IKEv1 IPsec site-to-site tunnels configureren met de ASDM of CLI op de ASA

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren Netwerkdiagram Configureren via de ASDM VPN Wizard Configureren via de CLI Site B configureren voor ASA versies 8.4 en hoger Site A configureren voor ASA versies 8.2 en eerder Groepsbeleid Verifiëren **ASDM** CLI Fase 1 Fase 2 Problemen oplossen ASA versies 8.4 en hoger ASA versies 8.3 en eerder

Inleiding

Dit document beschrijft hoe u een Internet Key Exchange versie 1 (IKEv1) IPsec site-to-site tunnel kunt configureren tussen een Cisco 5515-X Series adaptieve security applicatie (ASA) die softwareversie 9.2.x en een Cisco 5510 Series ASA draait op softwareversie 8.2.x.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- De end-to-end IP-verbinding moet tot stand worden gebracht
- Deze protocollen moeten worden toegestaan: User Datagram Protocol (UDP) 500 en 4500 voor het IPsec-besturingsplaneIP-protocol 50 voor insluitend security payload (ESP) voor het IPsec-gegevensvlak

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5510 Series ASA waarin softwareversie 8.2 wordt uitgevoerd
- Cisco 5515-X ASA waarop de softwareversie 9.2 wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

In deze sectie wordt beschreven hoe u de site-to-site VPN-tunnel kunt configureren via de wizard Adaptive Security Device Manager (ASDM) VPN of via de CLI.

Netwerkdiagram



Deze topologie wordt gebruikt voor de voorbeelden in dit document:

Configureren via de ASDM VPN Wizard

Voltooi deze stappen om de site-to-site VPN-tunnel in te stellen via de ASDM-wizard:

1. Open de ASDM en navigeer naar Wizards > VPN Wizards > Site-to-site VPN Wizard.

Cisco ASEM T4 tord		10 m		All of the local division of the local divis	1 miles - 10		0.0
View Toole W	erðs Window Help					We topic to search	illa altalla
HINE OF CON	Statup Weard.						CISCO
Derive List . But	VPN Waards * Sterlo sile VPN Waard.						1
or list	High Armidelity and Scalebility Woord_						
et 🛱 Celete	Unified Conversariation Weard Chevites 532 VPN Wzard		tank in the second				
	ASDM Identity Cartificate Waand. (Psec (REd) Remote Access VPN Waand.)		Entertace Status				
20. 120. 120. 12	Pashat Capture Wisand.	14	Interface:	IP Aldress Nak	Line	LHR	vitere
1.105.131.43	Heal Fame: electrate		4504	10.105.100.100/04	0.+	0.44	
ADD. 1201.100	AGA Version: 9.115319 Device Liptime: S6d Zh 44m 0s		inede	20.2.2.2.294	0 up	0.0	
5130100	40/mesoni 7.4(1) Jevie Troe ASA 5530, 55H-CSC-20-45		kneide2	10.4.4.1/24	0.40	0.0	
5.130.395	Pressel Mode: Readed Excitact Mode: Single		ousite	172.16.1.1(24	0.0	9 up	1
1.130.191	Tatal Rody 256 MB Total Memory 2648 MB	Colori as plantara to	unu no r ant o to t that				
136.122		14		and the second second			
303-138-224	Withourse State of the A		Patron Claim				
06.44.154	Date Creating where we have a set the contract of the contract	VENUE.	Have the not carrique	in case the link to compare it.			VILLAND R
200.44.205	System-Resources Status	3	Traffic Status				
6.106.72.0	(Pit tage (servert)		- Connections Pay Sec	cond licege			214
	60 60 1% 40 30						
	(8.40-4 (0.52) (0.52) (0.52)	10-40		K9 97	+3.00	45.00	6.0
	Henory Liage (HD)		In date Departure 7	afferi sana Mani			
			Tantade Littertade Interna Junge Plants				
			1.1				
	1000						
	500						
			1.1				
	UR454 0 1038 1037 1038 8030	10-00	10:58	10.07	+3.00	40.90	10-0
	Details		Povt Gps 1	OvbuctOpsi 0			
						1.000.000	
	Litest ASI/It Systep Hessages						13 - 6 - 1
	ASIZM logging a	feabled. To enable ASOM bogs	ng with informational level stogging	, dok the lautton below.			
at configuration leader	accessfully.			100	15		A INTERESTICTION

