使用智慧卡證書的PIX和Cisco VPN客戶端之間的 IPSec配置示例

目錄

 簡介

 必要條件

 需求

 採用元件

 慣例

 註冊並配置PIX

 組態

 註冊Cisco VPN客戶端證書

 配置Cisco VPN客戶端以使用證書連線到PIX

 安裝eToken智慧卡驅動程式

 驗證

 疑難排解

 相關資訊

<u> 簡介</u>

本文檔演示如何在PIX防火牆和Cisco VPN客戶端4.0.x之間配置IPSec VPN隧道。本文檔中的配置 示例還重點介紹了Cisco IOS®路由器和Cisco VPN客戶端的證書頒發機構(CA)註冊過程,以及智慧 卡用作證書儲存的方法。

請參閱<u>使用委託證書在Cisco IOS路由器和Cisco VPN客戶端之間配置IPSec</u>,以瞭解有關使用委託 證書在Cisco IOS路由器和Cisco VPN客戶端之間配置IPSec的詳細資訊。

請參閱<u>在Cisco IOS路由器上配置多身份證書頒發機構</u>,瞭解有關在Cisco IOS路由器上配置多身份 證書頒發機構的詳細資訊。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

• 運行軟體版本6.3(3)的Cisco PIX防火牆

- 運行Windows XP的PC上的Cisco VPN客戶端4.0.3
- •在本文檔中, Microsoft Windows 2000 CA伺服器用作CA伺服器。
- Cisco VPN使用者端上的憑證是使用<u>Aladdin</u> e-Token智慧卡儲存的。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱思科技術提示慣例。

<u>註冊並配置PIX</u>

本節提供用於設定本檔案中所述功能的資訊。

注意:若要查詢有關本文檔中使用的命令的其他資訊,請使用<u>命令查詢工具</u>(僅限<u>註冊</u>客戶)。

<u>組態</u>

本檔案會使用這些設定。

- PIX防火牆上的證書註冊
- <u>PIX防火牆配置</u>

PIX防火牆上的證書註冊
! 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(confirm that you have the correct time set on the
PIX show clock
clock set
! This command clears the PIX RSA keys. ca zeroize
rsa
ca den rsa kev
! 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
PIX防火牆配置

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)#

<u>註冊Cisco VPN客戶端證書</u>

請記得在PC上安裝智慧卡裝置隨附的所有必要的驅動程式和實用程式,以便與Cisco VPN客戶端配 合使用。

以下步驟演示用於註冊Cisco VPN Client for MS證書的過程。憑證儲存在<u>Aladdin</u> e-Token Smartcard儲存區上。

- 1. 啟動瀏覽器並前往憑證伺服器頁面(在本範例中為http://CAServeraddress/certsrv/)。
- 2. 選擇Request a certificate, 然後按一下Next。

Address i http://209.165.201.21/certsrv/	So Lir
Microsoft Certificate Services kobe	Home
Welcome	
You use this web site to request a certificate for your web other secure program. Once you acquire a certificate, you identify yourself to other people over the web, sign your e- your e-mail messages, and more depending upon the type	browser, e-mail client, or will be able to securely mail messages, encrypt e of certificate you request.
Select a task: Retrieve the CA certificate or certificate revocation li Request a certificate Check on a pending certificate 	ist
	Next >
在「選擇請求型別」視窗中,選擇 高級請求 ,然後按一下 下一步	0
Microsoft Certificate Services kobe	Home
Choose Request Type	
Please select the type of request you would like to make:	
 User certificate request: 	
Web Browser Certificate E-Mail Protection Certificate	

4. 選擇Submit a certificate request to this CA using a form,然後按一下Next。

Next >

Advanced request

Microsoft Certificate Services kobe	<u>Home</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a con following methods. Note that the policy of the certification author the certificates that you can obtain.	nputer using one of the rity (CA) will determine
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded PKC 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 u Card Enrollment Station. You must have an enrollment agent certificate to submit a request for	user using the Smart another user.
	Next >

5. 填寫「高級證書請求」表單中的所有專案。確保部門或組織單位(OU)對應於Cisco VPN客戶端 組名稱,如PIX vpngroup名稱中所配置。選擇適用於您的設定的正確證書服務提供商(CSP)。

			Inomi
Advanced Ce	rtificate Request		
aenalying inton			
Name:	ericetoken		
E-Mail:			
Company:	cisco		
Department:	vpncert		
City:	ctd		
State:	nsw		
Country/Region:	AU		
ntended Purpos	se:		
	Client Authentication Certificate 😒		
Key Options:			
CSP:	eToken Base Cryptographic Provider		
Key Usage:	○Exchange ○Signature ●Both		
Key Size:	512 Min: 384 (common key sizes: 512 1024) Max:1024		
	Oreate new key set		
	Set the container name		
	OUse existing key set		
	Enable strong private key protection		
	Mark keys as exportable		
	You must be an administrator to generate		
dditional Option	ns:	5.40 5.40	
Hash Algorithm:	SHA-1		
	Only used to sign request.		
	Save request to a PKCS #10 file		
Attributes:			
		Submit	>

