Konfigurieren von IKEv1-IPsec-Site-to-Site-Tunneln mit dem ASDM oder der CLI auf der ASA

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfiguration über den ASDM VPN Wizard Konfiguration über die CLI Konfigurieren von Standort B für ASA Version 8.4 und höher Konfigurieren von Standort A für ASA Version 8.2 und frühere Versionen Gruppenrichtlinie Überprüfung ASDM CLI Phase 1 Phase 2 Fehlerbehebung ASA Version 8.4 und höher ASA Version 8.3 und frühere Versionen

Einleitung

In diesem Dokument wird beschrieben, wie ein Internet Key Exchange Version 1 (IKEv1) IPsec-Site-to-Site-Tunnel zwischen einer Cisco 5515-X Series Adaptive Security Appliance (ASA) mit der Softwareversion 9.2.x und einer Cisco 5510 Series ASA mit der Softwareversion 8.2.x konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

• Die End-to-End-IP-Verbindung muss hergestellt werden.

 Diese Protokolle müssen zugelassen sein: User Datagram Protocol (UDP) 500 und 4500 für die IPsec-KontrollebeneEncapsulating Security Payload (ESP) IP Protocol 50 für die IPsec-Datenebene

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA der Serie 5510 mit Softwareversion 8.2
- Cisco 5515-X ASA mit der Softwareversion 9.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie den Site-to-Site-VPN-Tunnel mithilfe des ASDM-VPN-Assistenten (Adaptive Security Device Manager) oder über die CLI konfigurieren.

Netzwerkdiagramm

Diese Topologie wird für die Beispiele im gesamten Dokument verwendet:



Konfiguration über den ASDM VPN Wizard

Führen Sie die folgenden Schritte aus, um den Site-to-Site-VPN-Tunnel mithilfe des ASDM-Assistenten einzurichten:

1. Öffnen Sie den ASDM, und navigieren Sie zu Wizards > VPN Wizards > Site-to-site VPN Wizard.



2. Klicken Sie auf Next sobald Sie die Startseite des Assistenten erreichen.

🛅 Site-to-site VPN Connectic	on Setup Wizard
VPN Wizard	Introduction
	Use this wizerd 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

Hinweis: Die neuesten ASDM-Versionen bieten einen Link zu einem Video, in dem diese Konfiguration erläutert wird.

3. Konfigurieren Sie die IP-Adresse des Peers. In diesem Beispiel ist die Peer-IP-Adresse für Standort B auf 192.168.1.1 festgelegt. Wenn Sie die Peer-IP-Adresse an Standort A konfigurieren, muss sie in 172.16.1.1 geändert werden. Die Schnittstelle, über die das Remote-Ende erreicht werden kann, wird ebenfalls angegeben. Klicken Sie auf Next nach Abschluss.

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

4. Konfigurieren der lokalen und Remote-Netzwerke (Datenverkehrsquelle und -ziel) Dieses Bild zeigt die Konfiguration für Standort B (das Gegenteil trifft auf Standort A zu).

iteps	Traffic to protect			
Introduction Peer Device Identificatio Traffic to protect Security MAT Example	This step lets you Local Network: Remote Network:	dentify the local network and remote network betwee 10.2.2.0_24 10.1.1.0_24	n which the traffic is to be protected using IPsec encryption.	
6. Summerγ				

5. Konfigurieren Sie auf der Seite Sicherheit den vorinstallierten Schlüssel (er muss auf beiden Seiten übereinstimmen). Klicken Sie auf Next nach Abschluss.

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

6. Konfigurieren Sie die Quellschnittstelle f
ür den Datenverkehr auf der ASA. Der ASDM erstellt automatisch die Network Address Translation (NAT)-Regel auf Basis der ASA-Version und überträgt diese an die restliche Konfiguration im letzten Schritt. Hinweis: In diesem Beispiel ist "inside" die Quelle f
ür den

Datenverkehr.

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

7. Der Assistent bietet nun eine Zusammenfassung der Konfiguration, die per Push an die ASA gesendet wird. Überprüfen und überprüfen Sie die Konfigurationseinstellungen, und klicken Sie dann auf Finish.

