Konfigurationsbeispiel für IPsec zwischen zwei IOS-Routern mit sich überschneidenden privaten Netzwerken

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurationen Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie der Cisco IOS-Router in einem standortübergreifenden IPsec-VPN mit sich überschneidenden privaten Netzwerkadressen hinter VPN-Gateways konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS 3640-Routern, auf denen die Softwareversion 12.4 ausgeführt wird.

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).

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:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Sowohl Private_LAN1 als auch Private_LAN2 verfügen über das IP-Subnetz 192.168.1.0/24. Dadurch wird der sich überschneidende Adressbereich hinter jeder Seite des IPsec-Tunnels simuliert.

In diesem Beispiel führt der Site_A-Router eine bidirektionale Übersetzung durch, sodass die beiden privaten LANs über den IPsec-Tunnel kommunizieren können. Die Übersetzung bedeutet, dass Private_LAN1 Private_LAN2 durch den IPsec-Tunnel als 10.10.10.0/24 und Private_LAN2 durch den IPSec-Tunnel als 10.5.5.0/24 "erkennt".

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- <u>SDM-Konfiguration für Standort_A-Router</u>
- <u>CLI-Konfiguration für Standort A-Router</u>
- Konfiguration des Standorts_B-Routers

SDM-Konfiguration für Standort_A-Router

Hinweis: In diesem Dokument wird davon ausgegangen, dass der Router mit grundlegenden Einstellungen wie Schnittstellenkonfiguration usw. konfiguriert ist. Weitere Informationen finden Sie unter <u>Grundlegende Routerkonfiguration mit SDM</u>.

NAT-Konfiguration

Gehen Sie wie folgt vor, um mithilfe von NAT SDM auf dem Site_A-Router zu konfigurieren:

 Wählen Sie Configure > NAT > Edit NAT Configuration, und klicken Sie auf Designate NAT Interfaces (NAT-Schnittstellen festlegen), um vertrauenswürdige und nicht vertrauenswürdige Schnittstellen wie gezeigt zu

fg	Configure	Monitor	@ Refres) h Save	S						
2	🖗 NAT										
	Create NAT Configuration Edit NAT Configuration Designate NAT Interfaces.										
	AT Interface Settin Select the list of inf inside / outside.	ng terfaces that you	want to c	lesignate as	×						
	interface	inside(trust	ed)	outside(untrus	te						
	Ethernet0/0			~							
	FastEthernet1/0										
	LoopbackO	~									
definieren.	• OK	Cancel		Help	ŀ						

- 2. Klicken Sie auf OK.
- 3. Klicken Sie auf **Hinzufügen**, um die NAT-Übersetzung wie dargestellt von innen nach außen zu

Add Addres	s Translation Rul	e			
 Static 	c O Dyn	amic			
Dire	ction: From insid	le to outs de	•		
т	ranslate from inte	rface			
Insi	de Interface(s):	Loopba	ackO		
IPa	ddress:	192.16	8.1.0		
Net	vork Mask(option:	al): 255.25	5.255.0	or	24
		· · · · · ·			
	ranslate to interfa	ce			
0	utside Interface(s)): Ethernet0	/0		
Ту	/pe:	IP addres	s	•	
in	terface:	Ethernet0)/0	Y	
IP	address:	10.5.5.0			
	- Redirect Por	·			
				_	
)riginal Port:	Т	ranslated Por	t:	
konfigurieren.	OK	Cancel	dieH l		
4. Klicken Sie auf					
– Network Address Translation R	ules				
Inside Interface(s): Loopbac	k0				
Outside Interface(s): Ethernet	VO				
	Translat	ad address	Dule 7	ime	
102 169 1 0.102 169 1 255	10.5.5.0.	eu address	Rule I Static	Abe	Add

5. Klicken Sie erneut auf Hinzufügen, um die NAT-Übersetzung wie dargestellt von außen in die Richtung von innen zu

Add A	ddress Transl	ation Rule								
6	Ptotic	C Dunamia								
	otatic	Obynamic								
	Direction: From outside to inside									
	Translate from interface									
	Outside Inter	rface(s):	Ethernet0/0							
	IP address:		10.10.10.0							
	Network Mas	sk(optional):	255.255.255.0	or 24						
			1							
	Translate	to interface —								
	Inside Inte	rface(s):	LoopbackO							
	IP address	5:	192.168.1.0							
		Niroct Port								
	C mon	Cupp								
	Original F	Port:	Translated P	ort:						
konfigurieren.		ОК	Cancel He	lp						
6. Klicken Sie auf										
– Network Address Tra	nslation Rules —									
Inside Interface(s):	Loopback0									
Outside Interface(s):	Ethernet0/0									
Original address		Translate	d address	Rule Type						
192.168.1.0-192. 192.168.1.0-192	168.1.255 168.1.255	10.5.5.0-1	0.5.5.255	Static						

