IPsec tussen PIX en Cisco VPN-client met behulp van smartcard-certificaten

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies PIX invoeren en configureren Configuraties Cisco VPN-clientcertificaten invoeren Configureer de Cisco VPN-client om het certificaat voor verbinding met de PIX te gebruiken Installeer Token Smart-stuurprogramma's Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document toont aan hoe u een IPSec VPN-tunnel tussen een PIX-firewall en een Cisco VPNclient 4.0.x kunt configureren. Het configuratievoorbeeld in dit document benadrukt ook de certificeringsinstantie (CA) inschrijvingsprocedure voor zowel de Cisco IOS® router en de Cisco VPN client, evenals het gebruik van een Smartcard als certificatenopslag.

Raadpleeg <u>IPSec</u> configureren<u>tussen Cisco IOS-routers en Cisco VPN-client die</u> <u>vertrouwenscertificaten gebruikt</u> om meer te weten te komen over het configureren van IPSec tussen Cisco IOS-routers en Cisco VPN-client die vertrouwenscertificaten gebruikt.

Raadpleeg <u>de</u> optie <u>Meervoudige-Identity certificaatautoriteiten op Cisco IOS-routers configureren</u> om meer te weten te komen over het configureren van Meervoudige-Identity certificaatautoriteiten op Cisco IOS-routers.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco PIX Firewall met softwareversie 6.3(3)
- Cisco VPN-client 4.0.3 op een pc met Windows XP
- Een Microsoft Windows 2000 CA-server wordt in dit document gebruikt als CA-server.
- Certificaten op de Cisco VPN-client worden opgeslagen met <u>Aladdin</u> e-Token Smartcard.

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 <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

PIX invoeren en configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

N.B.: Gebruik het <u>Opdrachtupgereedschap</u> (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Configuraties

Dit document gebruikt deze configuraties.

- certificaatinschrijving op PIX-firewall
- Configuratie PIX-firewall

certificaatinschrijving op PIX-firewall			
<pre>! Define a hostname and domain name for the router. ! The fully qualified domain name (FQDN) is used ! as the identity of the router during certificate enrollment. pix(config)#hostname sv2-11 sv2-11(config)#domain-name cisco.com ! Confirm that you have the correct time set on the PIX. show clock clock set</pre>			
This command clears the PIX RSA Reys. Ca zeroize			
<pre>! Generate RSA (encryption and authentication) keys. ca gen rsa key</pre>			
<pre>! Select the modulus size (512 or 1024). ! Confirm the keys generated. show ca mypub rsa</pre>			