Su Su	immar y	
Brandh He	ere is the summary of the configuration.	
	lame	Value
THE REAL	Summary	
E Ene	Peer Device IP Address	192.168.1.1
Home	VPN Access Interface	outside
orborate Detwork	Protected Traffic	Local Network: 10.2,2,0/24 Remote Network: 10.1,10/24
	IKE Version Allowed	IKE version 1 and IKE version 2
a 14 9	Authentication Method	
1 total	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 state of the s	E DKE v1	
	IKE Policy	pre-share-aes-sha
B	IPsec Proposal	ESP-AE5-128-SHA, ESP-AE5-128-MDS, ESP-AE5-192-SHA, ESP-AE5-192-MDS, ESP-AE5-256-SHA, ESP-AE5-256-MD5, ESP-3DE5-SHA, ESP-3DE5-MD5, ESP-DE5-SHA, ESP-DE5-MD5
	E DKE v2	
	IKE Policy	
	IPsec Proposal	AES256, AES192, AES, 3DES, DES
	and the second	

Konfiguration über die CLI

In diesem Abschnitt wird beschrieben, wie der IKEv1-IPsec-Site-to-Site-Tunnel über die CLI konfiguriert wird.

Konfigurieren von Standort B für ASA Version 8.4 und höher

In der ASA-Version 8.4 und höher wurde die Unterstützung für IKEv1 und Internet Key Exchange Version 2 (IKEv2) eingeführt.

Tipp: Weitere Informationen zu den Unterschieden zwischen den beiden Versionen finden Sie im Abschnitt <u>Warum auf IKEv2 migrieren?</u> des Dokuments Swift Migration of IKEv1 to IKEv2 L2L Tunnel Configuration on ASA 8.4 Code Cisco.

Tipp: Ein IKEv2-Konfigurationsbeispiel mit der ASA finden Sie im Cisco Dokument <u>Site-to-</u> <u>Site IKEv2 Tunnel between ASA and Router Configuration Example</u>.

Phase 1 (IKEv1)

Führen Sie die folgenden Schritte für die Konfiguration von Phase 1 aus:

1. Geben Sie diesen Befehl in die CLI ein, um IKEv1 auf der externen Schnittstelle zu aktivieren:

crypto ikev1 enable outside

2. Erstellen Sie eine IKEv1-Richtlinie, die die Algorithmen/Methoden für Hashing, Authentifizierung, Diffie-Hellman-Gruppe, Lebensdauer und Verschlüsselung definiert:

```
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. Erstellen Sie eine Tunnelgruppe unter den IPsec-Attributen, und konfigurieren Sie die Peer-IP-Adresse und den vorinstallierten Tunnelschlüssel:

```
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)
```

Führen Sie die folgenden Schritte für die Konfiguration von Phase 2 aus:

 Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden und zu tunnelnden Datenverkehr definiert. In diesem Beispiel ist der Datenverkehr von Interesse der Datenverkehr aus dem Tunnel, der vom Subnetz 10.2.2.0 an 10.1.1.0 stammt. Sie kann mehrere Einträge enthalten, wenn zwischen den Standorten mehrere Subnetze vorhanden sind.

In Version 8.4 und höher können Objekte oder Objektgruppen erstellt werden, die als Container für Netzwerke, Subnetze, Host-IP-Adressen oder mehrere Objekte dienen. Erstellen Sie zwei Objekte mit den lokalen und den Remote-Subnetzen, und verwenden Sie sie sowohl für die Crypto Access Control List (ACL)- als auch für die NAT-Anweisungen.

```
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. Konfigurieren Sie den Transformationssatz (TS), der das Schlüsselwort enthalten muss. IKEv1. Auch am Remote-Ende muss ein identischer TS erstellt werden.

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

- 3. Konfigurieren Sie die Crypto Map, die folgende Komponenten enthält: Die Peer-IP-AdresseDie definierte Zugriffsliste, die den relevanten Datenverkehr enthältTSEine optionale PFS-Einstellung (Perfect Forward Secrecy), die ein neues Paar Diffie-Hellman-Schlüssel erstellt, die zum Schutz der Daten verwendet werden (beide Seiten müssen PFS-fähig sein, bevor Phase 2 aktiviert wird).
- 4. Wenden Sie die Crypto Map auf die externe Schnittstelle an:

crypto map outside_map 20 set ikev1 transform-set myset crypto map outside_map 20 set pfs crypto map outside_map interface outside

NAT-Ausnahme

Stellen Sie sicher, dass der VPN-Datenverkehr keiner anderen NAT-Regel unterliegt. Dies ist die verwendete NAT-Regel:

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

Hinweis: Wenn mehrere Subnetze verwendet werden, müssen Sie Objektgruppen mit allen Quell- und Zielsubnetzen erstellen und diese in der NAT-Regel verwenden.