2. Klik Next zodra u de startpagina van de wizard hebt bereikt.

🛅 Site-to-site VPN Connectio	in Setup Wizard
VPN Wizard	Introduction
	Use this warand to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.
	< Back Cancel Help

Opmerking: de meest recente ASDM-versies bevatten een link naar een video die deze configuratie uitlegt.

 Configureer het peer IP-adres. In dit voorbeeld is het peer IP-adres ingesteld op 192.168.1.1 op Site B. Als u het peer IP-adres op site A configureert, moet dit worden gewijzigd in 172.16.1.1. De interface waardoor het verre eind kan worden bereikt wordt ook gespecificeerd. Klik Next eenmaal voltooid.

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

4. Configureer de lokale en externe netwerken (verkeersbron en bestemming). Dit beeld toont de configuratie voor Site B (het omgekeerde geldt voor Site A).

Steps	Traffic to protect			
1. Introduction 2. 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.	
3. Traffic to protect	Local Network:	10.2.2.0_24		
4. Security	Remote Network:	10.1.1.0_24		
5. NAT Exempt 6. Summary				
			[222]	

5. Voor de pagina van de Veiligheid, vorm de pre-gedeelde sleutel (het moet op beide einden aanpassen). Klik Next eenmaal voltooid.

teps	Security	
Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary	This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IXE and ISAMMP 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=""> Centel He</back>	40

6. Configureer de broninterface voor het verkeer op de ASA. ASDM maakt automatisch de Network Address Translation (NAT)-regel op basis van de ASA-versie en duwt deze met de rest van de configuratie in de laatste stap. **Opmerking**: bij het voorbeeld in dit document is 'inside' de bron van het

verkeer.

Steps	NAT Exempt	
 Introduction Peer Device Identification Traffic to protect Security SAT Exempt Summary 	This step allows you to exempt the local network addresses from network translation. Exempt ASA side host/inetwork from address translation	
	< Back Next >	Cancel

7. De wizard geeft nu een samenvatting van de configuratie die naar de ASA is geduwd. Controleer de configuratie-instellingen en klik vervolgens op Finish.

Summary	
Here is the summary of the config	ation.
Name	Value
Summary	
Peer Device IP Address	192.168.1.1
VPN Access Interface	outside
Protected Traffic	Local Network: 10.2.2.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
DKE v1	Use pre-shared key
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 (S) Disabled
E DKE v1	
IKE Policy	pre-share-aes-sha
IPsec Proposal	ESP-AE5-128-SHA, ESP-AE5-128-MD5, ESP-AE5-192-SHA, ESP-AE5-192-MD5 ESP-AE5-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DE5-SHA, ESP-DE5-MD5
E IKE v2	
IKE Policy	
IPsec Proposal	AES256, AES192, AES, 3DES, DES

Configureren via de CLI

In deze sectie wordt beschreven hoe u de IKEv1 IPsec site-to-site tunnel via de CLI kunt configureren.

Site B configureren voor ASA versies 8.4 en hoger

In ASA versies 8.4 en hoger werd ondersteuning voor zowel IKEv1 als Internet Key Exchange versie 2 (IKEv2) geïntroduceerd.

Tip: Raadpleeg voor meer informatie over de verschillen tussen de twee versies <u>Why</u> <u>migrate to IKEv2?</u> sectie van de Swift Migration of IKEv1 to IKEv2 L2L Tunnel Configuration op ASA 8.4 Code Cisco-document.

Tip: Neem voor een IKEv2-configuratievoorbeeld met de ASA de <u>Site-to-Site IKEv2-tunnel</u> <u>tussen ASA en</u> Cisco <u>Router Configuration Voorbeelden</u>.

