# Configurazione dei tunnel IPsec IKEv1 da sito a sito con ASDM o CLI sull'appliance ASA

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Esempio di rete Configurazione mediante la procedura guidata VPN ASDM Configurazione dalla CLI Configurazione del sito B per ASA versione 8.4 e successive Configurazione del sito A per ASA versione 8.2 e precedenti Criteri di gruppo Verifica **ASDM** CLI Fase 1 Fase 2 Risoluzione dei problemi ASA versioni 8.4 e successive ASA versioni 8.3 e precedenti

# Introduzione

In questo documento viene descritto come configurare un tunnel IPsec Internet Key Exchange versione 1 (IKEv1) tra un'appliance Cisco Adaptive Security Appliance (ASA) serie 5515-X con software versione 9.2.x e un'appliance ASA Cisco serie 5510 con software versione 8.2.x.

# Prerequisiti

# Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Ènecessario stabilire la connettività IP end-to-end
- Devono essere consentiti i seguenti protocolli: UDP (User Datagram Protocol) 500 e 4500 per il control plane IPsecProtocollo IP 50 Encapsulating Security Payload (ESP) per il piano dati IPsec

# Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5510 ASA con software versione 8.2
- Cisco 5515-X ASA con software versione 9.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

In questa sezione viene descritto come configurare il tunnel VPN da sito a sito tramite la procedura guidata Adaptive Security Device Manager (ASDM) VPN o tramite la CLI.

# Esempio di rete



Questa topologia viene utilizzata per gli esempi riportati in questo documento:

# Configurazione mediante la procedura guidata VPN ASDM

Completare questi passaggi per configurare il tunnel VPN da sito a sito tramite la procedura guidata ASDM:

1. Aprire ASDM e passare a 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	Million Martine Martine Carries S2, VM Martine Million S2, VM Martine Martine Millionity Carlinate Wash. Proc (REA) Render Access VM Martine												
del 👔 Celata	ASDEM Salare									Interface Status				
and the second	Paulot Capt	Are Wisse	4.		to ave (name) -	CONTRACTOR OF CONTRACTOR			Interface.	IP Aldress Pask	Une	108	vibos	
0.003.138.55			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		
<ul> <li>30, 303, 130, 168</li> <li>30, 305, 130, 195</li> </ul>		Home results and a service and a service servi					outside	172.16.1.124	0.0	<b>0</b> w	1			
31.194		Indiana steres economy stering						Select an interface to view input and output itbpo						
- S 10.105.130.332		WN Dates							Fallove Data					
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;					Traffic Status					
06.72.0		O's stop berant					Connections Pay Second Licege							
		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	Henory Llage (HE)							Installer Interface Traffic Usage Blass					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	
		bends					Post Spall	Ovbutibesi 6						
	10	Latest 2600 Sector Researce						Del					10 0 0 0	
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	30	(0)	1.0.00.00.00
vot configuration loads	c successfully.									000	10	COM Pro-	m 10300	13 10/40140 AM L

2. Clic Next una volta raggiunta la home page della procedura guidata.

🚡 Site-to-site VPN Connectio	vn Setup Wizard
VPN Wizard	Introduction
	Use this worard to setup new site-to-site VPN turnel. A turnel between two devices is called a site-to-site tunnel and is bidrectional. A site-to-site VPN turnel protects the data using the Disc protocol.
	< Back Cancel Help

**Nota**: le versioni ASDM più recenti forniscono un collegamento a un video che spiega questa configurazione.

3. Configurare l'indirizzo IP del peer. In questo esempio, l'indirizzo IP del peer è impostato su 192.168.1.1 sul Sito B. Se si configura l'indirizzo IP del peer nel Sito A, deve essere modificato in 172.16.1.1. Viene inoltre specificata l'interfaccia attraverso la quale è possibile raggiungere l'estremità remota. Clic Next una volta completato.

iteos	Peer Device Identificat	ton		
1. Introduction	This step lets you ident	tify the peer VPN device by its IP address and the int	terface used to access the peer.	
2. Peer Device Identification	Peer IP Address:	192.168.1.1		
<ol> <li>Traffic to protect</li> <li>Security</li> </ol>	VPIN Access Interface:	outside	•	
. NAT Exempt				
5. Summary				

4. Configurare le reti locali e remote (origine e destinazione del traffico). Questa immagine mostra la configurazione per il Sito B (il contrario si applica al Sito A).