Hinweis: Dies ist die entsprechende CLI-Konfiguration:

VPN-Konfiguration

Gehen Sie wie folgt vor, um mithilfe von VPN SDM auf dem Site_A-Router zu konfigurieren:

1. Wählen Sie **Configure > VPN > VPN Components > IKE > IKE Policies > Add**, um die IKE-Richtlinien wie in diesem Bild dargestellt zu

	Configu	ire IKE Policy	·			
	Priority:			Authen PRE_S	tication: 3HARE	•
	Encryption DES	n:	•	D-H Gr group1	oup:	¥
	Hash: MD5		•	Lifetim 24	e: 0 0	HH:MM:SS
definieren.		0K		Cancel	He	elp

2. Klicken Sie auf

<u>OK.</u>						
IKE	Policies				Add	Edit Del
	Priority	Encryption	Hash	D-H Group	Authentication	Туре
	10	DES	MD5	aroup1	PRE SHARE	User Defined

Hinweis: Dies ist die entsprechende CLI-Konfiguration:

3. Wählen Sie **Configure > VPN > VPN Components >IKE > Pre-shared Keys > Add**, um den Wert des vorinstallierten Schlüssels mit der Peer-IP-Adresse

	Key:		****	****		
	Re-e	enter Key:	****	****		
	Н	ost/Netwo	rk—			
	Туре	9:	IP A	ddress	•	
	IP A	ddress:	172	.16.1.2		
	Sub (Op	net Mask: tional)	255	.255.255.0		24
	🔽 Us	er Authent	icati	on (XAuth)		
festzulegen.		ОК		Cancel		Help
4. MICKEN SIE a	aul					

OK.

Pre-	shared Keys		Add
	Peer IP/Name	Subnet Mask	pre-shared key
	1701610	266 266 266 0	*****

Hinweis: Dies ist die entsprechende CLI-Konfiguration:

5. Wählen Sie **Configure > VPN > VPN Components > IPSec > Transform Sets > Add** aus, um ein Konfigurationssatz-*Myset* zu erstellen, wie in diesem Bild

	Add Tran	sform Set						
	Name: myset							
		Data integrity	/ with	encryption (ESP)			
	Integrity Algorithm: ESP_MD5_HMAC							
	Encry	ption Algorit/	hm:	ESP_DES				
						Show Advani		
gezeigt.		ОК		Cancel		Help		

6. Klicken Sie auf

OK.

ransform Set			Add.
Name	ESP Encryption	ESP Integrity	AH Integrity
myset	ESP_DES	ESP_MD5_HMAC	

nweis: Dies ist die entsprechende CLI-Konfiguration:

7. Wählen Sie **Configure > VPN > VPN Components > IPSec > IPSec Rules(ACLs) > Add**, um eine Crypto Access Control List (ACL) *101* zu

٩dd	a Rule						
	Name/Num	iber:			Туре	B:	
	101				Exte	ended Rul	е
	Descriptior	i:					
	Rule Entry						
	permit ip 1	0.5.5.0 0.255	.255.25	5 192.1	68.1.	.0 0.255.	Add
							Clone.
							Edit
							Delete
							Move L
	•					▶	Move Do
	Interfac	e Associatio	n				
	None.					Ass	ociate
erstellen.		ОК	Ca	ancel		Help	

8. Klicken Sie auf **OK**.



Hinweis: Dies ist die entsprechende CLI-Konfiguration:

9. Wählen Sie Configure > VPN > VPN Components > IPSec > IPSec Policies > Add aus, um Cryto Map mymap zu erstellen, wie in diesem Bild

a 0-	7010	1 1
uez	<u>en</u>	л
9	-0.5	"