Fase 1 (IKEv1)

Voltooi de volgende stappen voor de configuratie van fase 1:

1. Voer deze opdracht in de CLI in om IKEv1 op de buiteninterface in te schakelen:

crypto ikev1 enable outside

2. Maak een IKEv1-beleid dat de algoritmen/methoden definieert die moeten worden gebruikt voor hashing, verificatie, Diffie-Hellman groep, levensduur en codering:

```
!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. Maak een tunnelgroep onder de IPsec-kenmerken en configureer het peer-IP-adres en de vooraf gedeelde tunnelsleutel:

```
tunnel-group 192.168.1.1 type ipsec-12l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
2 (IPsec)
```

Fase 2 (IPsec)

Voltooi de volgende stappen voor de configuratie van fase 2:

 Maak een toegangslijst waarin het te versleutelen en te tunnelen verkeer wordt gedefinieerd. In dit voorbeeld, is het verkeer van belang het verkeer van de tunnel die van 10.2.2.0 subnett aan 10.1.1.0 afkomstig is. Het kan meerdere ingangen bevatten als er meerdere subnetten tussen de sites betrokken zijn.

In versies 8.4 en hoger kunnen objecten of groepen objecten worden gemaakt die dienen als containers voor de netwerken, subnetten, host IP-adressen of meerdere objecten. Maak twee objecten met de lokale en externe subnetten en gebruik deze voor zowel de cryptotoegangscontrolelijst (ACL) als de NAT-verklaringen.

```
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. De transformatieset (TS) configureren, waarbij het trefwoord moet worden gebruikt IKEv1. Een identieke TS moet ook op het verre eind worden tot stand gebracht.

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

3. Configureer de crypto map, die deze componenten bevat:

Het peer IP-adresDe gedefinieerde toegangslijst die het relevante verkeer bevatHet TSEen optionele Perfect Forward Secrecy (PFS)-instelling, die een nieuw paar Diffie-Hellmantoetsen maakt die worden gebruikt om de gegevens te beschermen (beide kanten moeten PFS-ingeschakeld zijn voordat fase 2 verschijnt)

4. Pas de crypto kaart op de buiteninterface toe:

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-vrijstelling

Zorg ervoor dat het VPN-verkeer niet aan andere NAT-regels wordt onderworpen. Dit is de NATregel die wordt gebruikt:

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

Opmerking: wanneer meerdere subnetten worden gebruikt, moet u objectgroepen maken met alle bron- en doelsubnetten en deze gebruiken in de NAT-regel.

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

Volledige voorbeeldconfiguratie

Hier is de volledige configuratie voor Site B:

crypto ikev1 enable outside

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

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

Site A configureren voor ASA versies 8.2 en eerder

In deze sectie wordt beschreven hoe u Site A voor ASA versies 8.2 en hoger kunt configureren.

Fase 1 (ISAKMP)

Voltooi de volgende stappen voor de configuratie van fase 1:

1. Voer deze opdracht in de CLI in om Internet Security Association en Key Management Protocol (ISAKMP) op de buiteninterface in te schakelen:

crypto isakmp enable outside

Opmerking: omdat meerdere versies van IKE (IKEv1 en IKEv2) niet langer worden ondersteund, wordt ISAKMP gebruikt om naar fase 1 te verwijzen.

 Maak een ISAKMP-beleid dat de algoritmen/methoden definieert die moeten worden gebruikt om fase 1 te bouwen.

Opmerking: in deze voorbeeldconfiguratie wordt het trefwoord IKEv1 van versie 9.x wordt vervangen door ISAKMP.

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

3. Maak een tunnelgroep voor het peer IP-adres (extern IP-adres van 5515) met de vooraf gedeelde sleutel:

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

Fase 2 (IPsec)

Voltooi de volgende stappen voor de configuratie van fase 2:

1. Gelijkaardig aan de configuratie in versie 9.x, moet u een uitgebreide toegangslijst creëren om het verkeer van belang te bepalen.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

 Definieer een TS die alle beschikbare encryptie- en hashingalgoritmen bevat (aangeboden problemen hebben een vraagteken). Zorg ervoor dat deze identiek is aan de configuratie aan de andere kant.