2D6	Traffic to protect			
Introduction Peer Device Identificatio	This step lets you	dentify the local network and remote network betwe	en which the traffic is to be protected using IPsec encryption.	
. Traffic to protect	Local Network:	10.2.2.0_24		
Security	Remote Network:	10.1.1.0_24		
NAT Exempt				
Summary				

5. Nella pagina Protezione configurare la chiave già condivisa (deve corrispondere su entrambe le estremità). Clic Next una volta completato.

iteps	Security	
<ol> <li>Introduction</li> <li>Peer Device Identificatio</li> <li>Traffic to protect</li> <li>Security</li> <li>NAT Exempt</li> <li>Summary</li> </ol>	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 ISAKMP security parameters for 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 ASDM selected for you.	
	<back next=""> Cancel H</back>	de

6. Configurare l'interfaccia di origine per il traffico sull'appliance ASA. L'ASDM crea automaticamente la regola NAT (Network Address Translation) basata sulla versione ASA e la inserisce con il resto della configurazione nel passaggio finale. **Nota**: nell'esempio riportato nel documento, 'inside' è l'origine del

traffico.

Steps	NAT Exempt	
<ol> <li>Introduction</li> <li>Peer Device Identificatio</li> <li>Traffic to protect</li> <li>Security</li> <li>NAT Exempt</li> <li>Summery</li> </ol>	This step allows you to exempt the local network addresses from network translation.	
	< Back Next >	Cancel Help

7. La procedura guidata fornisce ora un riepilogo della configurazione trasferita all'appliance ASA. Controllare e verificare le impostazioni di configurazione, quindi fare clic su Finish.

Summary		
Branch Here is the	summary of the configuration.	
Name		Value
Summ	ary	
Peer De	evice IP Address	192,168, 1, 1
HORM VPN AC	cess Interface	outside
Protect	ted Traffic	Local Network: 10.2.2.0/24 Remote Network: 10.1.1.0/24
JKE Ver	sion Allowed	IKE version 1 and IKE version 2
Authen	tication 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
Encryp	tion Policy	
Perl	fect Forward Secrecy (PFS)	Disabled
DKE	ν1	
	IKE Policy	pre-share-aes-sha
	Psec Proposal	ESP-AE5-128-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 IKE	v2	
1	IKE Policy	
1	Psec Proposal	AE5256, AE5192, AES, 3DES, DES

## Configurazione dalla CLI

In questa sezione viene descritto come configurare il tunnel IPsec IKEv1 da sito a sito tramite la CLI.

### Configurazione del sito B per ASA versione 8.4 e successive

Nelle versioni ASA 8.4 e successive è stato introdotto il supporto per IKEv1 e IKEv2 (Internet Key Exchange versione 2).

**Suggerimento**: per ulteriori informazioni sulle differenze tra le due versioni, fare riferimento alla sezione <u>Perché migrare a IKEv2?</u> nel documento Cisco relativo alla migrazione rapida di IKEv1 a IKEv2 L2L Tunnel Configuration su ASA 8.4 Code.

**Suggerimento**: per un esempio di configurazione IKEv2 con l'appliance ASA, consultare il documento Cisco sugli <u>esempi di configurazione del tunnel IKEv2 da sito a sito tra</u> <u>l'appliance ASA e il router</u>.

## Fase 1 (IKEv1)

Completare i seguenti passaggi per la configurazione della fase 1:

1. Immettere questo comando nella CLI per abilitare IKEv1 sull'interfaccia esterna:

#### crypto ikev1 enable outside

2. Creare un criterio IKEv1 che definisca gli algoritmi o i metodi da utilizzare per l'hashing, l'autenticazione, il gruppo Diffie-Hellman, la durata e la crittografia:

```
crypto ikev1 policy 1
!The 1 in the above command refers to the Policy suite priority
(1 highest, 65535 lowest)
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. Creare un gruppo di tunnel con gli attributi IPsec e configurare l'indirizzo IP del peer e la chiave precondivisa del tunnel:

