# IPsec tussen twee IOS-routers met configuratievoorbeeld voor Private Networks

# Inhoud

InleidingVoorwaardenVereistenGebruikte componentenConventiesConfigurerenNetwerkdiagramConfiguratiesVerifiërenProblemen oplossenGerelateerde informatie

# Inleiding

Dit document beschrijft hoe u de Cisco IOS router in een site-to-site IPsec VPN met overlappende privé netwerkadressen achter VPN-gateways kunt configureren.

# **Voorwaarden**

## **Vereisten**

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS 3640 routers die softwareversie 12.4 uitvoeren.

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

## **Conventies**

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

# **Configureren**

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking:** Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

## **Netwerkdiagram**

Het netwerk in dit document is als volgt opgebouwd:



**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Zowel Private\_LAN1 als Private\_LAN2 hebben een IP-subtype van 192.168.1.0/24. Dit simuleert de overlappende adresruimte achter elke kant van de IPsec-tunnel.

In dit voorbeeld voert de Site\_A router een tweerichtingsvertaling uit zodat de twee particuliere LAN's kunnen communiceren via de IPsec-tunnel. De vertaling betekent dat Private\_LAN1 "ziet" Private\_LAN2 als 10.10.10.0/24 door de IPsec-tunnel en Private\_LAN2 "ziet" Private\_LAN1 als 10.5.5.0/24 door de IPSec-tunnel.

## **Configuraties**

Dit document gebruikt deze configuraties:

- <u>Configuratie van Site A router</u>
- <u>Configuratie van Site\_A router CLI</u>
- <u>Configuratie van Site\_B-router</u>

#### Configuratie van Site\_A router

**N.B.:** Dit document gaat ervan uit dat de router is ingesteld met basisinstellingen zoals de interfaceconfiguratie, enz. Raadpleeg de <u>basisrouterconfiguratie met</u> behulp<u>van</u> een<u>dm</u> voor meer informatie.

#### NAT-configuratie

Voltooi deze stappen om NAT te gebruiken om PDN op de Site\_A router te configureren:

1. Kies **Configureren > NAT > NAT-configuratie bewerken** en klik op **NAT-interfaces** toewijzen om vertrouwde en onvertrouwde interfaces te definiëren zoals

<b>;</b>	in the second	Configure	<b></b>	Monitor	Refre	▶ ish	<b></b> Save	S	
1	NAT	•							
	Create	NAT Confi	iguration	n Edit N	AT Confi	guration	1		
	Designate NAT Interfaces								
N	AT Int	erface Sel	tting					×	
	Select the list of interfaces that you want to designate as inside / outside.								
	ir	nterface	i	inside(trusted)			outside(untruste		
	Etheri	net0/0							
	FastE	thernet1/0	)						
	Loopt	oackO		V					
	•								
		0	К	Cance	!I	Help			

weergegeven

- 2. Klik op OK.
- 3. Klik op Add om de NAT-vertaling van binnen naar buiten te configureren zoals wordt

Add Address Translation Rule	
<ul> <li>Static</li> <li>O Dynamic</li> </ul>	
Direction: From inside to o	uts de 💌
Translate from interface _	
Inside Interface(s):	Loopback0
IP address:	192.168.1.0
Notwork Mack(ontional):	255 255 255 0 or 24
Network Mask(optional).	233.233.233.0
Tranclata ta interface	
Outside Interface(s):	Ethernet0/0
Type:	IP address 💌
Interfacer	Ethernet0/0
intenace.	
IP address:	10.5.5.0
Redirect Port	
Original Port:	Translated Port:
OK I	Cancel I Help I

4. Klik op

OK.			
- Network Address Translation Rules			
Inside Interface(s): Loopback0 Outside Interface(s): Ethernet0/0			
Original address	Translated address	Rule Type	Add
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static	

5. Klik nogmaals op **Add** om de NAT-vertaling van buiten naar binnen te configureren zoals wordt

		Add Addr	ess Transla	ation Rule			
		• St	atic	O Dynamic			
Direction: From outside to incide							
			nection. Jr				
			-Translate	from interface			
				f = ( - ) -	Ethere a 10/0		
		0	utside intei	nace(s):	Ethernetu/U		
		IF	? address:		10.10.10.0		
		- N	letwork Mas	sk(optional):	255.255.255.0	or 24	
					,	,	
			Translate	to interface —			
			Inside Inte	rface(s):	LoopbackO		
			IP address	2.	19216810		
			ii addies.		102.100.1.0		
			E Rec	direct Port 👘			
			Отор	OUDP			
			Original F	Port:	Translated Port:		
	weergegeven			ок	Cancel Help		
6.	Klik op						
	OK.						
	– Network Addre	ss Transla	tion Rules —				
	Inside Interface(	(s): Lo	opback0				
	Outside Interfac	e(s): Eth	ernet0/0				
		-(v). Eu	ionnotoro				
	Original ad	ddress	1.055	Translate	d address	Rule Type	
	192.168.1.	0-192.168. 0-192.168	1.255	10.5.5.0-1	0.5.5.255	Static	

