Dynamischer IPsec-Tunnel zwischen einer statisch adressierten ASA und einem dynamisch adressierten Cisco IOS-Router, der ein Konfigurationsbeispiel für CCP verwendet

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Hintergrundinformationen Konfigurieren Netzwerkdiagramm Konfigurationen Überprüfen Überprüfen Überprüfen des Tunnelparametern durch CCP Überprüfen des Tunnelparameter über die ASA CLI Überprüfen Sie die Tunnelparameter über die Router-CLI. Fehlerbehebung Zugehörige Informationen

# **Einführung**

Dieses Dokument enthält eine Beispielkonfiguration, wie die PIX/ASA Security Appliance so konfiguriert wird, dass sie dynamische IPsec-Verbindungen vom Cisco IOS<sup>®</sup> Router akzeptiert. In diesem Szenario wird der IPsec-Tunnel erstellt, wenn der Tunnel nur vom Routerende aus initiiert wird. ASA konnte wegen der dynamischen IPsec-Konfiguration keinen VPN-Tunnel initiieren.

Diese Konfiguration ermöglicht der PIX Security Appliance die Erstellung eines dynamischen IPsec LAN-to-LAN (L2L)-Tunnels mit einem Remote-VPN-Router. Dieser Router erhält dynamisch seine externe öffentliche IP-Adresse von seinem Internetdienstanbieter. Dynamic Host Configuration Protocol (DHCP) stellt diesen Mechanismus bereit, um IP-Adressen dynamisch vom Anbieter zuzuweisen. Dadurch können IP-Adressen wiederverwendet werden, wenn Hosts sie nicht mehr benötigen.

Die Konfiguration auf dem Router erfolgt mithilfe des <u>Cisco Configuration Professional</u> (CCP). CCP ist ein GUI-basiertes Gerätemanagement-Tool, mit dem Sie Cisco IOS-basierte Router konfigurieren können. Unter <u>Grundlegende Routerkonfiguration mit Cisco Configuration</u> <u>Professional</u> finden Sie weitere Informationen zum Konfigurieren eines Routers mit CCP. Weitere Informationen und Konfigurationsbeispiele zur Einrichtung von IPsec-Tunneln, die ASAund Cisco IOS-Routern verwenden, finden Sie unter <u>Site-to-Site-VPN (L2L) mit ASA</u>.

Unter <u>Site-to-Site-VPN (L2L) mit IOS</u> finden Sie weitere Informationen und ein Konfigurationsbeispiel für die dynamische Einrichtung von IPSec-Tunneln unter Verwendung von PIX und Cisco IOS-Routern.

# Voraussetzungen

#### **Anforderungen**

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass ASA und Router über eine Internetverbindung verfügen, um den IPSEC-Tunnel einzurichten.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Router1812, der Cisco IOS Software Release 12.4 ausführt
- Cisco ASA 5510 Softwareversion 8.0.3

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## **Hintergrundinformationen**

In diesem Szenario liegt das Netzwerk 192.168.100.0 hinter der ASA, und das Netzwerk 192.168.200.0 befindet sich hinter dem Cisco IOS-Router. Es wird davon ausgegangen, dass der Router seine öffentliche Adresse über DHCP vom ISP erhält. Da dies ein Problem bei der Konfiguration eines statischen Peers am ASA-Ende darstellt, müssen Sie sich der Methode der dynamischen Verschlüsselungskonfiguration nähern, um einen Site-to-Site-Tunnel zwischen ASA und dem Cisco IOS-Router einzurichten.

Die Internetbenutzer am ASA-Ende werden in die IP-Adresse der externen Schnittstelle übersetzt. Es wird davon ausgegangen, dass NAT nicht auf dem Cisco IOS-Router-Ende konfiguriert ist.

Dies sind die wichtigsten Schritte, die am ASA-Ende konfiguriert werden müssen, um einen dynamischen Tunnel einzurichten:

- 1. ISAKMP-bezogene Konfiguration Phase 1
- 2. Konfiguration der NAT-Freistellung
- 3. Dynamische Konfiguration der Crypto Map

Für den Cisco IOS-Router ist eine statische Crypto Map konfiguriert, da angenommen wird, dass die ASA über eine statische öffentliche IP-Adresse verfügt. Dies ist die Liste der wichtigsten Schritte, die auf dem Cisco IOS-Router-Ende konfiguriert werden müssen, um einen dynamischen IPSEC-Tunnel einzurichten.