3									
96 6	Configure	Monitor	Be	@ efresh	- Save	Q Search	? Help		
۵ 😫	/PN								
	9 VPN 	ite VPN	IPSec	Policies	;				Add
	🚰 Easy VP 🚰 Easy VP	N Remote N Server	Ш	Add IPS	ec Policy				×
	🚰 Dynamic] 🥶 SSL VPN	: Multipoint VPN N		Name	e: myr	nap			
Ė	VPN Cor	mponents		Cn	pto Maps ir	this IPSec P	olicy		
	P	Sec Policies (Cry namic Crypto Ma			Name		Seq No	Peers	Add
		Sec Profiles ansform Sets	Crypte						Edit
		Sec Rules(ACLS)	Nam						Delete
		E Policies e-shared Keys						,	
	E-C Easy	= Profiles VPN Server							- Jse Add Wizard
	VPN I	Keys Encryption		Dy	namic Crypt	to Map Sets ir	n this IPsec I	Policy	
			•		Dynamic	Comto Man S	et Name	Seg No	Associate
			Dynar		Dynamic	orpho map of	et raille	064140.	Associate
									Disassociate

10. Klicken Sie auf **Hinzufügen**.Klicken Sie auf die Registerkarte **Allgemein**, und behalten Sie die Standardeinstellungen

Add Crypto Ma	P				
General P	eer Information	Transform S	Bets IPSe	c Rule	
Name o	f IPSec Policy: n	nymap			
Descript	ion:				
Sequen	e Number:				
Security A 1 0 Idle Time:	ssociation Lifetim	ne: 3S 4608 3S	000	Kilobytes	
Perfect Revers	Forward Secrecy e Route Injection	grou	p1	¥	
ei.	ОК	Cancel	Help		Klicken Sie auf die

Registerkarte **Peer Information** (Peer-IP-Adresse), um die Peer-IP-Adresse 172.16.1.2



ken Sie auf die Registerkarte Transform Sets, um den gewünschten Transform Set myset

Add Crypt	o Map			
General	Peer Inform	ation (Tran	sform Sets IPS	ec Rule
Availat	le Transform :	Sets	Selected Trans in Order of Pre	form Sets ference
Nam	9	Туре	Name	
ESP-3	DES-SHA	SDM De	myset	_
		>	A	А.
		<	<	V
A0	<u></u> <u> </u>	JIT		
len.	ОК	Cano	el Help	

n Sie auf die Registerkarte IPSec Rule (IPSec-Regel), um die vorhandene Krypto-ACL 101

	General P	eer Inforr	mation	Transform	Sets IP	Sec Rule	
	IPPoor P	ulo:	101				
	IFSUCK	ule. j	101			Selection et	vistina
						Create a ne	w rule(
						None (Clea	r rule a
auszuwählen.		ОК		Cancel	Help		Kli

cken Sie auf **OK**.**Hinweis:** Dies ist die entsprechende CLI-Konfiguration:

11. Wählen Sie **Configure > VPN > Site-to-Site VPN > Edit Site-to-Site VPN > Add** aus, um crypto map *mymap* auf die Schnittstelle Ethernet0/0 anzuwenden.



12. Klicken Sie auf OK. Hinweis: Dies ist die entsprechende CLI-Konfiguration:

CLI-Konfiguration für Standort_A-Router

Standort_A-Router					
Site_A# show running-config					
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from					
console by console					
Building configuration					
Current configuration : 1545 bytes					
!					
version 12.4					
service timestamps debug datetime maea					
service timestamps log datetime msec					
: hostname Site A					
boot-start-marker					
boot-end-marker					
!					
!					
no aaa new-model					
!					
resource policy					
!					
1					
!					
ip cef					

```
crypto isakmp policy 10
hash md5
authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0
!--- Defines pre-shared secret used for IKE
authentication ! ! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
set peer 172.16.1.2
set transform-set myset
match address 101
!--- Defines crypto map. ! ! ! ! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
ip virtual-reassembly
1
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat outside
ip virtual-reassembly
half-duplex
crypto map mymap
!--- Apply crypto map on the outside interface. ! ! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip nat inside source static network 192.168.1.0 10.5.5.0
/24
!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24
!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255
!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. ! ! control-plane ! ! line con 0 line aux 0 line
vty 0 4 ! ! end Site_A#
```

CLI-Konfiguration des Standorts_B-Routers

Standort_B-Router

Site_B#**show running_config** Building configuration...

```
Current configuration : 939 bytes
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
1
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map mymap 10 ipsec-isakmp
set peer 10.1.1.2
set transform-set myset
match address 101
1
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
1
interface Ethernet1
ip address 172.16.1.2 255.255.255.0
crypto map mymap
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
1
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
1
line con 0
line aux 0
line vty 0 4
!
end
Site_B#
```

<u>Überprüfen</u>

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, 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**.

 show crypto isakmp sa: Zeigt alle aktuellen Sicherheitszuordnungen (SAs) f
ür Internet Key Exchange (IKE) auf einem Peer an.

