Configurer des tunnels de site à site IPsec IKEv1 à l'aide de l'ASDM ou de la CLI sur l'ASA

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Diagramme du réseau Configuration via l'assistant ASDM VPN Configuration via l'interface CLI Configuration du site B pour ASA versions 8.4 et ultérieures Configurer le site A pour ASA versions 8.2 et antérieures Stratégie de groupe Vérifier **ASDM** CLI Phase 1 Phase 2 Dépannage ASA versions 8.4 et ultérieures ASA versions 8.3 et antérieures

Introduction

Ce document décrit comment configurer un tunnel IPsec site à site d'échange de clés Internet version 1 (IKEv1) entre un dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5515-X qui exécute la version 9.2.x du logiciel et un ASA de la gamme Cisco 5510 qui exécute la version 8.2.x du logiciel.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connectivité IP de bout en bout doit être établie
- Ces protocoles doivent être autorisés : Protocole UDP (User Datagram Protocol) 500 et 4500 pour le plan de contrôle IPsecEncapsulating Security Payload (ESP) IP Protocol 50 pour le plan de données IPsec

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA de la gamme Cisco 5510 qui exécute la version logicielle 8.2
- Cisco 5515-X ASA qui exécute le logiciel version 9.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Cette section décrit comment configurer le tunnel VPN site à site via l'assistant VPN ASDM (Adaptive Security Device Manager) ou via l'interface de ligne de commande.

Diagramme du réseau



Cette topologie est utilisée pour les exemples de ce document :

Configuration via l'assistant ASDM VPN

Complétez ces étapes afin de configurer le tunnel VPN site à site via l'assistant ASDM :

1. Ouvrez l'ASDM et accédez à Wizards > VPN Wizards > Site-to-site VPN Wizard.

25511 74 tor 4	-2011/51/2010		8
Teols Wr	rða Wandow Halp	We top to sew dy to a set of the	
curt_	Satup Wised. Desc Provid Vice	CISCO	5
	VPN Meands Sterio sile VTN Waard.		÷.
	High Arailability and Scalability Woard		
3	Unified Conversariation Woord Citerates 532, VPN Waard	No. 1. West	5
-	ASDM Identity Calificate Wiend. IPsec (REd.) Remote Access VPN Waterd.	APPROVED AND A APPROVED AND APPROVED APPROVED AND APPROVED APPRO	
3	Panlart Capiture Wissend.	Interface IP Aldress/Next Line Line Kape	4
	Helliane: demana	400H 30.105.100.1002H Q up 0 up 1	4
	ASA Version: 9.8(5)29 Device liptine: S6d 7b 44m 0s		4
	ADMINESON 74(1) Devic Type ASA 5530, 55H CSC-30-49	0.00 12161124 Out Out	
	Presel Mode: Rauted Eastast Hode: Single		1
	Tatal Rock: ZSE MB BOOM BOOM PROVI ZBEE MB	Select an interface to view reput and output that	1
	WTI Sectors	Padros Dalus	Ē.
1	Disc: # Clerifies:03. Whit # AnyConnect Clerit: # Datable	Palore rationfipunt. Old the life to configure h. Candhaer	ι.
	System-Annual Series	Trafficiana	
	(Pi itage (servert)	Connections Per Second Loage	2
	19 40 30 08404 D 1037 1030 1030 1040		
	Henory Litage (HE)	A state interface (with inter there)	0
		I. LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL	£.,
	+500-		
	4598 1000		
	- 500	H	
	, <u>1</u>		
	(1444) 10.38 10.37 10.38 10.30 10.40	10.08 10.07 10.00 10.00 10.00	
	<u>beneb</u>		£.,
	Latest ASIII Syshig Hessages	0.9.0	5
	ASSM logging is disabled. To enable ASSM logging is disabled. To enable ASSM logging is disabled.	Nograp with informational level, dick the button balance.	
	1.8	And	
/1 loaded	constate.	Casca 125 La Mar 14 Har Hard 10 Har Hard 10 Ha	60

2. Cliquer Next une fois la page d'accueil de l'assistant atteinte.

🛅 Site-to-site VPN Connectio	m Setup Wizard
VPN Wizard	Introduction
Promits Promit	Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol. Site-to-Site VPN Vocal Cocal
	Here is a <u>video</u> on how to setup a site-to-site VPN connection.
(< Back Cancel Help

Remarque : les versions ASDM les plus récentes fournissent un lien vers une vidéo expliquant cette configuration.