- 1. ISAKMP-bezogene Konfiguration Phase 1
- 2. Statische Kryptozuordnungskonfiguration

Diese Schritte werden in diesen Konfigurationen ausführlich beschrieben.

# **Konfigurieren**

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

### **Netzwerkdiagramm**

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



### **Konfigurationen**

Dies ist die IPsec-VPN-Konfiguration auf dem VPN-Router mit CCP. Gehen Sie wie folgt vor:

 Öffnen Sie die CCP-Anwendung, und wählen Sie Configure > Security > VPN > Site-to-Site-VPN aus. Klicken Sie auf die Registerkarte Ausgewählte starten.



#### 2. Wählen Sie Schritt für Schritt den Assistenten aus und klicken Sie dann auf



3. Geben Sie die IP-Adresse des Remote-Peers zusammen mit den Authentifizierungsdetails

and the second se	Contraction of the second second second second						
VPN Wizard	Collection Information	VPN Connection Information					
	determenter of this will contact	Pasicalement Cetans.					
~ ~	Peer Identity						
	Select the type of peer(s) used for this connection:	VPN Peer with static P address					
	Enter the IP address of the remote peer.	209.165.201.2					
	Authentication						
	Authentication ensures that each and o	A REAL COMPLEX STREET,					
	key.	I the VPN connection uses the same secret					
	Pre-shared Keys	C Digital Certificates					
	Pre-shared Keys     pre-shared keys	C Digital Certificates					
R	Pre-shared Keys     Pre-shared Keys     Re-enter Key:	C Digital Certificates					
	Pre-shared Keys     pre-shared keys     Re-enter Key:	C Digital Certificates					
	Pre-shared Keys     pre-shared Keys     Re-enter Key:	C Digital Certificates					

4. Wählen Sie die IKE-Angebote aus, und klicken Sie auf

VPN Wizard	IKE pi IKE pi metho device device	oposals oposals s of that is o For the <sup>1</sup> should b	specify the en used by this n VPN connecti e configured	cryption algo outer when n on to be esta with at least	rithm, authenticat egotiating a VPN blished with the r one of the policie	ion algorithm and connection with t emote device, the s listed below.	d key exchange he remote s remote
	Olick	the Add Priority	button to add Encryption 3DES	1 more policie Hash SHA_1	D-H Group group2	Authentication	nisting policy Type Cisco CP Defa
					group		
KE				-			

5. Definieren Sie die Details zum Transformationssatz, und klicken Sie auf

Site-to-Site VPN Wizord				le l
VPN Wizard	Transform Set A transform set specifie data in the VPN tunnel, communicate, the remu one selected below Click the Add button to transform set Select Transform Set	es the encryption and auth Since the two devices mu ofe device must be config o add a new transform se	ientication algorit ist use the same ured with the sam t and the Edit bu	nms used to protect the algorithms to le transform set as the mon to edif the specified
	myset	2		
	Details of the speci	fied transform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
RA				3
	Add	Edit.	Back Next >   F	Cancel Help

Weiter.

6. Definieren Sie den zu verschlüsselnden Datenverkehr, und klicken Sie auf

VPN Wizard	Traffic to protect IPSec rules define the b protected by this VPN co device. You can protect specify an IPSec rule th	raffic, such as fil onnection. Other all traffic betwee al defines the tra	e trans r data tr in a pa affic typ	fers (FTP) and e-mail (Si affic will be sent unprote dicular source and destin es to be protected.	MTP) tha cted to t nation s	at will b he rem ubnet, c	e ote or
	Protect all traffic betw	een the followin	g subn	ets			
	Local Network			Remote Network			
	Enter the IP address a the network where IPS	and subnet mas Sec traffic origin:	ik of ate:s.	Enter the IP Address the destination Netwo	and Sub xk.	net Ma	sk
	IP Address:	-		IP Address:			
	192168.200.0	,		192.168.100.0			
	Subnet Mask:	1.100	n i	Subnet Mask		1.00	6
	299.299.299.0	01.74		255.255.255.0	-		6
D	← Create/Select an acce	ess-list for IPSe	c traffic	, , 23	,	- <mark>18</mark> - 72	

7. Überprüfen Sie die Zusammenfassung der IPsec-Konfiguration für die Verschlüsselung, und klicken Sie auf **Fertig** 

