Esempio di configurazione di IPSec tra PIX e client VPN Cisco con certificati smart card

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Registrare e configurare il PIX Configurazioni Registra certificati client VPN Cisco Configurare il client VPN Cisco per utilizzare il certificato per la connessione al PIX Installa driver per smart card eToken Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene illustrato come configurare un tunnel VPN IPSec tra un firewall PIX e un client VPN Cisco 4.0.x. L'esempio di configurazione riportato in questo documento evidenzia anche la procedura di registrazione dell'Autorità di certificazione (CA) per i router Cisco IOS® e i client VPN Cisco, nonché l'utilizzo di una Smartcard per l'archiviazione dei certificati.

Per ulteriori informazioni sulla configurazione di IPSec tra router Cisco IOS e client VPN Cisco con certificati Entrust, consultare il documento sulla <u>configurazione di IPSec tra router Cisco IOS e</u> <u>client VPN Cisco con certificati Entrust</u>.

Per ulteriori informazioni sulla configurazione di più autorità di certificazione di identità sui router Cisco IOS, consultare il documento sulla <u>configurazione di più autorità di certificazione di identità</u> <u>sui router Cisco IOS</u>.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco PIX Firewall con software versione 6.3(3)
- Cisco VPN Client 4.0.3 su un PC con Windows XP
- Nel presente documento, come server CA viene utilizzato un server CA Microsoft Windows 2000.
- I certificati sul client VPN Cisco vengono archiviati utilizzando la smart card <u>Aladdin</u> e-Token.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici</u>.

Registrare e configurare il PIX

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Configurazioni

Nel documento vengono usate queste configurazioni.

- <u>Registrazione certificato su PIX Firewall</u>
- <u>Configurazione firewall PIX</u>

Registrazione certificato su PIX Firewall				
! Define a hostname and domain name for the router.				
<pre>! The fully qualified domain name (FQDN) is used !</pre>				
as the identity of the router during certificate				
<pre>enrollment. pix(config)#hostname sv2-11</pre>				
<pre>sv2-11(config)#domain-name cisco.com</pre>				
<pre>! Confirm that you have the correct time set on the</pre>				
PIX. show clock				
clock set				
! This command clears the PIX RSA keys. ca zeroize				
rsa				
! Generate RSA (encryption and authentication) keys.				
ca gen rsa key				