3. Configurez l'adresse IP homologue. Dans cet exemple, l'adresse IP de l'homologue est définie sur 192.168.1.1 sur le site B. Si vous configurez l'adresse IP homologue sur le site A, elle doit être remplacée par 172.16.1.1. L'interface par laquelle l'extrémité distante peut être atteinte est également spécifiée. Cliquer Next une fois terminé.

I. Introduction This step lets you identify the peer VPN device by its IP address and the interface used to access the peer. Peer Device Identification Peer IP Address: 3. Traffic to protect VPN Access Interface: 4. Security VPN Access Interface: 5. NAT Exempt 6. Summary	
Introduction This step lets you identify the peer VPN device by its IP address and the interface used to access the peer. Identification Peer IP Address: 192.168.1.1 S. Traffic to protect VPN Access Interface: outside S. NAT Exempt • • S. Summary VPN Access Interface: outside	
A. Peer Device Identification Peer IP Address: 192.168.1.1 A. Traffic to protect VPN Access Interface: outside A. NAT Exempt . Summary .	
 A. Traffic to protect A. Security Access Interface: outside • 	
Security VPN Access Interface: outside NAT Exempt Summary	
NAT Exempt Summary	
Summary	

4. Configurez les réseaux locaux et distants (source et destination du trafic). Cette image montre la configuration du site B (l'inverse s'applique au site A).

Steps	Traffic to protect			
Introduction Peer Device Identificatio Traffic to protect Security	This step lets you Local Network: Remote Network:	dentify the local network and remote network betw 10.2.2.0_24 10.1.1.0_24	een which the traffic is to be protected using IPsec encryption.	
5. NAT Exempt 6. Summary				
	< Back	xi >	Cancel) Heb

5. Sur la page Security, configurez la clé pré-partagée (elle doit correspondre aux deux extrémités). Cliquer Next une fois terminé.

iteps	Security	
Introduction Peer Device Identificatie 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 ISAKMP security 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 ASD selected for you.	for
	Cancel Cancel	Help

6. Configurez l'interface source pour le trafic sur l'ASA. L'ASDM crée automatiquement la règle de traduction d'adresses de réseau (NAT) en fonction de la version de l'ASA et l'applique avec le reste de la configuration à l'étape finale. **Remarque** : dans l'exemple utilisé dans ce document, « inside » est la source du

23

Steps	NAT Exempt	
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summery 	This step allows you to exempt the local network addresses from network translation.	
	<back next=""></back>	Cancel

7. L'assistant fournit maintenant un résumé de la configuration qui est envoyée à l'ASA. Vérifiez les paramètres de configuration, puis cliquez sur Finish.

1.	summary	
Branch	Here is the summary of the configuration.	
n T	Name	Value
手町	⊡ Summary	
	Peer Device IP Address	192.168.1.1
PHON	VPN Access Interface	outside
porate work	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	
-1-10	DKE v1	Use pre-shared key
	DKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
	Encryption Policy	
	Perfect Forward Secrecy (PFS)	Disabled
The second	E DKE v1	
	IKE Policy	pre-share-aes-sha
6	IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5 ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
	🖂 DKE v2	
	IKE Policy	
	IPsec Proposal	AES256, AES192, AES, 3DES, DES

Configuration via l'interface CLI

Cette section décrit comment configurer le tunnel site à site IKEv1 IPsec via l'interface de ligne de commande.

Configuration du site B pour ASA versions 8.4 et ultérieures

Dans ASA versions 8.4 et ultérieures, la prise en charge d'IKEv1 et d'IKEv2 (Internet Key Exchange version 2) a été introduite.

Conseil : pour plus d'informations sur les différences entre les deux versions, référez-vous à la section <u>Pourquoi migrer vers IKEv2</u>? du document Cisco sur la migration rapide de IKEv1 vers la configuration de tunnel L2L IKEv2 sur le code ASA 8.4.

Conseil : pour obtenir un exemple de configuration IKEv2 avec l'ASA, consultez le document Cisco <u>Site-to-Site IKEv2 Tunnel between ASA and Router Configuration</u> Exemples.