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

- Configureer een crypto-kaart die deze componenten bevat: Het peer IP-adresDe gedefinieerde toegangslijst die het relevante verkeer bevatHet TSEen optionele PFS-instelling, die een nieuw paar Diffie-Hellman-toetsen creëert die worden gebruikt om de gegevens te beschermen (beide kanten moeten PFS-ingeschakeld zijn zodat fase 2 verschijnt)
- 4. Pas de crypto kaart op de buiteninterface toe:

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

NAT-vrijstelling

Creeer een toegangslijst die het verkeer dat van de NAT controles moet worden vrijgesteld bepaalt. In deze versie lijkt het op de toegangslijst die u voor het interesseverkeer hebt gedefinieerd:

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

Wanneer meerdere subnetten worden gebruikt, voegt u een andere regel toe aan dezelfde toegangslijst:

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

De toegangslijst wordt gebruikt met NAT, zoals hier getoond:

nat (inside) 0 access-list nonat

Opmerking: De 'binnenkant' verwijst hier naar de naam van de interne interface waarop de ASA het verkeer ontvangt dat overeenkomt met de toegangslijst.

Volledige voorbeeldconfiguratie

Hier is de volledige configuratie voor Site A:

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

Groepsbeleid

Groepsbeleid wordt gebruikt om specifieke instellingen te definiëren die van toepassing zijn op de tunnel. Dit beleid wordt gebruikt in combinatie met de tunnelgroep.

Het groepsbeleid kan worden gedefinieerd als hetzij intern, wat betekent dat de attributen worden getrokken van wat is gedefinieerd op de ASA, of het kan worden gedefinieerd als extern, waar de attributen worden gevraagd van een externe server. Dit is de opdracht die wordt gebruikt om het groepsbeleid te definiëren:

group-policy SITE_A internal

Opmerking: U kunt meerdere kenmerken definiëren in het groepsbeleid. Raadpleeg voor een lijst met alle mogelijke kenmerken het gedeelte <u>Groepsbeleid configureren</u> van de geselecteerde ASDM VPN-configuratieprocedures voor Cisco ASA 5500 Series, versie 5.2.

Optionele kenmerken voor groepsbeleid

Het vpn-tunnel-protocol het kenmerk bepaalt het tunneltype waarop deze instellingen moeten worden toegepast. In dit voorbeeld wordt IPsec gebruikt:

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

U hebt de optie om de tunnel te configureren zodat deze inactief blijft (geen verkeer) en niet omlaag gaat. Om deze optie te configureren klikt u op de vpn-idle-timeout de waarde van attributen moet minuten gebruiken, of u kunt de waarde instellen op none, wat betekent dat de tunnel nooit naar beneden gaat.

Hierna volgt een voorbeeld:

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;

Het default-group-policy De opdracht onder de algemene eigenschappen van de tunnelgroep definieert het groepsbeleid dat wordt gebruikt om bepaalde beleidsinstellingen voor de tunnel die wordt ingesteld te duwen. De standaardinstellingen voor de opties die u niet in het groepsbeleid hebt gedefinieerd, zijn afkomstig uit een algemeen standaardgroepsbeleid:

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

Verifiëren

Gebruik de informatie die in deze sectie wordt verstrekt om te verifiëren dat uw configuratie behoorlijk werkt.

ASDM

Om de tunnelstatus van de ASDM te bekijken, navigeer naar Monitoring > VPN. Deze informatie wordt verstrekt:

- Het peer IP-adres
- Het protocol dat wordt gebruikt om de tunnel te bouwen
- · Het encryptie-algoritme dat wordt gebruikt
- · Het tijdstip waarop de tunnel omhoog kwam en de up-time
- · Het aantal pakketten dat wordt ontvangen en overgebracht

Tip: klik op Refresh om de meest recente waarden weer te geven, aangezien de gegevens niet in real time worden bijgewerkt.