```
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.
? (IPecc)
```

#### Fase 2 (IPsec)

Completare i seguenti passaggi per la configurazione della Fase 2:

 Creare un elenco degli accessi che definisca il traffico da crittografare e tunneling. Nell'esempio, il traffico di interesse è il traffico proveniente dal tunnel che ha origine dalla subnet 10.2.2.0 fino a 10.1.1.0. Può contenere più voci se tra i siti sono coinvolte più subnet.

Nelle versioni 8.4 e successive, è possibile creare oggetti o gruppi di oggetti che fungono da contenitori per le reti, le subnet, gli indirizzi IP dell'host o più oggetti. Creare due oggetti che hanno le subnet locale e remota e usarli sia per l'elenco di controllo di accesso (ACL) crittografico che per le istruzioni 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. Configurare il set di trasformazioni (TS), che deve includere la parola chiave IKEv1. È necessario creare un servizio di terminal identico anche sull'estremità remota.

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

- Configurare la mappa crittografica, che contiene i seguenti componenti: Indirizzo IP peerL'elenco degli accessi definito che contiene il traffico di interesseTSImpostazione PFS (Perfect Forward Secrecy) facoltativa che crea una nuova coppia di chiavi Diffie-Hellman utilizzate per proteggere i dati (entrambi i lati devono essere abilitati PFS prima dell'attivazione della Fase 2)
- 4. Applicare la mappa crittografica sull'interfaccia esterna:

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

#### **Esenzione NAT**

Verificare che il traffico VPN non sia soggetto a nessun'altra regola NAT. Regola NAT utilizzata:

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

**Nota**: quando si utilizzano più subnet, è necessario creare gruppi di oggetti con tutte le subnet di origine e di destinazione e utilizzarli nella regola 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

#### Completa configurazione di esempio

Di seguito è riportata la configurazione completa per il sito 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
```

### Configurazione del sito A per ASA versione 8.2 e precedenti

In questa sezione viene descritto come configurare il sito A per ASA versione 8.2 e precedenti.

### Fase 1 (ISAKMP)

Completare i seguenti passaggi per la configurazione della fase 1:

1. Immettere questo comando nella CLI per abilitare Internet Security Association and Key Management Protocol (ISAKMP) sull'interfaccia esterna:

crypto isakmp enable outside

**Nota**: poiché più versioni di IKE (IKEv1 e IKEv2) non sono più supportate, per fare riferimento alla fase 1 viene utilizzato ISAKMP.

2. Creare una policy ISAKMP che definisca gli algoritmi/i metodi da utilizzare per compilare la Fase 1.

**Nota**: in questa configurazione di esempio, la parola chiave IKEv1 dalla versione 9.x è sostituito con ISAKMP.

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

3. Creare un gruppo di tunnel per l'indirizzo IP peer (indirizzo IP esterno di 5515) con la chiave già condivisa:

```
tunnel-group 172.16.1.1 type ipsec-121
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
```

#### Fase 2 (IPsec)

Completare i seguenti passaggi per la configurazione della Fase 2:

1. Analogamente alla configurazione della versione 9.x, per definire il traffico di interesse è necessario creare un elenco degli accessi esteso.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

2. Definire un TS contenente tutti gli algoritmi di crittografia e hash disponibili (i problemi offerti hanno un punto interrogativo). Accertarsi che sia identico a quello configurato sull'altro lato.

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

- Configurare una mappa crittografica contenente i seguenti componenti: Indirizzo IP peerL'elenco degli accessi definito che contiene il traffico di interesseTSImpostazione PFS facoltativa, che crea una nuova coppia di chiavi Diffie-Hellman utilizzate per proteggere i dati (entrambi i lati devono essere abilitati per PFS in modo che venga visualizzata la Fase 2)
- 4. Applicare la mappa crittografica sull'interfaccia esterna:

```
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
```

#### **Esenzione NAT**

Creare un elenco degli accessi che definisca il traffico da esentare dai controlli NAT. In questa versione, l'elenco è simile all'elenco degli accessi definito per il traffico di 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 Se si utilizzano più subnet, aggiungere un'altra riga allo stesso elenco degli accessi:

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

L'elenco degli accessi viene utilizzato con il NAT, come mostrato di seguito:

nat (inside) 0 access-list nonat

**Nota**: il valore 'inside' qui si riferisce al nome dell'interfaccia interna sulla quale l'ASA riceve il traffico che corrisponde all'elenco degli accessi.

#### Completa configurazione di esempio

Di seguito è riportata la configurazione completa per il sito 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 match address 100
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
10.2.2.0 255.255.0
nat (inside) 0 access-list nonat

#### Criteri di gruppo

Per definire impostazioni specifiche per il tunnel, vengono utilizzati Criteri di gruppo. Questi criteri vengono utilizzati in combinazione con il gruppo di tunnel.