**Opmerking:** Hier is de equivalente CLI-configuratie:

## VPN-configuratie

Voltooi deze stappen om VPN te gebruiken om PDM op de Site\_A router te configureren:

1. Kies Configureren > VPN > VPN-componenten >IKE > IKE-beleid > Toevoegen om het IKEbeleid te definiëren zoals in deze

	Configu	re IKE Policy	·				
	Priority: 10			Auther	iticatio BHARE	n: E	•
	Encryption DES	1:	•	D-H Gi group	roup: 1		•
	Hash: MD5		•	Lifetim 24	e: 0	0 Hł	H:MM:SS
afbeelding.		ОК		Cancel		Help	

ОК

	IKE	Policies				Add	Edit Del
ſ		Priority	Encryption	Hash	D-H Group	Authentication	Туре
		10	DES	MD5	aroup1	PRE SHARE	User Defined

**Opmerking:** Hier is de equivalente CLI-configuratie:

3. Kies Configureren > VPN > VPN-componenten >IKE > Voorgedeelde toetsen > Add om de voorgedeelde sleutelwaarde in te stellen met peer IP-

	Key:	*****				
	Re-enter Key:	*******				
	Host/Netwo	rk				
	Type:	IP Address	•			
	IP Address:	172.16.1.2				
	Subnet Mask: (Optional)	255.255.255.0	24			
	User Authentication (XAuth)					
adres.	ок	Cancel	Help			
Klikor						

4. Klik op OK.

Pre	shared Keys		Add
	Peer IP/Name	Subnet Mask	pre-shared key
	170464.0	255 255 255 0	*****

**Opmerking:** Hier is de equivalente CLI-configuratie:

5. Kies **Configureren > VPN-componenten > IPSec > Transformatiesets > Toevoegen** om een transformatieset *myset* te maken zoals in deze afbeelding wordt

N	lame:	myset	_			
Г	~	Data integrity	with	encryption (E	ESP)	
	Integ	rity Algorithm	:	ESP_MD5_	HMA	.C 🔻
	Encr	yption Algoriti	hm:	ESP_DES		-
						Show Advan
etoond.		ОК		Cancel		Help
(lik op						

Transform Set			Add
Name	ESP Encryption	ESP Integrity	AH Integrity
myset	ESP_DES	ESP_MD5_HMAC	of

pmerking: Hier is de equivalente CLI-configuratie:

7. Kies Configureren > VPN-componenten > IPSec > IPSec-regels (ACL's) > Add om een crypto toegangscontrolelijst (ACL's) *101* te

٩de	d a Rule				
	Name/Nun	nber:		Туре:	
	101			Extended R	ule
	Description	ו:			
	Rule Entry				
	permit ip 1	0.5.5.0 0.255.	255.255 192.1	68.1.0 0.255.	Add
					Clone.
					Edit
					Delete
					Move C
					Move Do
	Interfac	e Associatior	ì		
	None.			As	sociate
n		ОК	Cancel	Help	1
p					-



**Opmerking:** Hier is de equivalente CLI-configuratie:

9. Kies **Configureren > VPN-componenten > IPSec > IPSec-beleid > Add** in om cryto map *mymap* te maken zoals in deze

afbeelding.

Configure Monitor	Refresh Save Sea	rch Help	
🚰 VPN			
E- VPN	Sec Policies		Add
Easy VPN Remote Easy VPN Server	Add IPSec Policy		×
B-BSL VPN B-BVPN Components	Name: mymap	PSec Policy	
- PSec Policies (Cry - PSec Policies (Cry - PSec Policies (Cry - PSec Policies (Cry	Name	Seq No Peers	Add
Transform Sets	ryptc		Edit
⊡-∰ IKE ∰ IKE Policies ∰ Pre-shared Kevs	Nam		Delete
Easy VPN Server	<u> </u>	F	▶ Use Add Wizard
VPN Keys Encryption	Dynamic Crypto Map	Sets in this IPsec Policy	
	Dynamic Crypto	Map Set Name Seq No.	Associate
			Disassociate