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

Vollständige Beispielkonfiguration

Nachfolgend finden Sie die vollständige Konfiguration für Standort 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
```

Konfigurieren von Standort A für ASA Version 8.2 und frühere Versionen

In diesem Abschnitt wird die Konfiguration von Standort A für ASA Version 8.2 und frühere Versionen beschrieben.

Phase 1 (ISAKMP)

Führen Sie die folgenden Schritte für die Konfiguration von Phase 1 aus:

1. Geben Sie diesen Befehl in die CLI ein, um ISAKMP (Internet Security Association and Key Management Protocol) auf der externen Schnittstelle zu aktivieren:

crypto isakmp enable outside

Hinweis: Da mehrere Versionen von IKE (IKEv1 und IKEv2) nicht mehr unterstützt werden, wird ISAKMP verwendet, um auf Phase 1 zu verweisen.

2. Erstellen Sie eine ISAKMP-Richtlinie, die die Algorithmen/Methoden definiert, die für Phase 1 verwendet werden sollen.

Hinweis: In dieser Beispielkonfiguration wird das Schlüsselwort IKEv1 von Version 9.x wird ersetzt durch ISAKMP.

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

3. Erstellen Sie eine Tunnelgruppe für die Peer-IP-Adresse (externe IP-Adresse 5515) mit dem vorinstallierten Schlüssel:

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

Phase 2 (IPsec)

Führen Sie die folgenden Schritte für die Konfiguration von Phase 2 aus:

1. Ähnlich wie bei der Konfiguration in Version 9.x müssen Sie eine erweiterte Zugriffsliste erstellen, um den gewünschten Datenverkehr zu definieren.

access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

 Definieren Sie einen TS, der alle verfügbaren Verschlüsselungs- und Hashing-Algorithmen enthält (die angebotenen Probleme haben ein Fragezeichen). Stellen Sie sicher, dass sie mit der Konfiguration auf der anderen Seite übereinstimmt.

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

- 3. Konfigurieren Sie eine Crypto Map, die folgende Komponenten enthält: Die Peer-IP-AdresseDie definierte Zugriffsliste, die den relevanten Datenverkehr enthältTSEine optionale PFS-Einstellung, die ein neues Paar Diffie-Hellman-Schlüssel erstellt, die zum Schutz der Daten verwendet werden (beide Seiten müssen PFS-fähig sein, damit Phase 2 aktiviert wird).
- 4. Wenden Sie die Crypto Map auf die externe Schnittstelle an:

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-Ausnahme

Erstellen Sie eine Zugriffsliste, die den Verkehr definiert, der von den NAT-Prüfungen ausgenommen werden soll. In dieser Version ähnelt sie der Zugriffsliste, die Sie für den gewünschten Datenverkehr definiert haben:

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

Wenn mehrere Subnetze verwendet werden, fügen Sie derselben Zugriffsliste eine weitere Zeile hinzu:

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

Die Zugriffsliste wird mit der NAT verwendet, wie hier gezeigt:

nat (inside) 0 access-list nonat

Hinweis: Das "inside" bezieht sich auf den Namen der internen Schnittstelle, an der die ASA den Datenverkehr empfängt, der mit der Zugriffsliste übereinstimmt.

Vollständige Beispielkonfiguration

Nachfolgend finden Sie die vollständige Konfiguration für Standort 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

Gruppenrichtlinie

Gruppenrichtlinien werden verwendet, um spezifische Einstellungen für den Tunnel zu definieren. Diese Richtlinien werden zusammen mit der Tunnelgruppe verwendet.

Die Gruppenrichtlinie kann entweder als intern definiert werden, d. h., die Attribute werden von den Attributen abgefragt, die auf der ASA definiert sind, oder sie kann als extern definiert werden, wobei die Attribute von einem externen Server abgefragt werden. Mit diesem Befehl wird die Gruppenrichtlinie definiert:

group-policy SITE_A internal

