Konfigurationsbeispiel für IPSec zwischen PIX und Cisco VPN Client mithilfe von Smartcard-Zertifikaten

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Registrieren und Konfigurieren des PIX Konfigurationen Registrieren von Cisco VPN Client-Zertifikaten Konfigurieren Sie den Cisco VPN-Client, um das Zertifikat für die Verbindung zum PIX zu verwenden. eToken Smartcard-Treiber installieren Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument zeigt, wie ein IPSec-VPN-Tunnel zwischen einer PIX-Firewall und einem Cisco VPN-Client 4.0.x konfiguriert wird. Im Konfigurationsbeispiel in diesem Dokument wird auch das Anmeldeverfahren der Zertifizierungsstelle (CA) für den Cisco IOS® Router und den Cisco VPN Client sowie die Verwendung einer Smartcard als Zertifikatsspeicher hervorgehoben.

Unter Konfigurieren von IPSec zwischen Cisco IOS-Routern und dem Cisco VPN-Client mithilfe von Vertrauenzertifikaten finden Sie weitere Informationen zur Konfiguration von IPSec zwischen Cisco IOS-Routern und dem Cisco VPN-Client mithilfe von Vertrauenszertifikaten.

Unter Konfigurieren von Zertifizierungsstellen für mehrere Identitäten auf Cisco IOS-Routern finden Sie weitere Informationen zum Konfigurieren von Zertifizierungsstellen für mehrere Identitäten auf Cisco IOS-Routern.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco PIX Firewall mit Softwareversion 6.3(3)
- Cisco VPN Client 4.0.3 auf einem PC mit Windows XP
- Ein CA-Server für Microsoft Windows 2000 wird in diesem Dokument als CA-Server verwendet.
- Zertifikate auf dem Cisco VPN Client werden mit der <u>Aladdin</u> e-Token Smartcard gespeichert.

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>.

Registrieren und Konfigurieren des PIX

In diesem Abschnitt werden die Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen angezeigt.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das <u>Command Lookup Tool</u> (<u>nur registrierte</u> Kunden).

Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- Zertifikatsregistrierung für PIX-Firewall
- PIX-Firewall-Konfiguration



ISa
<i>! Generate RSA (encryption and authentication) keys.</i>
ca gen rsa key
! Select the modulus size (512 or 1024). ! Confirm
the keys generated. show ca mypub rsa
10.1.1.2. (next the CA identity. ca ident kobe
10.1.1.2:/certsrv/mscep/mscep.dll
ca coni kobe ra i zu criopt
ca auth Kobe
Confirm the certificate and validity show ca cert
PIX-Firewall-Konfiguration
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameli ethernet5 inti5 security10
enable password 8ky2ijiyt/kkx024 encrypted
passwa zkrynoniai.zkiou encrypted
domain nome sigge som
fixup protocol dng maximum-length 512
fixup protocol ftp 21
fixup protocol $h323$ $h225$ 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit tcp any host 209.165.201.21 eq
www
access-list 120 permit ip 10.1.1.0 255.255.255.0
10.0.0.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 209.165.201.20 255.255.255.224
ip address inside 10.1.1.10 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5

ļ

```
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 10.0.0.10-10.0.0.100
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask
255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpncert address-pool vpnpool
vpngroup vpncert idle-time 1800
vpngroup vpncert password *******
ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca configure kobe ra 1 20 crloptional
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum: 2ae252ac69e5218d13d35acdf1f30e55
: end
[OK]
sv2-11(config)#
```

Registrieren von Cisco VPN Client-Zertifikaten

Denken Sie daran, alle notwendigen Treiber und Dienstprogramme zu installieren, die mit dem

Smartcard-Gerät auf dem PC für die Verwendung mit dem Cisco VPN-Client ausgeliefert werden.

In diesen Schritten werden die Verfahren zur Registrierung des Cisco VPN Client für MS-Zertifikate veranschaulicht. Das Zertifikat wird im <u>Aladdin</u> e-Token Smartcard Store gespeichert.