VPN Wizard	Summary of the	Configuration		
	Click Finish to d	eliver the configuration	on to the router.	
	IKE Policies:			19
	Hash	DH Group	Authentication	Encryption
	MD5 SHA_1	group2 group2	PRE_SHARE PRE_SHARE	DES 3DES
1A	Transform Sets Name ESP E ESP In Mode:	: myset ncryption ESP_DES tegrity ESP_MD5_HI FUNNEL	мс	
NA	IPSec Rule: permit	all ip traffic from 192	.168.200.0 0.0.0.255 to	192.168.100.0.0.
~1	Test VPN cor	mectivity after configu	uting]	

8. Klicken Sie auf **Deliver**, um die Konfiguration an den VPN-Router zu

enden.	
Deliver Configuration to Router	
Deliver delta commands to the router's running config. Preview commands that will be delivered to the router's running configuration.	
crypto ipsec transform-set inyset esp-md5-hmac esp-des mode tunnel exit crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to209.165.201.2 set transform-set myset set peer 209.165.201.2 match address 101 exit interface FastEthernet1 po crypto map	
The differences between the running configuration and the startup configuration a the router is turned off.	are lost whenever
Deliver Cancel Save to file Help	

Commands Delivery Status	
Command Delivery Status:	=1
Preparing commands for delivery Submitting 31 commands, please wait Configuration delivered to router. Copying the Running config to Startup config of your router. Please wait Running config copied successfully to Startup Config of your router.	12
	2
ОК	

9. Klicken Sie auf **OK**.

## CLI-Konfiguration

- <u>Ciscoasa</u>
- VPN-Router

#### Ciscoasa

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.254
!
interface Ethernet0/1
nameif inside
 security-level 100
ip address 192.168.100.1 255.255.255.0
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0
no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
authentication pre-share
encryption des
hash md5
 group 2
lifetime 86400
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

inspect	h323 ras
inspect	netbios
inspect	rsh
inspect	rtsp
inspect	skinny
inspect	esmtp
inspect	sqlnet
inspect	sunrpc
inspect	tftp
inspect	sip
inspect	xdmcp
1	
service-po	olicy global_policy global
prompt hos	stname context
Cryptoched	cksum:d41d8cd98f00b204e9800998ecf8427e
: end	
ciscoasa(c	config)#

CCP erstellt diese Konfiguration auf dem VPN-Router.

```
VPN-Router
VPN-Router#show run
Building configuration...
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
1
!
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQ01
1
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
encrypt 3des
 authentication pre-share
group 2
!
crypto isakmp policy 2
hash md5
authentication pre-share
group 2
!
!
crypto isakmp key cisco123 address 209.165.201.2
1
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
1
1
crypto map SDM_CMAP_1 1 IPSec-isakmp
description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
match address 101
1
!
interface BRI0
no ip address
shutdown
!
interface Dot11Radio0
no ip address
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio1
no ip address
 shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
!
interface FastEthernet0
ip address 192.168.200.1 255.255.255.0
duplex auto
speed auto
1
interface FastEthernet1
ip address dhcp
duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
no ip address
shutdown
!
interface FastEthernet3
no ip address
shutdown
!
interface FastEthernet4
no ip address
shutdown
interface FastEthernet5
no ip address
shutdown
1
interface FastEthernet6
no ip address
shutdown
1
interface FastEthernet7
no ip address
shutdown
!
interface FastEthernet8
no ip address
shutdown
!
interface FastEthernet9
no ip address
shutdown
```

```
interface Vlan1
no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
1
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
privilege level 15
login local
transport input telnet ssh
1
no scheduler allocate
end
```

# <u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- Überprüfen der Tunnelparameter über CCP
- Überprüfen des Tunnelstatus über die ASA CLI
- <u>Überprüfen der Tunnelparameter über die Router-CLI</u>