!--- Define the CA identity. ca ident kobe 10.1.1.2:/certsrv/mscep/mscep.dll ca conf kobe ra 1 20 crlopt ca auth kobe ca enroll kobe [ipaddress] !--- Confirm the certificate and validity. show ca cert Configuratie PIX-firewall 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 nameif ethernet5 intf5 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname sv2-11 domain-name cisco.com fixup protocol dns 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 inside 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 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)#
```

Cisco VPN-clientcertificaten invoeren

Vergeet niet alle benodigde stuurprogramma's en hulpprogramma's te installeren die met het Smartcard-apparaat op de pc worden gebruikt voor gebruik met de Cisco VPN-client.

Deze stappen tonen de procedures aan die worden gebruikt om de Cisco VPN-client voor MScertificaten in te schrijven. Het certificaat is opgeslagen in de e-Token Smartcard winkel <u>Aladdin</u>.

- 1. Start een browser en ga naar de pagina van de certificaatserver (http://CAServeraddress/certsrv/, in dit voorbeeld).
- 2. Selecteer **Een certificaat aanvragen** en klik op **Volgende**

Merconft Contificato Services	Ham
Wicroson Certificate Services Kobe	nom
Welcome	
You use this web site to request a certificate for you other secure program. Once you acquire a certificat identify yourself to other people over the web, sign y your e-mail messages, and more depending upon the secure of the	r web browser, e-mail client, or te, you will be able to securely /our e-mail messages, encrypt he type of certificate you request
Select a task:	
Retrieve the CA certificate or certificate revoc	ation list
Request a certificate	

3. Selecteer in het venster Type aanvraag kiezen de optie **Geavanceerd** en klik op **Volgende**.

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. Selecteer een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik op

Volgende.

Microsoft Certificate Services kobe	<u>Home</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a com following methods. Note that the policy of the certification authori the certificates that you can obtain.	puter using one of the ty (CA) will determine
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded PKCS renewal request using a base64 encoded PKCS #7 file. 	S #10 file or a
Request a certificate for a smart card on behalf of another us Card Enrollment Station. You must have an enrollment agent certificate to submit a request for a	ser using the Smart another user.
	Next >

5. Vul alle items in op het formulier Geavanceerd certificaataanvraag.Zorg ervoor dat het departement of de organisatorische eenheid (OU) overeenkomt met de naam van de Cisco VPN-clientgroep, zoals ingesteld in de naam PIX-groep. Selecteer de juiste CSPserviceprovider voor uw instellingen.

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 >

 Selecteer Ja om door te gaan met de installatie wanneer u de waarschuwing voor de potentiele Schrift Validering krijgt.

Potenti	al Scripting Violation			
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to require certificate for you. Do you want to request a certificate now?				
	Yes No			
7. Bij de c	ertificaatinschrijving wordt gebruik gemaakt van de Token-winkel. Voer het			
	eToken Base Cryptographic Provider			
	eToken			

Input eToken password

eToken:

Password:

your private key.

Less <<

wachtwoord in en klik op OK.

8. Klik op Installeer dit

certificaat.

eToken [AKS ifdh 0]

Login to your eToken to enable using/creating/removing

0K

Cancel

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

 Selecteer Ja om door te gaan met de installatie wanneer u de waarschuwing voor de potentiele Schrift Validering krijgt.

Potential Scripting Violation



Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

No.	No
res	NU

10. Selecteer **Ja** om het basiscertificaat toe te voegen aan de Opslagwinkel.

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. Het venster Geïnstalleerd certificaat verschijnt en bevestigt de succesvolle installatie.

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

 Gebruik het venster Token Application Viewer om het certificaat te bekijken dat is opgeslagen op de kaart.

📑 eToken Prope	rties			
eToken				
	🔊 Advanced 🕗 Refr	esh 🔚 Help		
(min)	eToken [PRO]			
Local Machine	Details Settings Certi	ficates & keys		
Local Machine			Dalata	
	st Exchange key	<beb2b14a-e935-4476-bfb3-8e22d95< td=""><td>Delete</td><td></td></beb2b14a-e935-4476-bfb3-8e22d95<>	Delete	