10. Klik op Toevoegen.Klik op het tabblad Algemeen en bewaar de

	Add Crypto Map					
	General Peer Information Transform Sets IPSec Rule					
	Name of IPSec Policy: mymap					
	Description:					
	Sequence Number: 1					
	Security Association Lifetime: 1 0 0 HH:MM:SS 4608000 Kilobytes Idle Time: HH:MM:SS					
	Perfect Forward Secrecy group1					
	Reverse Route Injection					
standaardinstellingen.	OK Cancel Help					

lik op het tabblad Peer Informatie om het IP-adres van een peer toe te voegen



het tabblad **Omzetten** om de gewenste *myset* voor transformatie te

۸dd Crypto M	ар					
General	<sup>o</sup> eer Informa	tion <b>(Tr</b>	ansfo	orm Sets	IPSec Rule	
				Selected 1	Fransform Se	ets
Available 1	Fransform S	ets		in Order o	f Preference	
Name		Туре		Name		7
myset		User De		myset		
ESP-3DE	S-SHA	SDM De				
			>>			Λ.
			<<			V
Add		• I		L		
Auu		L				
	OK		ncel	Г	eln	
en.					orb	

het tabblad IPSec-regel om de bestaande crypto ACL 101 te

	General P	eer Informatio	n Transform	Sets IPSec	Rule
	IPSec F	tule: 101			$\nabla$
				Se	lect an existing
				Cr	eate a new rule(
				No	ne (Clear rule a
selecteren.		OK	Cancel	Help	Klik

op **OK**.**Opmerking:** Hier is de equivalente CLI-configuratie:

11. Kies **Configureer > VPN > Site-to-Site VPN > Site-to-Site VPN bewerken > Add** om crypto kaart van de interface met Ethernet0/0 toe te passen.



12. Klik op OK.Opmerking: Hier is de equivalente CLI-configuratie:

#### Configuratie van Site\_A router CLI

Site_A router
Site_A# <b>show running-config</b>
*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 msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
1
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#
```

#### Configuratie van Site\_B router CLI

#### Site\_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
1
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
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
!
interface Ethernet1
ip address 172.16.1.2 255.255.255.0
crypto map mymap
1
!--- 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#
```

# **Verifiëren**

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.  toon crypto isakmp sa-Toont alle huidige IKE (Internet Key Exchange) veiligheidsassociaties (SAs) bij een peer.

Site_A# <b>show c</b>	rypto isakmp sa				
dst	src	state	conn-id s	lot st	atus
172.16.1.2	10.1.1.2	QM_IDLE	1	0 AC'	TIVE

• toon crypto isakmp als detail-Toont de details van alle huidige IKE SAs bij een peer. 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)
```

• Laat crypto ipsec sa-displays de instellingen die worden gebruikt door de huidige SAs. 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#

    informatie over de ip nat vertalingen-displays met de vertaalsleuf.

  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
--- 10.5.5.0
                              192.168.1.1
192.168.1.0
                                                                                 ___
                                                        ____
                                                         ___
                                                                                   _ _ _
• ip nat statistics-displays statistische informatie over de vertaling tonen.
  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
  CEF Translated packets: 13, CEF Punted packets: 0
  Expired translations: 7
```

```
Dynamic mappings:
Queued Packets: 0
Site_A#
```

 Voltooi deze stappen om de verbinding te controleren: In het programma dm, kies Gereedschappen > Ping om de IPsec VPN-tunnel met bron IP als 192.168.1.1 en bestemming IP als 10.10.10 op te

zetten.				
Ping				
* Source:	192.168.1.1	Sending 5, 100-byte ICM	IP Echos to 10.10.10.1	, timeout is 2 secor
Destination:	10.10.10.1	Success rate is 40 perci	ent (2/5), round-trip mir	1/avg/max = 36/38/4
	Ping			
		•		<b>&gt;</b>
(*) Optional F	ield	Clear Output	Close	Help

Klik op **Test Tunnel** om te controleren of de IPsec VPN-tunnel is ingesteld zoals in deze afbeelding.

Create Site to Site VPN	Edit Site to Site VI	PN		
				Add   Delete
Status	Interface	Descriptio	n	IPSec Policy
오 Down	Ethernet0/0			mymap 1
				•
		Clear Connection	(Test Tunnel)	Generate Mirror
Klik op				J
Start.				
VPN Troubleshooting				
Tunnel Details —				
Interface: Etherne	et0/0	Peer:	172.16.1.2	
			📃 Summar	y 📓 Details
Activity				Status
Checking the tunnel	status			😜 Up
			M	
Inform	nation			
	•			
	VPN Troub	leshooting is succe	ssful !	
	The VPN T	unnel is up.		
Failure Rea		·	(s)	
	r	OK I	<u> </u>	
	<u>L.</u>	UK		
Start	Save Rep	oort	lose	Help

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

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

## Gerelateerde informatie

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- IPsec tussen ASA/PIX en Cisco VPN 3000 Concentrator met Overlappend Configuratievoorbeeld voor Private Networks

• Technische ondersteuning en documentatie – Cisco Systems