Site_A# show c	rypto isakmp sa				
dst	src	state	conn-id :	slot	status
172.16.1.2	10.1.1.2	QM_IDLE	1	0	ACTIVE

 show crypto isakmp sa detail: Zeigt die Details aller aktuellen IKE-SAs in einem Peer an. Site_A#show cryto isakmp sa detail

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
 C-id Local
            Remote I-VRF Status Encr Hash Auth DH Lifetime
  Cap.
 1 10.1.1.2 172.16.1.2
                                           ACTIVE des md5 psk 1 23:59:42
       Connection-id:Engine-id = 1:1(software)
• show crypto ipsec sa: Zeigt die von aktuellen SAs verwendeten Einstellungen an.
 Site_A#show crypto ipsec sa
 interface: Ethernet0/0
    Crypto map tag: mymap, local addr 10.1.1.2
    protected vrf: (none)
    local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 172.16.1.2 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
 #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 3, #recv errors 0
```

```
local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x1A9CDC0A(446487562)
```

```
inbound esp sas:
spi: 0x99C7BA58(2580003416)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4478520/3336)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x1A9CDC0A(446487562)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4478520/3335)
  IV size: 8 bytes
```

```
replay detection support: Y
         Status: ACTIVE
      outbound ah sas:
      outbound pcp sas:
 Site_A#

    show ip nat translations: Zeigt Informationen zu Übersetzungssteckplätzen an.

 Site_A#show ip nat translations
 Pro Inside global Inside local
                                           Outside local
                                                              Outside global
 ----
                        _ _ _
                                           10.10.10.1
                                                              192.168.1.1
 ____
                        _ _ _
                                           10.10.10.0
                                                             192.168.1.0
                                                              ___
 --- 10.5.5.1
                       192.168.1.1
                                           ___
 --- 10.5.5.0
                       192.168.1.0
                                           _ _ _
                                                               _ _ _
• show ip nat statistics: Zeigt statische Informationen über die Übersetzung an.
 Site_A#show ip nat statistics
 Total active translations: 4 (2 static, 2 dynamic; 0 extended)
 Outside interfaces:
   Ethernet0/0
 Inside interfaces:
   Loopback0
 Hits: 42 Misses: 2
```

Gehen Sie wie folgt vor, um die Verbindung zu überprüfen:Wählen Sie in SDM Extras > Ping aus, um den IPsec-VPN-Tunnel mit der Quell-IP als 192.168.1.1 und der Ziel-IP als 10.10.10.1 einzurichten.
 Ping

 * Source: 192.168.1.1
 Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seco

CEF Translated packets: 13, CEF Punted packets: 0

Expired translations: 7

Dynamic mappings: Queued Packets: 0

Site_A#

* Source:	192.168.1.1	Sendin	g 5, 100-byte ICMF	^o Echos to 10.10.10	.1, timeout is 2 secor
Destination:	10.10.10.1	Succes	ss rate is 40 perce	nt (2/5), round-trip n	nin/avg/max = 36/38/4
	Ping				
		•			
(*) Optional Fi	eld		Clear Output	Close	Help

Klicken Sie auf **Test Tunnel**, um zu überprüfen, ob der IPsec VPN-Tunnel wie in diesem Bild gezeigt eingerichtet ist.

Create Site to Site VPN	Edit Site to Site VPN		
			Add
Status	Interface	Description	IPSec Policy
🗢 Down	Ethernet0/0		mymap 1
			•
	C	lear Connection	nel.). Generate Mirror
Klicken Sie auf Start.			_
VPN Troubleshooting			
Tunnel Details			
Interface: Etherne	et0/0	Peer: 172.16.1.2	
1			
		🗐 Su	immary 📓 Details
Activity			Status
Checking the tunnel	status		🙄 Up
Inform Failure Rea	Nation VPN Troubles The VPN Tunn	nooting is successful ! el is up.	(s)
Start	Save Report.	Close	Help

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:

Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 192.168.1.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.1.1 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms Site A# *Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- <u>Konfigurationsbeispiel für IPSec zwischen ASA/PIX und dem Cisco VPN 3000-Concentrator</u> mit sich überschneidenden privaten Netzwerken

<u>Technischer Support und Dokumentation - Cisco Systems</u>