i -				
eToken [AKS if				
	Version	V3		^
	Serial number	11 00 00 00 00 00 5d 41 81 23		
	Signature algorithm	All new old activen upp keeps		· 11
	Valid from	Tuesday, 14 October 2003 2-24-59 AM		
	Valid to	Thursday, 14 October 2003 2:24:58 AM		
	Subject	AU, nsw, ctd, cisco, vpncert, ericetoken		200004
	Keu container	heh2h14a-e935-4476-hfh3-8e22d95a3d19		~
			Refr	esh
			Mor	B:

Configureer de Cisco VPN-client om het certificaat voor verbinding met de PIX te gebruiken

Deze stappen tonen de procedures aan die worden gebruikt om de Cisco VPN-client te configureren om het certificaat voor PIX-verbindingen te gebruiken.

1. Start de Cisco VPN-client. Onder Connection-ingangen klikt u op **Nieuw** om een nieuwe verbinding te maken.

Ø VPN Client - Version	n 4.0.3 (Rel)			
Connection Entries Status	Certificates Log	Options	Help	
<u>C</u> onnect to to_pix	Ctrl+O	-	×4	CISCO SYSTEMS
Disconnect	Ctrl+D		Delete	كالتحاقي التح
C <u>r</u> eate Shortcut <u>M</u> odify				
D <u>e</u> lete Dyplicate				1 fans
Set as Default Connect	ion Entry			
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			¥
[▲]				•
Not connected.				

2. Specificeer de verbindingsdetails, specificeer certificaatverificatie, selecteer het certificaat dat uit inschrijving is verkregen. Klik op

Create New VPN Connection Entr	y 🛛
to_pix	-
connection to pix	- 5000
209.165.201.20	
Transport Backup Servers Dial-Up	1
ntication	
vord:	
uthentication	
token (Microsoft)	<u> </u>
Certificate Chain	
word <u>S</u> ave	e Cancel
	Create New VPN Connection Entration to_pix connection to pix 209.165.201.20 Transport Backup Servers Dial-Up ntication vord: uthentication token (Microsoft) Certificate Chain word

3. Als u de Cisco VPN-clientverbinding naar de PIX wilt starten, selecteert u de gewenste

Connection-ingang en vervolgens klikt u op **Connect**.

🙆 VPN Client - Versio	on 4.0.3 (Rel)			
Connection Entries Status	C <u>e</u> rtificates <u>L</u> og	Options	Help	
<u>C</u> onnect to to_pix	Ctrl+O	-	24	CISCO SYSTEM
Disconnect	: Ctrl+D		Delete	ale ale
Create Shortcut		pully	Delete	
<u>M</u> odify		2	Heat	T
D <u>e</u> lete			209.165.201	.20 IPS
Dyplicate				
<u>S</u> et as Default Connec	tion Entry]		
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			
•		1		
Not connected.				

Installeer Token Smart-stuurprogramma's

Deze stappen tonen de installatie van de Aladdin-<u>Smartcard-</u>chauffeurs aan.

1. Open de wizard Token Run Time Environment 3.51 (Tijdmilieu).



2. Accepteer de bepalingen van de Licentieovereenkomst en klik op **Volgende**.

End-User License Agreement	Tokon
Please read the following license agreement carefully	Your Key to eSecurity R
ALADDIN KNOWLEDGE SYSTE	EMS LTD.
ETOKEN ENTERPRISE END USER LI	CENSE AGREEMENT
CAREFULLY BEFORE OPENING THE PA 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 AGREEMENT ACKAGE AND/OR USING ORE DOWNLOADING OR ALL ORDERS FOR AND RODUCTS (including without , eToken® keys and the User ALADDIN KNOWLADGE
 I accept the license agree I do not accept the license 	ement se agreement
Reset KBa	ck Next > Cancel

3. Klik op **Install** (Installeren).

🙀 eToken Run Time Environment	3.51 Setup 📃 🗖 🔀
Ready to Install the Application	T-Proven
Click Next to begin installation.	Your Key to eSecurity RTE
	Please click Next to begin installation.
	<back next=""> Cancel</back>

4. De Token Smartcard stuurprogramma's zijn nu geïnstalleerd. Klik op **Voltooien** om de wizard te

verlaten.



Verifiëren

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

Bepaalde opdrachten met **show worden ondersteund door de tool** <u>Output Interpreter (alleen voor</u> <u>geregistreerde klanten)</u>. <u>Hiermee kunt u een analyse van de output van opdrachten met</u> **show genereren**.

• toon crypto isakmp sa-Toont alle huidige IKE (Internet Key Exchange) veiligheidsassociaties (SAs) bij een peer.

```
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
```

 Laat crypto ipsec sa-displays de instellingen die worden gebruikt door de huidige beveiligingsassociaties.

```
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:

Problemen oplossen

Raadpleeg <u>Problemen oplossen de PIX om gegevensverkeer via een vaste IPSec-tunnelbestand</u> <u>door te geven</u> voor meer informatie over het oplossen van deze configuratie.

Gerelateerde informatie

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Ondersteuningspagina voor IPsec (IP security protocol)
- <u>Cisco VPN-clientondersteuningspagina</u>
- Ondersteuning van PIX 500 Series firewalls
- Technische ondersteuning Cisco-systemen