Phase 1 (IKEv1)

Complétez ces étapes pour la configuration de la phase 1 :

1. Entrez cette commande dans l'interface de ligne de commande afin d'activer IKEv1 sur l'interface externe :

crypto ikev1 enable outside

2. Créez une stratégie IKEv1 qui définit les algorithmes/méthodes à utiliser pour le hachage, l'authentification, le groupe Diffie-Hellman, la durée de vie et le cryptage :

```
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. Créez un groupe de tunnels sous les attributs IPsec et configurez l'adresse IP de l'homologue et la clé pré-partagée du 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.
Phase 2 (IPsec)
```

Complétez ces étapes pour la configuration de la phase 2 :

 Créez une liste d'accès qui définit le trafic à chiffrer et à tunnelliser. Dans cet exemple, le trafic d'intérêt est le trafic du tunnel qui provient du sous-réseau 10.2.2.0 vers 10.1.1.0. Elle peut contenir plusieurs entrées si plusieurs sous-réseaux sont impliqués entre les sites.

Dans les versions 8.4 et ultérieures, il est possible de créer des objets ou des groupes d'objets qui servent de conteneurs pour les réseaux, les sous-réseaux, les adresses IP d'hôte ou plusieurs objets. Créez deux objets ayant les sous-réseaux local et distant et utilisez-les pour la liste de contrôle d'accès (ACL) de chiffrement et les instructions 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. Configurez le Transform Set (TS), qui doit impliquer le mot clé IKEv1. Un TS identique doit également être créé sur l'extrémité distante.

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

- 3. Configurez la crypto-carte, qui contient les composants suivants : Adresse IP de l'homologueLa liste d'accès définie qui contient le trafic d'intérêtLe TSParamètre PFS (Perfect Forward Secrecy) facultatif, qui crée une nouvelle paire de clés Diffie-Hellman utilisées afin de protéger les données (les deux côtés doivent être compatibles PFS avant que la phase 2 ne s'affiche)
- 4. Appliquez la crypto-carte sur l'interface externe :

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

Exemption NAT

Assurez-vous que le trafic VPN n'est soumis à aucune autre règle NAT. Il s'agit de la règle NAT utilisée :

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

Remarque : lorsque plusieurs sous-réseaux sont utilisés, vous devez créer des groupes d'objets avec tous les sous-réseaux source et de destination et les utiliser dans la règle 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

Exemple complet de configuration

Voici la configuration complète du site B :

crypto ikev1 enable outside

crypto ikev1 policy 10 authentication pre-share encryption aes hash sha group 2 lifetime 86400 tunnel-group 192.168.1.1 type ipsec-121 tunnel-group 192.168.1.1 ipsec-attributes ikev1 pre-shared-key cisco !Note the IKEv1 keyword at the beginning of the pre-shared-key command. object network 10.2.2.0_24 subnet 10.2.2.0 255.255.255.0 object network 10.1.1.0_24 subnet 10.1.1.0 255.255.255.0 access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24 crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac crypto map outside_map 20 match address 100

crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static

Configurer le site A pour ASA versions 8.2 et antérieures

10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup

Cette section décrit comment configurer le site A pour les versions 8.2 et antérieures d'ASA.

Phase 1 (ISAKMP)

Complétez ces étapes pour la configuration de la phase 1 :

1. Entrez cette commande dans l'interface de ligne de commande afin d'activer le protocole ISAKMP (Internet Security Association and Key Management Protocol) sur l'interface externe :

crypto isakmp enable outside

Remarque : étant donné que plusieurs versions d'IKE (IKEv1 et IKEv2) ne sont plus prises en charge, ISAKMP est utilisé pour faire référence à la Phase 1.

2. Créez une politique ISAKMP qui définit les algorithmes/méthodes à utiliser afin de construire la Phase 1.

Remarque : dans cet exemple de configuration, le mot clé IKEv1 de la version 9.x est remplacé par ISAKMP.

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

3. Créez un groupe de tunnels pour l'adresse IP de l'homologue (adresse IP externe 5515) avec la clé pré-partagée :

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

Phase 2 (IPsec)

Complétez ces étapes pour la configuration de la phase 2 :

1. Comme dans la configuration de la version 9.x, vous devez créer une liste de contrôle d'accès étendue afin de définir le trafic concerné. Définissez un TS qui contient tous les algorithmes de chiffrement et de hachage disponibles (les problèmes proposés ont un point d'interrogation). Assurez-vous qu'il est identique à celui qui a été configuré de l'autre côté.