- 1. Starten Sie einen Browser, und wechseln Sie zur Zertifikatserverseite (in diesem Beispiel http://CAServeraddress/certsrv/).
- 2. Wählen Sie Zertifikat anfordern aus, und klicken Sie auf Weiter

Address 🕘 http://209.165.201.21/certsrv/	So Lin
Microsoft Certificate Services kobe	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, other secure program. Once you acquire a certificate, you will be at identify yourself to other people over the web, sign your e-mail mess your e-mail messages, and more depending upon the type of certifi	e-mail client, or ble to securely sages, encrypt cate you request.
Select a task:	
Retrieve the CA certificate or certificate revocation list	
 Request a certificate 	
Check on a pending certificate	
	Next >

3. Wählen Sie im Fenster Anfragetyp auswählen die Option **Erweiterte Anforderung aus**, und klicken Sie auf

Weiter.

Microsoft Certificate Services kobe	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request:	
Web Browser Certificate E-Mail Protection Certificate	
 Advanced request 	
	Next >

4. Wählen Sie eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus, und klicken Sie auf Weiter

Microsoft Certificate Services kobe Ho	<u>me</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of following methods. Note that the policy of the certification authority (CA) will determ the certificates that you can obtain.	the nine
 Submit a certificate request to this CA using a form. 	
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.	
 Request a certificate for a smart card on behalf of another user using the Smar Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user. 	rt

5. Füllen Sie alle Felder im Formular für erweiterte Zertifikatsanforderung aus. Stellen Sie sicher, dass die Abteilung oder Organisationseinheit (OU) dem im PIX-vpngroup-Namen konfigurierten Cisco VPN Client-Gruppennamen entspricht. Wählen Sie den für Ihre Einrichtung geeigneten Zertifikatsdienstanbieter (Certificate Service Provider, CSP) aus.

Next >

		and a second and a second s
Advanced Ce	rtificate Request	
dentifying Infor	mation:	
Name:	ericetoken	
E-Mail:		
Company:	cisco	
Department:	vpncert	
City:	ctd	
State:	nsw	
Country/Region:	AU	
ntended Purpos	se:	
	Client Authentication Certificate 💌	
(ey Options:		
CSP:	eToken Base Cryptographic Provider	
Key Usage:	⊙Exchange ⊙Signature ⊚Both	
Key Size:	512 Min: 384 Max1024 (common key sizes: <u>512</u> <u>1024</u>)	
	Create new key set	
	Set the container name	
	◯ Use existing key set	
	Enable strong private key protection	
	🔲 Mark keys as exportable	
	Use local machine store	
dditional Optio	ns:	
Hash Algorithm:	SHA-1	
	Only used to sign request.	
	Save request to a PKCS #10 file	
Attributes:	< > > > > > > > > > > > > > > > > > > >	
		Submit >

6. Wählen Sie **Yes (Ja)** aus, um die Installation fortzusetzen, wenn Sie die Warnung zur Prüfung potenzieller Skripte erhalten.

Potenti	al Scripting Violation 🔣
⚠	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

7. Die Zertifikatregistrierung ruft den eToken-Speicher auf. Geben Sie das Kennwort ein, und

	eToken Base Cryptographic Provider 🛛 🛛 🔀
	eToken
	Input eToken password
	eToken: eToken [AKS ifdh 0]
	Password: ******
	Login to your eToken to enable using/creating/removing your private key.
klicken Sie auf OK .	Less << OK Cancel

8. Klicken Sie auf **Zertifikat**

Microsoft Certificate Services kobe	<u>Home</u>
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	

9. Wählen Sie **Yes (Ja)** aus, um die Installation fortzusetzen, wenn Sie die Warnung zur Prüfung potenzieller Skripte erhalten.

Potential Scripting Violation Image: Construct of the state is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No. Yes No

10. Wählen Sie **Yes (Ja)** aus, um das Stammzertifikat dem Root Store hinzuzufügen

Root Cer	rtificate Store 🔀
	Do you want to ADD the following certificate to the Root Store? Subject : kobe, vpn, apt-vpn, ctd, nsw, AU Issuer : Self Issued Time Validity : Monday, 25 August 2003 through Thursday, 25 August 2005 Serial Number : 43C2EE28 43CE56A6 4457F2D2 23EDFED2 Thumbprint (sha1) : 3D47C8F6 2703B88D C2BD4F68 7B5300A0 3A927B4E Thumbprint (md5) : A1E23E81 08538FA4 6BB4F187 49EC774F Yes No

11. Das Fenster Zertifikat installiert wird angezeigt und bestätigt die erfolgreiche Installation.

Microsoft Certificate Services kobe	<u>Home</u>
Certificate Installed	
Your new certificate has been successfully installed.	