Image of the field of the second of the field of the	
landaran 2.VEL 2.VEL 2.UEL 2.	
Fired Sk, VH Fired Name She folder Other fold Nith Chert Nachter Notal Creative Creative Notal Name Na	
Part No. 100 Part of the second of the seco	
termine Site 6 Site Open Open Site 6 Site Open Site 6 Site Open Site 6 Site 0 Open Site 0	uditations State
0 1 0 0 0 0 0	
here for (2014) Searce	1
The formation of the second se	
Of Packford Deviation Deviation Deviation Operation Deviation Deviation Deviation Operation Deviation Deviation Deviation Deviation Deviation Deviation Deviation <td></td>	
No. 1 So per VMI seasone, right dds as the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. So per VMI seasone, right dds as the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. Source first in the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. Image: Source first in the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. Image: Source first in the doon table and sales fields fort Order from pape annu. Image: Source in the doon table and sales fields fort Order from pape annu. Image: Source first in the doon table and sales fields fort Order first in the doon table and sales fields fort Order first in the doon table and sales fields fort Order first in the doon table and table field fort in the doon table and table field fort in the doon table and table field fort in the doon table field fort in the doon table and table field fort in the doon table and table field fort in the doon table field fort in the doon table fort in the doon table field fort in the doon table field fort in the doon table fort in table field fort in the doon table fort in the doon table field fort in the doon table fort in the doon table fort in the doon table fort in table field fort in the doon table fort in the doon table fort in table fort in the doon table fort in tab	
Do art Will seasons, right dol an the dows table and salest fields fort Order from papag nerve. ingenuit for ind Seasons I help I h	
To per 1994 sensors, replicible on the down table and axies Table Sort Order from poour nerv. ingrad The Addisement → Ingred Sensors Ingred The Addisement → Ingred Sensors Ingred The Addisement → Ingred Sensors Ingred The Addise Transford The Addise	
To part VM autoons, right-doisen the adove table and select field Sort Onite from papage menu. tergend for in Al Seamers	
To per 1991 sessore, repli-data in the above table and select Table Sort Order from papage nerve. Largent Reserve	
Do por VMI assessore, replicable on the above table and select Table Sort Order from paper renu. Luggest for	
To art VM autors, rgf1 db ar the does take and select Table Sort Order from paper name. ingend from Ad Seamers	
So ser 14% assessment, regin club, and basies fields for 0 form from papage nerve. ingrade fire	
To sor 1991 essence. rg1-cldue the done table and select field Sort Order from papage nerve. togene for	
So ary 1998 assessors, regist-labore table and select table Sort Order from papage nerve. targent from	
To any tVM assesses, right clds at the dow table and select Table Sort Over from papar nerv. ingraw from	
Di part VM essense, nghi dab ar Be alcon table and seinct fielle Son Order from popus menu. isque fire indi Seamme	
To sort VM essense, right dates the end select fields for Order from popular nerve. Insertients To sort VM essenses. To sort VM essenses. The formation in the above bable and select fields for Order from popular nerve. Insertients The formation in the above bable and select fields for Order from popular nerve. Insertients The formation in the above bable and select fields for Order from popular nerve. Insertients The formation in the above bable and select fields for Order from popular nerve. Insertients The formation in the above bable and select fields for Order from popular nerve. Insertients The formation in the above bable and select fields for Order formation The formation in the above bable and select fields for Order formation The formation in the above bable and select fields for Order formation The formation in the formation in the above bable and select fields for Order formation The formation in the formation in the above bable and select fields for Order formation The formation in the formation in the above bable and select fields for Order formation The formation in the formation in the above bable and select fields for Order formation The formation in the formation in the above bable and select field for Order formation The formation in the formation in the above field for Order formation The formation in the formation in the above field for Order formation The formation in the formation in the formation in the above field for Order formation in the format	
Is nor 1991 sessors, right datum the aloue table and select fields forn (Page Tennes. Ingen fire _ Ald Sessors +	
To sort VM assore, ngli chika on the down table and select "table Sort Order from popus neru. tagent for	
To sor (MI assesse, right data or the above table and select Table Sort Order from papar nerv. ingree for	
No sor tif M assence, regit i club on table and select Table Sort Other from papara nerve. Ingrie The Ad Seasons + Ingrie Teenson - Ingrie T	
To part HM seasons, ngh citik an the above table and sales Table Sort Order from papar nerv. ingent fin	
ingene fin ind Seeners - + ingene Seeners restant.	
Image: Source of the source	
Image: Section Control Contro	
With and an analysis Presidence Pre	
No a Help Nmg Date (total () 100) 100 () 10	
001 2 201 <th>1 C08</th>	1 C08
Alter Processon huffe hubbles + Seasons The Section 2 VEL 2 TH Statistics + Seasons Tree Active Canadrane Performance Sect-36 VM Sect-36 VM Sec	
And Help The Help The State of the State o	
r Halo Dec Other Other Other Other Other Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser-to-Ser SH1 Ser to-Ser SH1 Ser SH1 Se	
ong i Dec Q forder VICE 2 UTC Statistics + Sections Type Active Cunsides Active Cunsides Period Statistics + Section 4 4 36:-10 Pec 3 4 There by: Breeches 6:01e • Information - Information Patrone Provide Box (Information - Information Patrone Patrone Pat	The Role Diseron
In the second state of the second sec	
Type Active Candidate Peek Concurrent Sette-546 991 Sette-549 901 Sette-549 902 Take by: Setter-549 902 Take by: Setter-549 902 Packets Exception (Setter-549 90291) Packets Exception (Setter-549 90291) Setter-558 Setter-549 902 Setter-549 902	
Type Active Cumulative Peet Concurrent Site-U-Site Vol 3 41 Site-U-Site Vol 3 41 Filter Sy: 1 1 Filter Sy: Precisitie-Vol 1 Filter Sy: Precisitie-Vol 1 Correction Hraffie Protocol Precisitie (P Address) Protocol Precisitie Valees Site Protocol Protocol No sets Site Protocol Protocol No sets Site Protocol Protocol	
Ske-b-Ske VH 2 4 Ske-b-Ske VH 2 4 The Ske Ske Ske Ske Ske Ske Ske Ske Ske Sk	Inective
There are no set of the second	3
Main Tyr, Mexame to Gale	1
This Ty: Declar to be	
There Tare to date • • • • • • • • • • • • • • • • • • •	
Take by: Unexcise to date • • • • • • • • • • • • • • • • • • •	
Connection Huttle Person P. Admess Econymics Duardon Here Six NO 298-31	
Alexand Department (Constraint)	
NG 998 1 1 MGY 1 (BNG 136 Prove) (Brither de	