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

- 3. Configurez une crypto-carte, qui contient les composants suivants : Adresse IP de l'homologueLa liste d'accès définie qui contient le trafic d'intérêtLe TSUn paramètre PFS facultatif, qui crée une nouvelle paire de clés Diffie-Hellman utilisées afin de protéger les données (les deux côtés doivent être compatibles PFS pour que la phase 2 s'affiche)
- 4. Appliquez la crypto-carte sur l'interface externe :

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

Exemption NAT

Créez une liste d'accès qui définit le trafic à exempter des vérifications NAT. Dans cette version, il ressemble à la liste d'accès que vous avez définie pour le trafic d'intérêt :

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

Lorsque plusieurs sous-réseaux sont utilisés, ajoutez une autre ligne à la même liste d'accès :

```
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 liste d'accès est utilisée avec la fonction NAT, comme indiqué ci-dessous :

nat (inside) 0 access-list nonat

Remarque : « inside » fait ici référence au nom de l'interface interne sur laquelle l'ASA reçoit le trafic qui correspond à la liste d'accès.

Exemple complet de configuration

Voici la configuration complète du site A :

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
```

hash sha group 2 lifetime 86400 tunnel-group 172.16.1.1 type ipsec-121 tunnel-group 172.16.1.1 ipsec-attributes pre-shared-key cisco access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 crypto ipsec transform-set myset esp-aes esp-sha-hmac crypto map outside_map 20 set peer crypto map outside_map 20 match address 100 crypto map outside_map 20 set transform-set myset crypto map outside_map 20 set pfs crypto map outside_map interface outside access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat

Stratégie de groupe

Les stratégies de groupe sont utilisées afin de définir des paramètres spécifiques qui s'appliquent au tunnel. Ces politiques sont utilisées conjointement avec le groupe de tunnels.

La stratégie de groupe peut être définie comme interne, ce qui signifie que les attributs sont extraits de celui qui est défini sur l'ASA, ou elle peut être définie comme externe, où les attributs sont interrogés à partir d'un serveur externe. Il s'agit de la commande utilisée pour définir la stratégie de groupe :

group-policy SITE_A internal

Remarque : vous pouvez définir plusieurs attributs dans la stratégie de groupe. Pour une liste de tous les attributs possibles, référez-vous à la section <u>Configuration des stratégies de groupe</u> des Procédures de configuration VPN ASDM sélectionnées pour la gamme Cisco ASA 5500, version 5.2.

Attributs facultatifs de stratégie de groupe

Les vpn-tunnel-protocol détermine le type de tunnel auquel ces paramètres doivent être appliqués. Dans cet exemple, IPsec est utilisé :

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

Vous avez la possibilité de configurer le tunnel de sorte qu'il reste inactif (aucun trafic) et ne tombe pas en panne. Afin de configurer cette option, le vpn-idle-timeout la valeur de l'attribut doit utiliser des minutes, ou vous pouvez définir la valeur sur none, ce qui signifie que le tunnel ne tombe jamais en panne.

Voici un exemple :

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;

Les default-group-policy sous les attributs généraux du groupe de tunnels définit la stratégie de groupe qui est utilisée afin de pousser certains paramètres de stratégie pour le tunnel qui est établi. Les paramètres par défaut des options que vous n'avez pas définies dans la stratégie de groupe proviennent d'une stratégie de groupe globale par défaut :

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

Vérifier

Utilisez les informations fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

ASDM

Pour afficher l'état du tunnel à partir de l'ASDM, accédez à Monitoring > VPN. Ces informations sont fournies :

- Adresse IP de l'homologue
- Protocole utilisé afin de construire le tunnel.
- Algorithme de chiffrement utilisé.
- L'heure à laquelle le tunnel est arrivé et le temps de disponibilité
- Nombre de paquets reçus et transférés.

Conseil : cliquez sur Refresh afin d'afficher les dernières valeurs, car les données ne sont pas mises à jour en temps réel.