I Criteri di gruppo possono essere definiti come interni, ovvero gli attributi vengono estratti da quelli definiti sull'appliance ASA, oppure come esterni, ovvero gli attributi vengono estratti da un server esterno. Questo è il comando utilizzato per definire i Criteri di gruppo:

#### group-policy SITE\_A internal

**Nota**: è possibile definire più attributi in Criteri di gruppo. Per un elenco di tutti gli attributi possibili, fare riferimento alla sezione <u>Configurazione dei criteri di gruppo</u> delle procedure di configurazione della VPN ASDM selezionate per Cisco ASA serie 5500, versione 5.2.

#### Attributi facoltativi di Criteri di gruppo

OSPF (Open Shortest Path First) vpn-tunnel-protocol determina il tipo di tunnel a cui applicare queste impostazioni. Nell'esempio viene usato 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

Èpossibile configurare il tunnel in modo che rimanga inattivo (nessun traffico) e non si blocchi. Per configurare questa opzione, è necessario vpn-idle-timeout il valore dell'attributo deve essere espresso in minuti oppure è possibile impostare il valore su none, il che significa che il tunnel non scenderà mai.

Di seguito è riportato un esempio:

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;

OSPF (Open Shortest Path First) default-group-policy in attributi generali del gruppo di tunnel vengono definiti i criteri di gruppo utilizzati per eseguire il push di determinate impostazioni dei criteri per il tunnel stabilito. Le impostazioni predefinite per le opzioni non definite nei Criteri di gruppo sono derivate da un criterio di gruppo predefinito globale:

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

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

# ASDM

Per visualizzare lo stato del tunnel da ASDM, passare a Monitoring > VPN. Queste informazioni sono fornite:

- Indirizzo IP peer
- Protocollo utilizzato per compilare il tunnel
- Algoritmo di crittografia utilizzato
- L'ora in cui è stato realizzato il tunnel e il tempo di attività
- Numero di pacchetti ricevuti e trasferiti

Suggerimento: fare clic Refresh per visualizzare i valori più recenti, poiché i dati non vengono aggiornati in tempo reale.