## Überprüfung von Tunnelparametern durch CCP

 Überwachen des Datenverkehrs durch den IPsec-Tunnel

	and the second			
pplication Help				
Norme 🛞 teefigure 🚮 He	anar 🕴 🚖 🥹	Cisc	o Configura	tion Professional CISC
Select Conversions Hernberg	w Nonitor > Security > VPN State	us > 1PSec Turnels		
18.37.246.111 (*	nice and an and a second second			
Router	ST VPH Bratus			
Sugara	CMI.Phi Turneis	Each row represents one (PSec Tunnel		Stop Wonitoring   Test Tannel. Update
Const Hotel	A DERIVER AND A DERIVER	finale formers form	Tanana Distan	Gelectiters to Nordan
Solar anteri	GETVPN KASSIN	200 105 200 1 210 106 201 2 200 105 201 2 500	Contraction of the second	P Exceptulation Packets
Distant Torviale	GEOETVPN Group Member	and the second	a	P Decapeulation Packets
Distant Turvati				P Received Errar Packets
DINI 64				
The second se		-		34
Dana araya		Turvel Safat		
Tarec collects		Very Hervel Roal See size every 13 cec 🗸		
PALL HAN		Encounterior Partieto Decastario	on Packets, Sena Exce	Paciate Paciety December Paciety
		100 Det	1	
	1	Emaposition Pasteria	Same and same	Becagendation: Peckela
	0		64	
			e 99 311	
	1.		<ul> <li>•• 211</li> </ul>	
			10	
		Unida Technology	12:51-25	Time Data and sch
		1 888 (1993) 2 16 83		THE REPORT OF THE PARTY OF THE
		Secal Data Packets		Reserved First Parkets
		Sector Data ( Sector Se		Spinised from Parkets
				Telefore Fills Patkets
			05	
			03	
		Second Larger Parkets           6           1	1	The Doctof (S)

• Überwachen Sie den Status der Phase I ISAKMP



#### Überprüfen des Tunnelstatus über die ASA CLI

Überprüfen Sie den Status von Phase I ISAKMP SA.
 ciscoasa#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: 209.165.200.12
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE
ciscoasa#
```

**Hinweis:** Beachten Sie die Rolle als Responder, die angibt, dass der Initiator dieses Tunnels am anderen Ende ist, z. B. der VPN-Router.

```
    Überprüfen Sie die Parameter der Phase II IPSEC SA.

 ciscoasa#show crypto ipsec sa
 interface: outside
     Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2
       local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
       current_peer: 209.165.200.12
       #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
       #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12
       path mtu 1500, IPSec overhead 58, media mtu 1500
       current outbound spi: E7B37960
     inbound esp sas:
       spi: 0xABB49C64 (2880740452)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0xE7B37960 (3887298912)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
```

#### Überprüfen Sie die Tunnelparameter über die Router-CLI.

• Überprüfen Sie den Status von Phase I ISAKMP SA. VPN-Router#show crypto isakmp sa dst src state conn-id slot status 209.165.201.2 209.165.200.12 QM\_IDLE 1 0 ACTIVE

```
    Überprüfen Sie die Parameter der Phase II IPSEC SA.

 VPN-Router#show crypto ipsec sa
 interface: FastEthernet1
     Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12
    protected vrf: (none)
    local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
    current_peer 209.165.201.2 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
     #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 6, #recv errors 0
      local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
      path mtu 1500, ip mtu 1500
      current outbound spi: 0xABB49C64(2880740452)
      inbound esp sas:
       spi: 0xE7B37960(3887298912)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
         sa timing: remaining key lifetime (k/sec): (4481818/3375)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0xABB49C64(2880740452)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
         sa timing: remaining key lifetime (k/sec): (4481818/3371)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE
      outbound ah sas:
      outbound pcp sas:
```

## **Fehlerbehebung**

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

```
• Abbau der vorhandenen Kryptoverbindungen.
ciscoasa#clear crypto ipsec sa
```

```
ciscoasa#clear crypto isakmp sa
```

VPN-Router#clear crypto isakmp

 Verwenden Sie Debug-Befehle, um Probleme mit dem VPN-Tunnel zu beheben.Hinweis: Wenn Sie Debugging aktivieren, kann dies den Betrieb des Routers unterbrechen, wenn bei Internetworks hohe Ladebedingungen auftreten.Verwenden Sie debug-Befehle mit Vorsicht. Im Allgemeinen wird empfohlen, dass diese Befehle nur unter der Anleitung des technischen Supports für den Router verwendet werden, wenn spezifische Probleme behoben werden. ciscoasa#debug crypto engine

ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPSec ciscoasa#

VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISAKMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#

Weitere Informationen zu Debugbefehlen finden Sie unter <u>debug crypto isakmp</u> in <u>Understanding</u> and <u>Using debug Commands</u>.Zugehörige Informationen

- Support-Seite für IPSEC-Verhandlung/IKE-Protokolle
- Dokumentation für die Betriebssystem-Software der Cisco ASA Security Appliance
- Häufigste IPSEC VPN-Fehlerbehebungslösungen
- Anforderungen für Kommentare (RFCs)