12. Verwenden Sie den eToken-Anwendungs-Viewer, um das auf der Smartcard gespeicherte Zertifikat

anzuzeigen.

Image: Settings Certificates & keys	🚍 eToken Propertie	\$		
Advanced Refresh Advanced Refresh Image: Control of the stress in the stress	eToken			
eToken [PRO] Details Settings Certificates & keys Image: Settings Details Setial number 11 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beh2b14a=e935.4476.bfb3.8e22495.3/d19	×	Advanced 🕗 Ref	iresh 김 Help	
Local Machine Details Settings Certificates & keys Image: Control Contrel Control Control Contect Control Control Contrecontect Control	ето	ken [PRO]		
Image: circetoken Delete Image: circetoken Image: circetoken Image: circetoken Circetoken	Local Machine	Details Settings Cert	ificates & keys	
Exchange key <beb2b14a-e935-4476-bfb3-8e22d95 00="" 11="" 14="" 2003="" 2004="" 23="" 2:24:58="" 2:34:58="" 41="" 5d="" 81="" algorithm="" am="" apt-vpn,="" au,="" beb2b14a-e935-4476-bfb3-8e22d95a3d19="" cisco,="" container="" ctd,="" ericetoken="" from="" issuer="" keu="" kobe="" more<="" nsw,="" number="" october="" refresh="" rsa_sha1rsa="" serial="" signature="" subject="" th="" thursday,="" to="" tuesday,="" v3="" valid="" version="" vpn,="" vpncert,=""><th></th><th>ericetoken</th><th></th><th>Delete</th></beb2b14a-e935-4476-bfb3-8e22d95>		ericetoken		Delete
eToken [AKS if Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a=e935-4476-bfb3.8e22d95a3d19 Refresh More		🗯 Exchange ke	y <beb2b14a-e935-4476-bfb3-8e22d95< td=""><td></td></beb2b14a-e935-4476-bfb3-8e22d95<>	
Version V3 Serial number 11 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a=e935-4476-bfb3-8e22d95a3d19 Refresh More_	eToken [AKS if			
Version V3 Serial number 11 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a=e935-4476-bfb3-8e22d95a3d19 Refresh More				
Serial number 11 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a=e935-4476-bfb3-8e22d95a3d19 Refresh More		Version	V3	~
Signature algorithm HSA_SHATHSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncet, ericetoken Key container heb/2b14a-e935-4476-bfb3-8e22d95a3d19		Serial number	11 00 00 00 00 00 5d 41 81 23	
Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a-e935-4476-bfb3-8e22d95a3d19		Signature algorithm	HSA_SHATHSA	· 111
Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container heb/2h14a-e935-4476-bfb3-8e22d95a3d19		Issuer Valid from	AU, nsw, ctd, apt-vpn, vpn, kobe	
Subject AU, nsw, ctd, cisco, vpncert, ericetoken		Valid from	Thursday, 14 October 2003 2:24:56 AM	
Keu container beb2b14a-e935-4476-bfb3-8e22d95a3d19		Subject	All new old cisco upnoat aristokan	
Refresh More		Keu container	heh2h14a-e935-4476-bfh3-8e22d95a3d19	~
More		and the second second		
More				Refresh
				More

Konfigurieren Sie den Cisco VPN-Client, um das Zertifikat für die Verbindung zum PIX zu verwenden.

In diesen Schritten werden die Verfahren veranschaulicht, mit denen der Cisco VPN Client für die Verwendung des Zertifikats für PIX-Verbindungen konfiguriert wird.

1. Starten Sie den Cisco VPN Client. Klicken Sie unter Verbindungseinträge auf **Neu**, um eine neue Verbindung zu erstellen.

Connection Entries Status	Certificates Log	Options	Help	
<u>Connect to to_pix</u>	Ctrl+O	-	×4	CISCO SYSTEMS
Disconnect	Ctrl+D	22	Delete	فالف مألف
C <u>r</u> eate Shortcut <u>M</u> odify				
D <u>e</u> lete D <u>u</u> plicate			Host	Tans
Set as Default Connecti	on Entry			
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			
4		_		•

2. Füllen Sie die Verbindungsdetails aus, geben Sie die Zertifikatauthentifizierung an, und wählen Sie das Zertifikat aus, das Sie bei der Registrierung erhalten haben. Klicken Sie auf

VPN Client Create New VPN Co	onnection Entry 🛛 📔
Connection Entry: to_pix	- Calle
Description: connection to pix	
Host: 209,165.201.20	
Authentication Transport Backup Ser	rvers Dial-Up
C Group Authentication	
Name:	
Password:	
C <u>o</u> nfirm Password:	
G. Catiliasta Authentiastian	
Name: Rejected on (Missess 9)	
Send CA Certificate Chain	
Erase <u>U</u> ser Password	<u>S</u> ave Cancel

Speichern.