Hinweis: Sie können mehrere Attribute in der Gruppenrichtlinie definieren. Eine Liste aller möglichen Attribute finden Sie im Abschnitt <u>Configuring Group Policies (Konfigurieren von Gruppenrichtlinien)</u> der Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series, Version 5.2.

Optionale Gruppenrichtlinienattribute

Die Fehlermeldung vpn-tunnel-protocol legt den Tunneltyp fest, auf den diese Einstellungen angewendet werden müssen. In diesem Beispiel wird IPsec verwendet:

svc SSL VPN Client webvpn WebVPN

vpn-tunnel-protocol ipsec - Versions 8.2 and prior vpn-tunnel-protocol ikev1 - Version 8.4 and later

Sie haben die Möglichkeit, den Tunnel so zu konfigurieren, dass er inaktiv bleibt (kein Datenverkehr) und nicht ausfällt. Um diese Option zu konfigurieren, müssen Sie vpn-idle-timeout - Attributwert muss Minuten dauern, oder Sie können den Wert auf none, was bedeutet, dass der Tunnel nie abwärts geht.

Hier ein Beispiel:

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;

Die Fehlermeldung default-group-policy definiert die Gruppenrichtlinie, die verwendet wird, um bestimmte Richtlinieneinstellungen für den erstellten Tunnel zu übertragen. Die Standardeinstellungen für die Optionen, die Sie nicht in der Gruppenrichtlinie definiert haben, stammen aus einer globalen Standardgruppenrichtlinie:

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

Überprüfung

Überprüfen Sie anhand der Informationen in diesem Abschnitt, ob Ihre Konfiguration ordnungsgemäß funktioniert.

ASDM

Um den Tunnelstatus vom ASDM aus anzuzeigen, navigieren Sie zu Monitoring > VPN. Diese Informationen werden bereitgestellt:

- Die Peer-IP-Adresse
- Das Protokoll, das zum Erstellen des Tunnels verwendet wird.
- Der verwendete Verschlüsselungsalgorithmus
- Der Zeitpunkt, zu dem der Tunnel hochgefahren wurde, und die Betriebszeit
- Die Anzahl der empfangenen und übertragenen Pakete

Tipp: Klicken Refresh um die neuesten Werte anzuzeigen, da die Daten nicht in Echtzeit aktualisiert werden.

Help								Type hopic to whatsh	1.64
IN Store (Reten Obal	Otward 2 Hoto	F						
diaday > VIII.> V	19 Statelius > Sende								
		(Contractor)							
rsec		SSL VPN				E-railmox	PilloedBaarong	Total	Total
CORE!	Site-to-Site	Gentesr	With Client	listive	Sotal		- Samerana (Cursula
	1	- 1	0	0	0	. 0	0	1	2
ter by: IFac Sta-k		- Al Seasare -		. the					
amector Hufe	Pretocol	Login Time		Eves Tr.					
IP Address	Encryption	Duration	Mark Mark	Bytes Ro					
2.6.1	405120	in the Sta		-					
sort VPN memoria, re	ght-old-on the above tai	ble and select Table Sort Ord	der from populat menu.						
age of Face - All Second	· ·	. He	specif Genetices						
					and the second sec				
					. formation				int industry
ŧ.				_	. tarter.		2000 J		Lex Updated
Halp							joses (2	Frie Kor & serve	
Help I and Series (CA	eter Otax (Ofweed ? Hote		_			jose 2	Five Kox, b texto	
Help Telp Generation 2 Million 200	netes Otos (Onward 💡 Hate		_			joses ji	NOT TO IT D SOLV	
Help I and Source QA Reactions - VIII - 10	letes of los (Oread State					joses ji	The for the service	
Help Help Terden 2 MR 2 MR Fr	i let esi 💽 tadi (11. Statistica - Sensier	Active		Gmildre		Peak Concurrent	jones 2	For tex b servin	
Help Description 2 APR 2 APR Annotation 2 APR 2 APR April 10 APR April 10 APR	n fortes 💽 tast (11 Statistics - Sensition	Normand V Holy		Qualifiere 1		Peek Concurrent 41 41	jona 2	Free tox b soron	
Help Dig Store () forming 2: VII 2: VII pr to-Star VII Co-STRAC	i fortesi 💽 tasi (R Statistica - Sanaa	Differented Protocologi an Active		Candebre 1 1		Pail Concernent 41 41	joses ji	Furt tox b serve Sector 3 3	
Hely Hely Foreigne 2 173 a 101 pr pr pr to-Site 1991 Gri (Prec	fetes 💽 tox (Orward ? Hos		Gandebre 1		Peek Concurrent 44 41	joses ji	Fore too: to sav dr.	