ing sort (	A Select C Block								
A REAL PROPERTY OF A REAL PROPER	Contraction of the second	Chanter A uso	1						
othering in VTB.2.5	173 Statelits > Scenic	(FR. )							
Porc.		SSL VPN				A DEPOSIS		1.00	
Namella Access	Site-to-Site	Gertless	With Client	listive	Total	EnelProv	VPII Load Balancing	Total	Cursulati
<u> </u>	1	1	0	0	0	0	0	1	2
Nor Iv: URec.Ste-	-to Site -	- Al Seatore -	-	Cone					
Connector Profile	Pretocol	Logn Time		Eves 1x					
IP Address	Encryption	Duration	Avenue:	Bytte Ro					
2.4.11	401-130	Ry Lines Sta		40					
o port VPN memoria, r	right-click on the above ta	ble and select Table Sort G	der fron popus nerv.						
Agent for Land See		1.2	ADATA CARBONN						
					and an an an and a second s				
					taliah				Liez Updated
					tabah		000 2		Last Updated
					talaat		000 J	8	Let Updated
14					. Rafush		jose )1		Let Update
Help				_	faint		ione 1	We tak b seron	
Pada Talago Carto (C	letes Otox (	Ormand 🦻 may		_	falsah		joes (2	Five for to send	Les Lpdered
Help To Dave Qu Restor - 1171 - 11	a forest 🗿 sax (	Ormed ? He		_	Taluh		joes jz	First fact is servit	Les Lipderes
	a tetres O tax (	Orward ? rep at		Quality	Talut	Pair Concernet	jose ji	five tax b sort	Les Uptres
Hels Hels Soc Q Horiso - VIII - 11 pr s-to-Sis 191	a teres O tos (	O forward 💡 inde ex Active		Canakter	Tainah	Paik Document 41	jose ji	Free tox: b sorron	Les Uptrest
Help Help Tarden - Vill - V et-Site Vill ICvi Dec	> terest O tox ( TR31stitutes - Sensite	Onevent ? into ak		Canalabae 2	. Rainah	Paik Decement 41 41	jose ji	Fire tax b serve	Les Lipderes
Help Help Torden - VIII - 11 pr pr - Sta-Sta (P) NDv1 (Prec	\$ totos ( O tos ( TR Statistica - Sanata	Onevand ? into ax Active		Canaldre B	Tainah	Pak Dromet 41 41	jose ji	Fire tax b sort	Les Updared
Help Participation - Vitta - 11 Participation - 11 Participatio - 11 Participation - 11 Participation	Sectors O tox ( TR Statistics - Sector	Onevent ? into ax Active		Canalabae B	Tainah	Paik Concent 41 41	jos j	Fire tox b serve	Les Lipolees
Help Participation (C) Participation (C) Partici	S tetes O tos ( TR Statistics - Sensite 0.036 • /	At the second se		Canalabiae 2 1	Tainah	Pak Cronert 41 41	jose ji	Port fact to server	
Help To Control of the second second of the second of th	<ul> <li>terest o tos (</li> <li>tereste</li> <li>tereste</li> <li>tereste</li> <li>tereste</li> </ul>	Ather	•	Canaletre 2 1 Priter (1)	Tainah	Peek Concernent 44 45	joe j	Part los: b ser di	
Help The Source Con- pro- set-Sta (Pin HC+1 (Prec) Ter Cy: Desc Star (Con- precision Hundle Precision Hundle Precision Hundle	<ul> <li>Antreal (2) 100.1 (1)</li> <li>Constraints - Second Constraints - Second Con</li></ul>	Ather	•	Consistre 1 1 Statis To Notes To Notes To	Taitadh	Pesk Circurset 41 41	joe jr	Inclus 1	
Help Help To Some Q Some NML = 1 Help ( Decision - MML = 1 Help ( Decision - MML = 1 Help ( Decision - MML = 1 Pactores Pactores Pactores	<ul> <li>Anteriori Data (</li> <li>Anteriori Secondaria)</li> <li>Anteriori Secondaria</li> <li>Anteriori Secondaria</li></ul>	Active Costs Costs	v 12111 -	Consistere 2 2 Price To Broos Ro Price To Broos Ro	Taihadh	Pask Concenter 41 11	joe ji	Inclus 1	
Help Help Tag Sone Q Interfere 2 VIII = 1 Per Interfere 2 VIII = 1 Per	<ul> <li>Actes</li> <li></li></ul>	Active Ac	• •	Considere 2 2 State To State To State To State To	Reineh	Pail Croster 4 1	jose j	Not fail to solve	
Help Help Tag Store (C and actions 2: VISE = 1 Pro- In- 1 (Pro- In- 1) (Pro- In	<ul> <li>Notice State</li> <li>Notice State</li> <li>Notice State</li> <li>Notice State</li> </ul>	Active Ac	<ul> <li>(1)</li> <li>(1)</li> <li>(2)</li> <li>(3)</li> <li>(4)</li> <li>(5)</li> <li>(5)</li> <li>(6)</li> <li>(7)</li> <li>(7)</li></ul>	Canddre 2 3 Mos N Mos N	Reinel	Park Concernent 41 41	jose : jr	Port Nor. 5 servin	
Help Torton I- VPU - V Torton I- VPU - V Torton I- VPU - V Torton I- VPU I- VPU I	Internet i to acceleration     Sectore      Sectore     Secto	Active Active Active Al Security - Logistics Active Al Security - Constant Const Active	P 1231	Canaldone 2 2 Notes To Notes To Notes To	Reinek	Pair Concerner 41 41	joe j	Protine Disord	
Hela Torona Contraction of the	<ul> <li>Interior into a loss (</li> <li>Interior into a loss interior interior into a loss interior interio interior interior interior interior interior</li></ul>	Active		Camaletre 2 3 Distance Price To Price To	Reinek	Pak Dronert 41 41	joe j	Fire too: b servit	
Help Help To Control of the Help State (Control Help State (Control	Antreal ( ) 100 1	Active Active Active Al Deserve - Logis Tree Deserved Active Al Deserve -	9 10.111	Canalabas 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Tainah	Pak Cronert 41 41		Port loc biseron	
Help To Deve C To deve - MEL = 1 yer ne-to-Sta VPi HE-1 (Proc Deve Sta VPi P Alteres P Alteres P Alteres	<ul> <li>Antreal (2) tool (1)</li> <li>Antreal (2) tool (2)</li> <li>Antreal (2)<td>Ather Ather Al Secure - Logit The Desition Call</td><td>yr 102811 -</td><td>Canaletre 2 3 Softer To Notes To Notes To Notes To Notes To Notes To</td><td>Reineh</td><td>Peek Concernent 41 41</td><td></td><td>Port los: lo ser di</td><td></td></li></ul>	Ather Ather Al Secure - Logit The Desition Call	yr 102811 -	Canaletre 2 3 Softer To Notes To Notes To Notes To Notes To Notes To	Reineh	Peek Concernent 41 41		Port los: lo ser di	
Help Tag Sone (C Sone - ME = 1 yes introdes - ME =	<ul> <li>Antical Dista ( IN Statutica &gt; Securitar Distance - I ~ Priston Provinsion</li> </ul>	Active Active Active Additional - Logis The Database Control of the Control Database	v 19.711	Canaletre B 3 Mitter for Mitter for Mitter for Mitter for Mitter for	Reinek	Peek Concentrat 41 41	jose j	Pore los: lo serviti	
Help Help To Some Q Interdent - MTE = 1 yer interd-Sta VPin HE-1 (Prec) Interdy: IPrec) Interd P address To State 1	<ul> <li>Antical Distance</li> <li>Bandardista</li> <li>Ban</li></ul>	Active	SF 10.711	Consister 1 1 1 1 1 1 1 1 1 1 1 1 1	Rainah	Paik Concerner 4 1	jose j	Pore los: lo serviti	
Help Help To Some C Some NUM = 1 Help to Some Help to Some Description Harding Protocols Description Harding Description Harding Descriptio	<ul> <li>Antron Distance</li> <li>Antron Science</li> <li>Antron Science</li> <li>Antron Science</li> <li>Antron Science</li> <li>Antron Science</li> </ul>	Active Active Active Upget The Upget	9 10.211	Considere 2 2 Mitter To Mitter To	Reinsh	Pel Croster 4 1	jose : j	Norther a starter	
Help Help Torriso Le VII Le V PP Redo-Sta UN BC 1 Dec Iner Dy: Enerclase 6 precision from P ANTHONE P ANTHONE P ANTHONE P ANTHONE	<ul> <li>Actes</li> <li>Sector</li> <li>Sector</li></ul>	Active	<ul> <li>• 1</li> <li>• 1</li></ul>	Canddre I I Mites N Mites N	Reineh	Peé Crosrer 4 1		Port Nor. D rear Or	