3. Um die Verbindung des Cisco VPN-Clients mit dem PIX zu starten, wählen Sie den

gewünschten Verbindungseintrag aus, und klicken Sie auf Verbinden.

👌 VPN Client - Versio	n 4.0.3 (Rel)				
Connection Entries Status	Certificates Log	Options	Help		
Connect to to_pix	Ctrl+O	-	×4	C	ISCO SYSTEMS
Disconnect	: Ctrl+D		Delete		ale ale
C <u>r</u> eate Shortcut Modify					
 Delete Duplicate		-	Host 209.165.201	.20	Trans IPSe
Set as Default Connect	tion Entry	_			
<u>N</u> ew <u>I</u> mport					
Exit VPN Client	Ctrl+Q	- 			<u>*</u>
Not connected.					

eToken Smartcard-Treiber installieren

Diese Schritte veranschaulichen die Installation der <u>Aladdin</u> eToken Smartcard-Treiber.

1. Öffnen Sie den eToken Run Time Environment 3.51 Setup-Assistenten.



2. Akzeptieren Sie die Lizenzvertragsbedingungen, und klicken Sie auf **Weiter**.

End-User License Agreement	Tatan	
Please read the following license agreement carefully	Your Key to eSecurity	RTI
ALADDIN KNOWLEDGE SYSTE	EMS LTD.	^
ETOKEN ENTERPRISE END USER LI	CENSE AGREEMENT	
IMPORTANT INFORMATION - PLEASE CAREFULLY BEFORE OPENING THE P. THE CONTENTS THEREOF AND/OR BEF INSTALLING THE SOFTWARE PROGRAM USE OF THE ETOKEN ENETERPRISE PF limitation, libraries, utilities, diskettes, CD_ROM Guide) (hereinafter "Product") SUPPLIED BY	READ THIS AGREEMEN ACKAGE AND/OR USIN ORE DOWNLOADING OI I. ALL ORDERS FOR ANI RODUCTS (including withou , eToken® keys and the Use ALADDIN KNOWLADG	T G D ut E
 I accept the license agre I do not accept the licens 	ement se agreement	
Reset < Ba	ck Next> Cance	n Ó

3. Klicken Sie auf Installieren.

51 Setup 📃 🗖 🔀
T -
Your Key to eSecurity RTE
Please click Next to begin installation.
< Back Next > Cancel

4. Die eToken Smartcard-Treiber sind jetzt installiert. Klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.



<u>Überprüfen</u>

Dieser Abschnitt enthält Informationen, die Sie verwenden können, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

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

```
SV2-11(config)#show crypto isa sa
Total : 1
Embryonic : 0
dst src state pending created
209.165.201.20 209.165.201.19 QM_IDLE 0 1
```

• show crypto ipsec sa: Zeigt die von aktuellen Sicherheitszuordnungen verwendeten

```
Einstellungen an.
SV1-11(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, local addr. 209.165.201.20
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0)
current_peer: 209.165.201.19:500
dynamic allocated peer ip: 10.0.0.10
PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
```

```
#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.: 209.165.201.20, remote crypto endpt.: 209.165.201.19
    path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: c9a9220e
inbound esp sas:
spi: 0xa9857984(2844096900)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607996/28746)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xc9a9220e(3383304718)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28748)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Fehlerbehebung

Weitere Informationen zur <u>Fehlerbehebung bei PIX zur Weiterleitung des Datenverkehrs an einen</u> etablierten IPSec-Tunnel finden Sie unter Problembehandlung für diesen <u>Datenverkehr</u>.

Zugehörige Informationen

- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Anforderungen für Kommentare (RFCs)
- <u>Support-Seite für IPSec (IP Security Protocol)</u>
- Support-Seite für Cisco VPN-Clients
- <u>Support-Seite für Firewalls der Serie PIX 500</u>
- <u>Technischer Support Cisco Systems</u>