CLI

two Refreshed Successfully

🔒 Trand Mora G

3.

To set

inquitiv - Alter

In deze sectie wordt beschreven hoe u uw configuratie via de CLI kunt verifiëren.

t Order Floma

Logout Sessions

Fase 1

Voer deze opdracht in de CLI in om de configuratie van fase 1 op de kant van Site B (5515) te verifiëren:

Refresh

😹 🖬 🕴 👔 🖓 100,000 100,000 PP units

```
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
```

Voer deze opdracht in de CLI in om de configuratie van fase 1 op de zijde van Site A (5510) te verifiëren:

show crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

Fase 2

Het show crypto ipsec sa Het bevel toont IPsec SAs die tussen de peers worden gebouwd. De versleutelde tunnel is gebouwd tussen IP-adressen 192.168.1.1 en 172.16.1.1 voor verkeer dat tussen de netwerken 10.1.1.0 en 10.2.2.0 stroomt. U kunt de twee ESP SA's zien die zijn gebouwd voor het inkomende en uitgaande verkeer. De verificatieheader (AH) wordt niet gebruikt omdat er geen AH-SA's zijn.

Voer deze opdracht in de CLI in om de fase 2-configuratie op de site B (5515)-kant te verifiëren:

```
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
```

Voer deze opdracht in de CLI in om de fase 2-configuratie op de zijde van Site A (5510) te verifiëren:

```
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
```

Problemen oplossen

Gebruik de informatie die in deze sectie wordt verstrekt om configuratieproblemen op te lossen.