Hely Dente 2 MT 2 MT for loss 2 MT 2 MT pr pr pr ct-Sta VPA Ct-1 (Pace	retea 💽 tos (11 Statistics - Sensier	O Parward ? Help		Gandebre 1		Peil Concernent 4 11	jones ji	Interior to solver	
Holo Torologi 2 Store (C Torologi 2 MTR 2 MTR -to-Site VPI Co-1 (Proc. W Pr.: (Proc.Site 40)	n tetes i tos (11 Statistics > Sensier 13 a t	Affree of the second se		Canalebore 2 2 Miles		PubliConcurrent 41 41	joses jī	Interior to solver	
Help Help Forder = MR = M Forder = M F	i tetesh 💽 tas (15 Skettellas = Senater 1936 – V	Active		Considere 1 1		Pub Concentry 44 41	jose j1	Interior to some	
Help Help Sove Q Territor - VIT - VIT For Sove Q Territor - VIT - VIT For Sove Q For Sove Q Fo	sketesk 💽 bas (15 Sketeska - Secondar Ster • Pritad Encryfon Golf Park	Active Active Active Al Seasons – Logn Time Surgion	•	Camiletre 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Peek Concernent 41 45	jose ji	Pare tor to soroli factor 1	
Help Help Sont Q Sont Q Help He	dae • 7 7	Active Active Active Al Secure - Logis The System System Call Active Al Secure Call	•)	Candidate 1 1 Miles Note To Rose to		Pail Concentre 41 41	jores jr	France to concorre	
Help Help Storeter = VIII = 10 pr etc-bits VPi Criffwic Help Help Help Help Help Help Help Help Help Help Help Help Help Help Help Help Help Help	Steres States	Active Active Al Seasers Logy Time Duration Time (CL) CLOCK And Decision		Considere 1 1		Peek Concurrent 44 41	jores jr	For loc 0 sorts	
Help Help Der Control State Particles > MS + M Particles > M Particles	dae •	Active Active Additional Addition	P 10.211	Considere 1 1 Main X		Peek Concurrent 44 11	jones ji	Inche 3 3	
Hele Terefore 2 MTR 2 MT Pro- to-Sate VPL Co-10 Proc. ar By: Proc.Sate do wrc.300 Huffe Praderess	ate •	Active Active Ad Secure - Upgin Time Departure Ad Secure - Constant Ad Secure -	P PUBLE	Considere 1 1 Materia Nata No		Peil Concentrat 4 11	jones ji	Inclus 1	Les updates
Help Help Territor - VIT - VIT For the State Coll (Pace art Pyr. Precision do wrection Profile P Address Address	Site of a second	Active Active Active Al Sequence – Logistics Active Al Sequence – Logistics Active Al Sequence –	- 10-2011	Curulebre 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Peek Concernent 41 41	joses ji	Interior to solve	
Help Help Sont Q Territor - MTR - MT Pr to-Star V91 Ch-1 (Pac) ar Tr, Preschardo mecclan Huffe (P address Territor - M	stetes Sast	Active Ac	P 10.211	Candebre 1 2 1 Miles Note To Rote To		Pail Concentre 41 43	joes jr	For tex b series	
Help Source - MTR - MTR Pr 	steres Sources	Active Active Ad Security Ad Security System		Canaletre 1 1 Pres Pa		Peek Concurrent 41 41	jores jr	Port foot to sor of	
Hele Source - ATR - TT Pro- to-Sate VPI Grid (Proc. art By: Energiatedo wrc. State - Sate Atr Pro- Pro- Sate - Sate VPI Grid (Proc. Sate - Sate Atr Pro- Sate - Sate - S	das v r Hotela Statutions - Securitor data v r Hotelada Batta Part Securitoria	Active Active Al Sessena – Upper Steel Al Sessena – Upper Steel Al Sessena – Upper Steel Active	• •	Considere 2 2 Moto X		Peek Concurrent 44 11	jores ji	Inche 3 3	
Help Help Forces = VFR = VF Forces = VFR = VF Forces Forces Help Help Forces Help	date v v	Active Active Al Saussers – Logis Tale Cognition Cogniti		Considere 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1		Peil Concernent 4 12	jores ji	Inclus 1	Les Lydere
Help Help Territor - VIT - TT Pr to-Star VPi Cr I Prec: ar Py: Prec: Star So wrection Profile P Address Address	Site of State of Stat	Active Active Active Addisections Addisectio		Curuletse 1 1 Mise Notes N		Pell Concurrent 41 42		Part tox b soron	