- Select the modulus size (512 or 1024). !--- Confirm the keys generated. show ca mypub rsa - 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 Configurazione firewall PIX 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
floodquard 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)#
```

Registra certificati client VPN Cisco

Ricorda di installare tutti i driver e le utilità necessari forniti con il dispositivo Smartcard sul PC per poterlo usare con il client VPN Cisco.

In questa procedura vengono illustrate le procedure utilizzate per registrare il client VPN Cisco per

i certificati MS. Il certificato è archiviato nell'archivio smart card <u>Aladdin</u> e-Token.

- 1. Avviare un browser e accedere alla pagina del server dei certificati (http://CAServeraddress/certsrv/, in questo esempio).
- 2. Selezionare **Richiedi certificato** e fare clic su

Home
Hom
client, or ecurely encrypt ou request

3. Nella finestra Scegli tipo di richiesta, selezionare **Richiesta avanzata** e fare clic su **Avanti**.

Microsoft Certificate Services kobe	Hon
Choose Request Type	
Please select the type of request you would like to make:	
lease select the type of request you would like to make.	
 User certificate request: 	
Web Browser Certificate	
E-Mail Protection Certificate	
 Advanced request 	
	Next >

4. Selezionare Invia una richiesta di certificato a questa CA utilizzando un modulo e fare clic su Avanti.

Microsoft Certificate Services kobe	<u>Home</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another u following methods. Note that the policy of the certifi the certificates that you can obtain.	ser, or a computer using one of the cation authority (CA) will determine
 Submit a certificate request to this CA using a 	form.
 Submit a certificate request using a base64 er renewal request using a base64 encoded PKC 	ncoded PKCS #10 file or a CS #7 file.
 Request a certificate for a smart card on behal Card Enrollment Station. You must have an enrollment agent certificate to subm. 	f of another user using the Smart

5. Compilare tutti gli elementi del modulo Richiesta avanzata di certificati.Accertarsi che il reparto o l'unità organizzativa corrisponda al nome del gruppo Cisco VPN Client, come configurato nel nome del gruppo VPN PIX. Selezionare il provider di servizi certificati (CSP) corretto per l'instellazione

l'installazione.

microsom certilit	cate Services Kobe		ш
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 Option	ns:		
Hash Algorithm:	SHA-1	2.24	
, and the second se	Only used to sign request.		
	Save request to a PKCS #10 file		
Attributes:	× ×		
		Submit >	_

6. Selezionare **Sì** per continuare l'installazione quando viene visualizzato l'avviso Convalida script

potenziale.

	This Web site is requesting a new certificate on your behalf. You should allow only trusted web sites to request a certificate for you.
<u> </u>	Do you want to request a certificate now?
	Yes No

7. La registrazione certificati richiama l'archivio eToken. Immettere la password e fare clic su

Input el ok	en password
eToken:	eToken [AKS ifdh 0]
Password:	******
Login to yo your privat	our eToken to enable using/creating/removi e key.

8. Fare clic su Installa il

certificato.

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

9. Selezionare **Sì** per continuare l'installazione quando viene visualizzato l'avviso Convalida script

potenziale.

Potenti	al Scripting Violation
1	This Web site 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. Selezionare Sì per aggiungere il certificato radice all'archivio

Subject : kobe, vpn, apt-vpn, ctd, nsw, AU	e/
Subject : kobe, vpn, apt-vpn, ctd, nsw, AU	
Subject hereby (ph) and (ph) call (bil) he	
Issuer : Self Issued	
Time Validity : Monday, 25 August 2003 through Thursday, 25	5 August 20
Serial Number : 43C2EE28 43CE56A6 4457F2D2 23EDFED2	-
Thumbprint (sha1) : 3D47C8F6 2703B88D C2BD4F68 7B5300A	40 3A927B4
Thumbprint (md5) : A1E23E81 08538FA4 6BB4F187 49EC774F	-

11. Viene visualizzata la finestra Certificato installato che conferma l'installazione.

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

12. Per visualizzare il certificato archiviato nella smart card, utilizzare il visualizzatore applicazioni

eToken.

🖶 eToken Proper	rties		
eToken			
	🕺 Advanced 🕗 Ref	resh 🛛 💦 Help	
	eToken [PRO]		
		-	
Local Machine	Details Settings Cert	ificates & keys	