ASA versies 8.4 en hoger

Voer deze debug-opdrachten in om de locatie van de tunnelfout te bepalen:

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

Hier is een volledig voorbeeld van debug uitvoer:

```
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 pavload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
```

```
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco
VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
1
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group
192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating
kevs for Initiator ...
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing
ID pavload
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing
hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive
payload: proposal=32767/32767 sec.
1
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing dpd vid payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT
Detection Status: Remote end is NOT behind a NAT device This end is NOT behind
a NAT device
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing
ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR ID received 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
```

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing VID payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley begin 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 quick mode Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing proxy ID Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Transmitting Proxy Id: Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending Initial Contact Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing qm hash payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,

processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, loading all IPSEC SAs Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key! Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0x6f0e03f0, SCB: 0x75B6DD00, Direction: outbound SPI : 0x1BA0C55C Session ID: 0x00004000 VPIF num : 0x0000002 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x1BA0C55C IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C Flags: 0x0000005 SA : 0x6f0e03f0 SPI : 0x1BA0C55C MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x0B47D387 Channel: 0x6ef0a5c0 IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C VPN handle: 0x0000f614 IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C Src addr: 10.2.2.0 Src mask: 255.255.255.0 Dst addr: 10.1.1.0 Dst mask: 255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C Rule ID: 0x74e1c558 IPSEC: New outbound permit rule, SPI 0x1BA0C55C Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0

```
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0;
encrypt_rule=752972d0; tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation
complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7,
Outbound SPI = 0x1ba0c55c
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley
constructing final quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator
sending 3rd QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + NONE (0) total length : 76
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD
msg for SA: SPI = 0x1ba0c55c
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x0000002
Tunnel type: 121
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x0000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x0000000
Peer : 0x0000F614
SCB : 0x0B4707C7
Channel: 0x6ef0a5c0
IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x00011f6c
IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C
Flags: 0x0000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x00011F6C
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
```

Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7 Rule ID: 0x74e1b4a0 IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7 Rule ID: 0x6f0de830 IPSEC: New inbound permit rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7 Rule ID: 0x6f0de8d8 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher: received KEY_UPDATE, spi 0x3fc9db7 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P2 rekey timer: 24480 seconds. Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2 COMPLETED (msgid=4c073b21)

ASA versies 8.3 en eerder

Voer deze debug-opdrachten in om de locatie van de tunnelfout te bepalen:

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

Hier is een volledig voorbeeld van debug uitvoer:

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

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys for Responder... Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR ID received 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for TSAKMP 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--255.255.25.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing notify payload Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa not found by addr Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside_map, seq = 20... Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside_map, seq = 20 is a successful match Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside_map Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0xAB5C63A8, SCB: 0xABD54E98, Direction: inbound SPI : 0x1BA0C55C Session ID: 0x00004000 VPIF num : 0x0000001 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI from key engine: SPI = 0x1ba0c55c Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley constucting quick mode Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing blank hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec nonce pavload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing proxy ID Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting Proxv 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 om hash pavload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder sending 2nd QM pkt: msg id = 4c073b21 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all IPSEC SAs Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key! Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned

cs_id=ab9302f0; rule=ab9309b0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0xAB570B58, SCB: 0xABD55378, Direction: outbound SPI : 0x03FC9DB7 Session ID: 0x00004000 VPIF num : 0x0000001 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x03FC9DB7 IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7 Flags: 0x0000005 SA : 0xAB570B58 SPI : 0x03FC9DB7 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x01512E71 Channel: 0xA7A98400 IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7 VPN handle: 0x0000F99C IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7 Src addr: 10.1.1.0 Src mask: 255.255.255.0 Dst addr: 10.2.2.0 Dst mask: 255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7 Rule ID: 0xABD557B0 IPSEC: New outbound permit rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7 Rule ID: 0xABD55848 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;

```
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0 \times 03 \text{fc} 9 \text{db} 7
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)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.