Help Help Sout C and Review - MTR - MTR Pro- to-Star V91 Ch-1 (Proc.) art Type: Pro- star Type: Pro- South Help Pro- South Help Pro- Pro- South Help Pro- South Help Pro- South Help Pro- Pr	steres State	Attra		Candidate 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Pail Concentre 41 41		For text to control	
Help Source - MS - M Protection - MS - M Protection - MS - M Protection - MS - M Protection - M Protection - Function Protection - Function Protection Protection - Function	Steres Social States - Sector Pation Company Sector Patients of	Active Active Al Seasons - Logistics System Al Seasons - Logistics Al Seasons - Logistics Active	P 10.2111	Considere 1 1		Peek Concurrent 41 11		For loc 0 sorts	
Hele Terefore 2 MTR 2 MTR Pro- to-Sate VPI Co-1 (Proc. ar Byc. (Proc.Sate do mrc.Sate Null Pro- Address 2 Sate 1 Sate 1 Sat	dae •	Active Active Ad Seasons – Upp Time Days Store Ad Seasons – Upp Time Active Ad Seasons –	P* 10.4211	Considere 1 1 Miter N Miter N		Peek Concurrent 44 91		Fore too: to solve)	
Hele Source - MR - M Forder - MR - M Forder - MR - M Forder - MR - M Forder - M Ford	dae • 1 -	Active Active Ad Sectors Ad Sectors Cognition	•	Considere 2 2 2 2 2 2 2 2 2 2 2 2 2		Peek Concurrent 44 11		Inclus 3 3	
Help Source - MR - M Review - MR - M Review - MR - M Review - MR - M Review - MR Review - M Review - M Rev	Alerea to too (11 Statistics - Senser Alerea to (Pringer Pri	Active Active Al Saussers – Logis Tale Cogis		Considere 1 1 1 1 1 1 1 1 1 1 1 1 1		Peil Concentri 4 11		Partie to: biordi	
Help Help Sont Constraints For the Sont C	Steller () Social () Steller () Stel	Attras Attras Af Sequence - Upper Time Burdson Al Sequence - Upper Time Burdson Al Sequence -	P 10.011	Candidate 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Pail Concentre 41 41		Port tox b torror.	
Help U Sont C Territoria - MTR - MT Territoria - MTR - MT Territoria - MTR - MT Territoria Territoria MT TER - MTR - MT Territoria MT TER - MT Territoria MT TER - MT MT TER - MT MT MT TER - MT MT MT TER - MT MT MT MT MT MT MT MT MT MT	Site • • •	Active Active Al Seamers - Logis Time Duration Al Seamers - Logis Time Al Seamers - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time - Logis Time -	e fonzosa nens patientes patientes	Considere 1 1 Proto Do		Peik Circursett 41 41		Port foot to sorvit. A 3 3 3	
Hele Terreter 2 MR 2 MR Pro- to-Star UPA Co-Star UPA Co-Star UPA Star Drace Terreter 2 MR Pro- Pro- Star Drace Terreter 2 MR Pro- Star Drace Pro- Star Drace Pro- P	A fortest 💽 box (R Statistics - Service date • 7 Patrod Patrod Box (10 Patrod Box (10 Patrod Patrod Box (10 Patrod Pa	Active Active Ad Southers - Logistion Constant C	• Ton popul retrus get Sessins	Considere 1 2 Mos No Nos No No Nos No No No No No No No No No No No No No N		Pesk Concurrent 44 11		Fore too: to servite a 3 3	

CLI

tara Refreshed SuccessMix

In diesem Abschnitt wird beschrieben, wie Sie Ihre Konfiguration über die CLI überprüfen.

| 🙀 🔂 | | 🙆 | value acatemetre

14

Phase 1

Geben Sie diesen Befehl in die CLI ein, um die Phase 1-Konfiguration auf Seite von Standort B (5515) zu überprüfen:

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**

Geben Sie diesen Befehl in die CLI ein, um die Phase-1-Konfiguration auf Seite von Standort A (5510) zu überprüfen:

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

Phase 2

Die Fehlermeldung show crypto ipsec sa zeigt die IPsec-SAs an, die zwischen den Peers erstellt werden. Der verschlüsselte Tunnel wird für den Datenverkehr zwischen den Netzwerken 10.1.1.0 und 10.2.2.0 zwischen den IP-Adressen 192.168.1.1 und 172.16.1.1 erstellt. Hier sehen Sie die beiden ESP-SAs, die für den ein- und ausgehenden Datenverkehr erstellt wurden. Der Authentication Header (AH) wird nicht verwendet, da keine AH-SAs vorhanden sind.

Geben Sie diesen Befehl in die CLI ein, um die Phase-2-Konfiguration auf Seite von Standort B (5515) zu überprüfen:

