Is search	Les Upder
Help Help Received to 1983	 A leftesh Q lost Tift Statistica = Second 	Offerended ? Hebe	regnal Santiers	_	. shat.		jasa ji	Vite 100K to scored	
Help Help Reference VIII a	 Actros O 1001 This Statution > Second 	O Poread ? Hote	regnal Tantiers	12212	falset.		jow jt	Frat tox is sourch	
Help Help Type Type	 A leftedi Q lost Titt Statulita - Senat 	O Forward ? Hole	regnal Tantinn	Canaletree	Talash.	PaskGroutert	joo ji	Fore tax. Is sourch	
Help Help Type Arto-Star (9) 30-1 (Fee:	 A lefted Q lost The State of Law 2 	O Forward ? Hole	regnal Tantinn	Candebre 1	Talash.	Peek Concernent 41 41	joo ji	France Nox. 19 yearsh	-Lex Upder
Help Help Type Ra-to-Star USL a Sto-to-Star USL a	3 fettest Q loss	Offerende ? Hole and Active	regnal Tantinn	Canaletine 2	Talash.	Peak Cancerent 41 41	jana ji	Viet Kox. Is sourch	
Help Help Trag and Star (1996) Alter Star (1996) Alter Star (1996)	3 fetted Q loss	O Poresad ? Hole mai	Ingenil Section	Canaletine 2	Talash.	Peek Concernent 41 41	jose ji	Viet Korr. Is sourch	
Help Help Trag (g) Store (g) Antonious 2 ATE (a Antonious 2 ATE (a Antonious 2 ATE (a Antonious 2 ATE (a Antonious 2 ATE (a) Antonious 2 ATE (a) ATE (a) A	 A leftedi Q lock Trittichilita - Serat Social - Serat 	Athen	regnal Section	Candobre 1	Talash.	Peek Concernent 44 41	jose jr	France Hook, Bry Sourch	
Help Help Type Type The choice is ATE is Type The choice is ATE is Type The choice is ATE is The choice is ATE is ATE is The choice is ATE is ATE is ATE is ATE is	 A fecteuri Q book The Stational tax = Second Socialis + 1 	Affree	regnal Section	Candebre 3 2 PVCS TX	Talash.	Peak Concurrent 44 41	joo ji	Viet Kox, Is sourch	
Halp Halp Halp Tree Rest-Stat (PA) 30% (The: 186% (PA) 40% (PA) 40	andre • •	Active	regnal Sentirm	Canalative 1 1 Mate (Mate () Note ()	Talash	Peik Concurrent 41 41	joes ja	Viet Kor & sourch	Les upde
Help Help Help Tree Rest-Stat (PAL Bible (PAL Bible (PAL Bible (PAL Palameter Hard by: Breestate Thard by: Breestate Hard by: Breestate	anders - +	Active ctive Active A	- egent Sentitre	Canalative 1 1 Notes To: Notes To: Notes To:	. tatisat.	Peek Concurrent 44 41	jose ja	Vert Nor: D your ch Inclus 3 3	- Les locks
Here and a second secon	Andrea () A tetrest () took TTT Statistics = Second Andrea () Andrea ()	Attre	- equal Section	Candabae 3 2 Protection Protectio	. talaat.	Peek Concernent 44 41	jose 2	Not have been on	
Here and a second secon	Andrea () A tetrest () This Statistical is a Second Statistical is a Second This Statistical is a Second Second () Price of the Second () Price	Active	- equival Exercision (c)	Consistive 2 2 Process for Process for Pro	. Rainak	Peek Concurrent 4 11	jose jr	Not too bearch	
Han the Last S Han The Last S Han The Sec 4 Han The Sec 4	Andrea () A fect cat	Active	Apr 17.2311	Considere 2 3 Procession Processi	Tarinak.	Pask Concernent 4 1	jose j	Vice tox: is sorth	
Help Help Type Sate-Sate Vitt - Type Sate-Sate Vitt - Type Sate-Sate Vitt - Packerson Packerson Packerson	audera () audera ()	Active Active Active M Secures - Upp Toto Toto: () Active M Secures -	Apr 172111	Canaletre 1 3	Tarinah.	Pail Crosser 41 11	jose : jr	Viet tox to search	
Help Help Type and the State S	anders	Active Ac	negrad Renderm	Camiletine 3 3 Protect Tax Protect Tax	Tailant	Pail Crosser 4 1	jose : jt	Fort tox: to scarch	
Help Help Help Trag and and the AME is An American AME is An American AME is A American AME is A American Ameri	existen	Active	AP 17.2111	Camaletre 1 3 Protes To Protes To Protes To	Tailait	Pail Concentral 41 41	jose jr.	Fore tox: is sourch	
Help Help Help Trag () Store () Antiothese - MTE () Trag Antiothese - MTE () Help Help Store () Antiothese - MTE () Help Store () Antiothese -	extensi	Active	AP 17211	Canalative 2 2 Protect To Receiption	Tailait	Peit Concurrent 41 41	joes 2	Fore tox: is sourch	
Help Help Help Trans Que Carlos - MEL Andres - MEL Help Startes - MEL	extensi	Active	- egent Sectors	Canalative 2 2 Protect To Receiption	Tailait	Peit Concentral 41 41	jose 2	Fore tox: is sourch	
Help Help The and the second s	extension + +	Attre	- equal Sectors -	Consistence 2 2 Procession Proces		Peek Concurrent 44 41	jose jr	Fore tox: is sourch	
High High High Tray Rest-Station Rest-Rest-Rest-Rest-Rest-Rest-Rest-Rest-	Andrea () A tetrest () A tet	Active	- equal Section	Considere 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Peek Concernent 44 41	jose 2	Not tax to servit	
Help Help Help Tree Rest-Station - Mile Rest-Station There Patheres There Str. Helpschilt Patheres There Str. Helpschilt Patheres	Andrea () A tetrest () A tet	Active	Apr 10.2311	Consistive 2 3 Protection		Peek Concernent 44 11		Inclus 3 3	
Help Help Type Antonious - VITE - Type Antonious - VITE - Type Antonious - VITE - Type Antonious - VITE - Pactorias - Pactorias - Pactorias -	Andrew () A fect cal	Active	Apr 17.2311	Canalebre 2 3 Wees To Newson To News		Peek Concurrent 4 11		Prote toxic is reservit.	
Help Help Type and the ATT - Type and the ATT - Type the ATT - P Address Att - Type Addre	anders () () () () () () () () () () () () ()	Active Active Active M Secures - Upp Toto France (1) Active Active	Apr 172111	Considere 1 3 Notes To Notes To		Pask Concernent 41 41		Viet tox to solv th Detter 3 3	