## Fase 1

Tranting

S. rours

CLI

tara Refreshed SuccessMix

To set 9

inquitity - Al Sessors

Immettere questo comando nella CLI per verificare la configurazione della fase 1 sul lato sito B (5515):

Refresh

😹 🖬 🕴 👔 🖓 ANDALE BADA REPORTED

t Order From pop

Questa sezione descrive come verificare la configurazione tramite la CLI.

Logout Sessions

```
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
```

Immettere questo comando nella CLI per verificare la configurazione della fase 1 sul lato sito A (5510):

show crypto isakmp sa

Rekey : no State : MM\_ACTIVE

```
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
```

#### Fase 2

OSPF (Open Shortest Path First) show crypto ipsec sa II comando mostra le SA IPsec generate tra i peer. Il tunnel crittografato è costruito tra gli indirizzi IP 192.168.1.1 e 172.16.1.1 per il traffico che scorre tra le reti 10.1.1.0 e 10.2.2.0. È possibile visualizzare le due associazioni di protezione ESP create per il traffico in entrata e in uscita. L'intestazione AH (Authentication Header) non viene utilizzata perché non sono presenti associazioni di protezione AH.

Immettere questo comando nella CLI per verificare la configurazione della fase 2 sul lato sito 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
```

Immettere questo comando nella CLI per verificare la configurazione della fase 2 sul lato sito 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
```

# Risoluzione dei problemi

Utilizzare le informazioni fornite in questa sezione per risolvere i problemi di configurazione.

### ASA versioni 8.4 e successive

Immettere questi comandi di debug per determinare la posizione dell'errore del tunnel:

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

Di seguito è riportato un esempio completo dell'output del comando 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)

Immettere questi comandi di debug per determinare la posizione dell'errore del tunnel:

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

Di seguito è riportato un esempio completo dell'output del comando 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)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).