```
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
```

Geben Sie diesen Befehl in die CLI ein, um die Phase-2-Konfiguration auf Seite von Standort A (5510) zu überprüfen:

```
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
```

Fehlerbehebung

Verwenden Sie die Informationen in diesem Abschnitt, um Konfigurationsprobleme zu beheben.

ASA Version 8.4 und höher

Geben Sie die folgenden Debugbefehle ein, um den Standort des Tunnelausfalls zu bestimmen:

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

Hier ist ein vollständiges Beispiel für die Debug-Ausgabe:

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
```

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

Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing VID pavload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley begin quick mode Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21 Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds. IPSEC: New embryonic SA created @ 0x75298588, SCB: 0x75C34F18, Direction: inbound SPI : 0x03FC9DB7 Session ID: 0x00004000 VPIF num : 0x0000002 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got SPI from key engine: SPI = 0x03fc9db7 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constucting guick mode Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing proxy ID Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Transmitting Proxy Id: Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending Initial Contact Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing qm hash payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500 Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing SA payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing nonce payload Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,

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

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

Dst mask: 255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7 Rule ID: 0x74e1b4a0 IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7 Rule ID: 0x6f0de830 IPSEC: New inbound permit rule, SPI 0x03FC9DB7 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x03FC9DB7 Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7 Rule ID: 0x6f0de8d8 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher: received KEY_UPDATE, spi 0x3fc9db7 Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P2 rekey timer: 24480 seconds. Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2 COMPLETED (msgid=4c073b21)

Geben Sie die folgenden Debugbefehle ein, um den Standort des Tunnelausfalls zu bestimmen:

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

Hier ist ein vollständiges Beispiel für die Debug-Ausgabe:

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

ASA GW VID Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys for Responder... Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID pavload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR ID received 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing VID payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing ID payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing dpd vid payload Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1 rekey timer: 82080 seconds. Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id = 4c073b21 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing nonce payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP

Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing notify payload Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa not found by addr Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside_map, seq = 20... Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside_map, seq = 20 is a successful match Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside_map Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0xAB5C63A8, SCB: 0xABD54E98, Direction: inbound SPT : 0x1BA0C55C Session ID: 0x00004000 VPIF num : 0x0000001 Tunnel type: 121 Protocol : esp Lifetime : 240 seconds Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI from key engine: SPI = 0x1ba0c55c Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley constucting guick mode Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing blank hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec SA payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing IPSec nonce payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing proxy ID Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting Proxy Id: Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing qm hash payload Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder sending 2nd QM pkt: msg id = 4c073b21 Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all IPSEC SAs Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating Quick Mode Key!

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

```
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0x03fc9db7
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a
KEY_ADD msg for SA: SPI = 0x03fc9db7
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C
Flags: 0x0000006
SA : 0xAB5C63A8
SPI : 0x1BA0C55C
MTU : 0 bytes
VCID : 0x0000000
Peer : 0x0000F99C
SCB : 0x0150B419
Channel: 0xA7A98400
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0001169C
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7
Flags: 0x0000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x0000000
Peer : 0x0001169C
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x0000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C
Rule ID: 0xAB8D98A8
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
```

Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x1BA0C55C Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C Rule ID: 0xABD55CB0 IPSEC: New inbound permit rule, SPI 0x1BA0C55C Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x1BA0C55C Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C Rule ID: 0xABD55D48 Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received KEY_UPDATE, spi 0x1ba0c55c Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey timer: 27360 seconds. Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED (msgid=4c073b21)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.