tora hereshed SuccessMy.

ingout By: -- Al Sessons

CLI

En esta sección se describe cómo verificar la configuración mediante la CLI.

Legent Sessions

Fase 1

Ingrese este comando en la CLI para verificar la configuración de la fase 1 en el lado del sitio B (5515):

Refresh

😹 🖬 🔰 👔 👘 Marca poseserence

```
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

Ingrese este comando en la CLI para verificar la configuración de la fase 1 en el lado del sitio 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

show crypto ipsec sa muestra las SAs IPsec que se construyen entre los peers. El túnel cifrado se construye entre las direcciones IP 192.168.1.1 y 172.16.1.1 para el tráfico que fluye entre las redes 10.1.1.0 y 10.2.2.0. Puede ver las dos SA ESP creadas para el tráfico entrante y saliente. El Encabezado de autenticación (AH) no se utiliza porque no hay SA AH.

Ingrese este comando en la CLI para verificar la configuración de la Fase 2 en el lado del Sitio 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:
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
```

Ingrese este comando en la CLI para verificar la configuración de la Fase 2 en el lado del Sitio A (5510):

```
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
```

Troubleshoot

Utilice la información que se proporciona en esta sección para resolver problemas de

configuración.

ASA versiones 8.4 y posteriores

Ingrese estos comandos debug para determinar la ubicación de la falla del túnel:

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

Aquí hay un ejemplo completo de resultado de debug:

```
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 pavload 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 : 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 guick 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 SPT: 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)

Ingrese estos comandos debug para determinar la ubicación de la falla del túnel:

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

Aquí hay un ejemplo completo de resultado de debug:

```
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 pavload 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 SPT : 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 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 : 172Feb 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 = 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: 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)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).