	🖳 ericetoken		Delete
	端 Exchange ke	y <beb2b14a-e935-4476-bfb3-8e22d95< td=""><td></td></beb2b14a-e935-4476-bfb3-8e22d95<>	
<u>.</u>			
eToken [AKS if			
	Version	V3	
	Serial number	11 00 00 00 00 00 5d 41 81 23	
	Issuer	AU, nsw, ctd, apt-vpn, vpn, kobe	1111
	Valid from	Tuesday, 14 October 2003 2:24:58 AM	
	Subject	AU, nsw, ctd, cisco, vpncert, ericetoken	
	Keu container	heh2h14a-e935-4476-hfh3-8e22d95a3d19	
			Refresh
			More

Configurare il client VPN Cisco per utilizzare il certificato per la connessione al PIX

In questa procedura vengono illustrate le procedure utilizzate per configurare il client VPN Cisco in modo che utilizzi il certificato per le connessioni PIX.

1. Avviare il client VPN Cisco. In Voci di connessione fare clic su **Nuovo** per creare una nuova connessione.

VPN Client - Version 4.0.3 (Rel)				
Connection Entries Status	Certificates Log	Options	Help	
<u>C</u> onnect to to_pix	Ctrl+O	-	M	CISCO SYSTEMS
Disconnect	Ctrl+D	22	Delete	بال بال
C <u>r</u> eate Shortcut <u>M</u> odify				
D <u>e</u> lete Dyplicate			HOSE	11ans
Set as Default Connect	ion Entry			
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			
I				<u> </u>
Not connected.				

2. Completare i dettagli di connessione, specificare l'autenticazione certificato, selezionare il certificato ottenuto dalla registrazione. Fare clic su

🤌 VPN Client	Create New VPN Connecti	on Entry	
Connection Entry:	to_pix		- Ca
Description:	connection to pix	S	
<u>H</u> ost:	209.165.201.20		
Authentication	Transport Backup Servers	Dial-Up	
C Group Authe	ntication		
<u>N</u> ame:			
Password:			
C <u>o</u> nfirm Passv	ord:		
Certificate A:	thentication		
Name:	oken (Microsoft)		
Send CA (Certificate Chain		
(
Erase User Passv	vord	Save	Cance
AT 15 TO 16 STATE OF A TO 16 TO 16 TO 16	2019-01	Contraction of the local data	2.21 2.122

3. Per avviare la connessione del client VPN Cisco al PIX, selezionare la voce di connessione

desiderata e fare clic su **Connetti**.

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	C	ISCO SYSTEMS
Disconnect	Ctrl+D		2 Delaha		ih ih
C <u>r</u> eate Shortcut Modifu		pairy	Delete		
moully		-	Host		Trans
D <u>e</u> lete Dyplicate			209.165.201	.20	IPSe
<u>S</u> et as Default Connect	on Entry				
<u>N</u> ew <u>I</u> mport					
Exit VPN Client	Ctrl+Q				
					•
Not connected.					

Installa driver per smart card eToken

In questa procedura viene illustrata l'installazione dei driver per smart card <u>Aladdin</u> eToken.

1. Aprire l'installazione guidata di eToken Run Time Environment 3.51.



2. Accettare i termini del Contratto di Licenza e fare clic su Avanti.

Your Key to eSecurity S LTD. NSE AGREEMENT AD THIS AGREEME CAGE AND/OR USI	NT
S LTD. NSE AGREEMENT Ad This Agreeme (Age And/or Usi)	NT
NSE AGREEMENT Ad This Agreeme (Age And/or Usi)	NT
AD THIS AGREEME AGE AND/OR USI	NT NG
E DOWNLOADING (LL ORDERS FOR AI UCTS (including with oken® keys and the U ADDIN KNOWLAD	OR ND Iout Ser GE
t reement	
	L ORDERS FOR A UCTS (including with ken® keys and the U ADDIN KNOWLAD sement

3. Fare clic su **Installa**.

🙀 eToken Run Time Environment	3.51 Setup
Ready to Install the Application	eToken
Llick Next to begin installation.	Your Key to eSecurity RTE
ſ	
	Please click Next to begin installation.
	< Back Next > Cancel
ę.,	ومراجع المستر المالي المراجع

4. I driver eToken Smartcard sono stati installati. Per uscire dall'installazione guidata, fare clic su

Fine.



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** <u>strumento Output Interpreter (solo utenti</u> <u>registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> **show.**

• show crypto isakmp sa: visualizza tutte le associazioni di sicurezza (SA) IKE (Internet Key Exchange) correnti in un 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
```

 show crypto ipsec sa: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.

```
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:
```

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi di configurazione, consultare il documento sulla <u>risoluzione dei problemi relativi al PIX per il passaggio del traffico di dati su un tunnel IPSec</u> <u>stabilito</u>.

Informazioni correlate

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Pagina di supporto per IPSec (IP Security Protocol)
- Pagina di supporto per Cisco VPN Client
- Pagina di supporto per i firewall PIX serie 500
- <u>Supporto tecnico Cisco Systems</u>