THE LOOK STORE									
Call and	Question Quest	C Prevari 🦉 Hebo	1					-145	
collecting in VPR.	o. MTS Statistica > Secold	-							
Read		GE VPM							
Ramella	Site on Site	Clarifierr	Vite Cart	hatha	Tana	E-raimou	VPN Load Balancing	10494	
Access	pie woke	UCTION I	p.	b.ove	0				
1 100	- C.								-
Har By: (Page St	te-to-Site +	- Al Sealard -	-						
Connector Huffle	Protocol	Login Time		Eves Tx					
215611	HE WAY	216960724	April 1915						
	Pass and			1.00	-				
o sort VPN assess	s, right-click on the above ta	die and select Table Sort G	inder from popular menu.						
agent for -ALS			Logisti Geostern						
					Exclusion .				
							iono 2	8	LIER U
Help				_			000 J	Frie Nox D sort	
Help Tol Deve (() tetes () tax (Orward 💡 🗠		_			1000 J	Five loss to sort	
Help To Sert (🚱 ketesi 🗿 kas (Orward ? Ho		_		1	josa ji	Nie kok biesz	
Huly Fig tors (🕢 tetes 🚺 tax (Orward ? Hos		Omities		Del Decaret	jone 2	Nie kor b kord	
Help Fig Sort (Stories > VIII > pe a-to-Site (Pi)	Q tetest Q taxa (200 Shebalta - Sease	Origonal ? into as		Canábre		Pail Orcanet 41	jone 2	Net for 5 for 7	
Help Top Store (Rection 2 Mill 2 Not Star (Pil ND+1 (Pilet:	Q tetest Q tax (Onevent ? Hep as Active		Candidates 1		Pack Concernent 41 41	jone 2	Twe tax b serve	
Help Help Jackson & Million (199 Jackson & Million Help J Press	🐼 ketesk 🧿 koz. (1775 Sketalica – Senate	Onerend ? Hos as		Canaktre 1		Peek Concurrent 41 11	jone ja	Port for the series	
Helg Helg Source (Marcine 2: Million Source (Source (Sour	🐼 hetros 🧿 box.) 1775 Shebalita - Seadar	Onerend ? Hop as		Canaktre 1		Peek Concurrent 41 11	jone ja	Port for the series	
Help Help Martine & Mill J Martine & Mill J	C tetes O tos (Athen		Canaktre 1		Pail Concernent 41 41	joe j	Five tool is send	
Hig Hig Store (Store 2 Hill o Inter-Star (PA Bit-1 (Piece Inter-Star (PA Bit-1 (Piece)	Control Control THE Statistics - Second Hereit	Active		Considere 1 1		Peek Concernent 41 41	joes j2	Institut 3	
Help Help Torter 2 MT Internet MT Internet Internet Internet Internet Internet	Contect Statutes - Service	Active		Canaktre 3 1 Svits Ta Nover fa		Peek Concurrent 41 11	joe 1	Institute 3 3	
Help Help Torter 2 VIC Inter 2 VIC Inter 3 Constant New Street	tetrest totas tetrest totas	Active	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Considere 3 3 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Pail Concerner 41 12	1000 J	Net Nor. D 1997	
Help Help Torress AND Instantion AND Not The Not The Help States Padoress	tetrest O bass (tetrest O bass (tetrest - Second tetrest - Second tetrest - tetrest tetrest - tetrest	Active Active Active Ad Secure - Logis Tree Day	AP 702111	Considence 2 3 million Prices Tax Revises for		PubliConcentert 41 41	jone 2	Viet Nor. D. Servit	
Help Help To Dec (Herbartes, MR) Herbartes Herbartes Herbartes Herbartes Herbartes Herbartes Herbartes	Contrast Contrast of the second secon	Active Ac		Cambibine 2 3 		Public Concurrent 41 41	joe j	Viet Nor. ID 1924 // Dectre 3 3	1991
Hig Hig To the first of the first for the to Sets (PH Not - Sets (PH Not - Sets (PH Patients) And the first Patients Sets (First Patients)	Actrol Data Actrol Data Millad Mil	Ather Ather Alberter User The Busice And Sector Cert And Sector Cert	AC 10/2111-	Considere 2 3 Interim Bytes To Bytes To Bytes To		Pail Concernent 41 41	joe j	Pure too: to search	
Hag Hag Sove (and actions in Million Instandard in Million Mar dy: Effective Derection fruite Paddress States and Soversity (Paddress States and Soversity (Paddress States and Soversity (Paddress States and Soversity (Paddress States and Soversity (Paddress States and Soversity (Paddress States and States a	Actron O Box (This Standards > Second This Standards > Second This Standards > Conditions = Conditions	Active Ac		Cunsidere 2 1 Maria Pros Ta Rese for		Paik Concernent 41 41	joes j2	Institut 3	
Hag Hag Sove (Antoning 2 MB) Insta-Site (PA Balance) Patients Patients Patients	Content Content The State of the State of t	Active Ac	AP 10 2011	Cunaktre 1 1 Stati The Stati The Stati The		Peek Concurrent 41 11	joes ji	I vet tox: to serve	
Halp Halp Toring 2 Store (Interfere 2 VTR Interfere 2 VTR Interfere 2 VTR Interfere Interfere Pacification P	Contract Contractors	Active Active -Al Secure - Logistics Constants - Constant - Constants - Constant - Constant - Constant - Constant - Constant -	AP: 10.2111	Considere 3 1 Most Ro Note Ro		Peek Concurrent 41 12		Institute 3 1	
Help Help Toring 2 Street International Street Street Street Street Street Street Street Street Street Street Street Street Street Stre	C tottet O tos (TTT Statelias - Second escate •	Active	2 ■ 1 1 1 1 1 1 1 1 1 1 1 1 1	Considere 2 3 5 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Pail Concerner 41 12		Net Nor. D 1997	
Help Help To Dec (Inter Str. 1996) Inter Str. 1996: Inter St	e so 356 v	Active Active Active Ad Secure - Logistics Add Add Add Add Add Add Add Add Add Ad	AF 172711	Considence 2 3 Procession Reversion		Puel Concerner 41 12		Viet Nor. D. Your O	
Help Help To Deve (and foreboard - XTE of Non- State of the Constraints Non-State Office Processor Procesor Pro	e solate Pritado Pritado Dorrychon Dorry	At Secure - Logistics Secure -		Considence 2 5 Prote Tx Reset for Prote Tx		Pail Concern 41 41		Pure tox. Is yeard	
Hig Hig Sole Introduce 1 Mill Introduce 1 Mill Mi	Actral D base	Active		Cunsidere 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Park Concernent 41 41		Inetite 3	
Help Help Sove (and and an 2 Mill and Her Sole (PH Baches) March (PH Paddress And An 1 Phone Sole March (Phone Sole Paddress And An 1 Phone Sole Paddress	Contraction of the second of t	Active	AP 102011	Conditions 1 1 Prove Da		Peek Concernent 41 41		Institut la servi	
Halp Halp Tool Store (Antonious 2 1973) Inter-Site 1991 Bits - 1 Office Pacification Pacificati	Contract Contract of the second secon	Active	AP: 10 2011	Cunaktre 1 1 1 Marine Marine Marine Marine Marine Marine		Peek Concurrent 41 11		Net too: Unicerof	
Help Help To Jone (Herber - Million - Million Herber - Million Her	tetrest totas tetrest totas tot	Active	Ar: 17.211 h -	Considere 2 2 Most No Nost No		Peek Concurrent 41 12		Viet Nor. In Sector	
Help Help To Dec 1 Help Sec 1 Help Sec 1 Sec 1 Help Sec 1 H	Actral O bas	Active	Apr 10 2011	Considere 3 5 1 Switch in Switch in		Pail Concerner 4 1		Viet Nov. D reard	

CLI

1 vere

tara hefteshed Successfully

Cette section décrit comment vérifier votre configuration via l'interface de ligne de commande.

Refesh

😹 🔂 🕴 👔 🔄 Hatalat selas es munc

Phase 1

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 1 du côté du site B (5515) :

show crypto ikev1 sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM ACTIVE
```

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 1 du côté du site 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

Phase 2

Les show crypto ipsec sa affiche les associations de sécurité IPsec qui sont créées entre les homologues. Le tunnel chiffré est construit entre les adresses IP 192.168.1.1 et 172.16.1.1 pour le trafic qui circule entre les réseaux 10.1.1.0 et 10.2.2.0. Vous pouvez voir les deux associations de sécurité ESP conçues pour le trafic entrant et sortant. L'en-tête d'authentification (AH) n'est pas utilisé car il n'existe aucune SA AH.

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 2 du côté du site B (5515) :

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

```
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
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
```

Entrez cette commande dans l'interface de ligne de commande afin de vérifier la configuration de phase 2 du côté du site 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
```

Dépannage

Utilisez les informations fournies dans cette section afin de résoudre les problèmes de configuration.

ASA versions 8.4 et ultérieures

Entrez ces commandes debug afin de déterminer l'emplacement de la défaillance du tunnel :

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

Voici un exemple complet des résultats du débogage :

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 pavload
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 = 0x1ba0c55cFeb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing final guick 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)
```

Entrez ces commandes debug afin de déterminer l'emplacement de la défaillance du tunnel :

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

Voici un exemple complet des résultats du débogage :

```
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: 2000001)
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)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.