6. 選擇Yes可在收到潛在指令碼驗證警告時繼續安裝。

Potential Sc	cripting Violation
	is Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a rtificate for you. 9 you want to request a certificate now?
	Yes No
7. 證書註冊將	呼叫eToken儲存。輸入密碼並按一下OK。
eToken E	Base Cryptographic Provider 🛛 🔯
eTo Input eTo	ken password
eToken:	eToken [AKS ifdh 0]
Password	******
Login to y your priva	vour eToken to enable using/creating/removing ate key.

8. 按一下「Install this certificate」。

Less <<

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

Cancel

0K

 Puterinal Seripting violation

 Image: Seripting violation

 <th

10. 選擇Yes以將根證書新增到根儲存區。

Root Certificate Store Image: Store St

11. 出現「Certificate Installed(證書已安裝)」視窗,確認安裝成功。



12. 使用eToken Application Viewer可檢視智慧卡上儲存的證書。

🖶 eToken Properties	8		
eToken			
Local Machine	Advanced Ref ken [PRO] Details Settings Cert ericetoken Exchange ke	resh nelp ificates & keys y <beb2b14a-e935-4476-bfb3-8e22d95< th=""><th>Delete</th></beb2b14a-e935-4476-bfb3-8e22d95<>	Delete
	Version Serial number Signature algorithm Issuer Valid from Valid to Subject Key container	V3 11 00 00 00 00 00 5d 41 81 23 RSA_SHA1RSA AU, nsw, ctd, apt-vpn, vpn, kobe Tuesday, 14 October 2003 2:24:58 AM Thursday, 14 October 2004 2:34:58 AM AU, nsw, ctd, cisco, vpncert, ericetoken heb2b14a-e935-4476-bfb3-8e22d95a3d19	Refresh More

配置Cisco VPN客戶端以使用證書連線到PIX

這些步驟演示了將Cisco VPN客戶端配置為使用證書進行PIX連線的過程。

1. 啟動Cisco VPN客戶端。在Connection Entries下,按一下New以建立新連線。

oppection Entries Status	Certificates Log	Options	Help	
<u>Connect to to_pix</u>	Ctrl+O			CISCO SYSTEM
Disconnect	Ctrl+D			
Create Shortcut		-bdity	Delete	
Modify			Haat	т.
D <u>e</u> lete				- 10
Duplicate				
Set as Default Connection	on Entry			
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			¥
1.		_		

2. 完成連線詳細資訊,指定證書身份驗證,選擇從註冊中獲取的證書。按一下「Save」。

Connection Entry: to_pix				allow .
Description: connection	on to pix		50	
	201.00			
Host 209, 165.2	201.20	herzania di		
Authentication Transpo	ort Backup Server:	s Dial-Up		r.
C Group Authentication				
Name:				
Password:				
Confirm Password:				
Certificate Authentication	on			
<u>N</u> ame: ericetoken (Mid	crosoft)		•	
Send CA Certificate	Chain			
Send CA Certificate	Chain			
Erase User Password	Chain	Save	Cano	el
Erase User Password	Chain	<u>S</u> ave	Cano	el
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN	Chain 客戶端連線,請選擇	<u>S</u> ave 所需的連線條目	Canc 1,然後按一	el F 連線 。
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version	Chain 客戶端連線,請選擇 n 4.0.3 (Rel)	<u>S</u> ave 所需的連線條目	Canc 1,然後按一	eel 下連線。
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version Connection Entries Status	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) C <u>e</u> rtificates Log Op	<u>S</u> ave 所需的連線條目 tions <u>H</u> elp	Canc 1,然後按一 ^一	el F連線。
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version Connection Entries Status Connect to to_pix Disconnect	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O	<u>S</u> ave 所需的連線條目 tions <u>H</u> elp	Canc 1,然後按一 ^一	el F連線。 Cisco Systems
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version Connection Entries Status Connect to to_pix Disconnect Create Shortcut	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>S</u> ave 所需的連線條目 tions <u>H</u> elp	Canc 1,然後按一	el 下連線。 Cisco Systems
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version Connection Entries Status Connect to to_pix Disconnect Create Shortcut Modify	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O	<u>S</u> ave 所需的連線條目 tions <u>H</u> elp	Canc 1,然後按一	eel 下連線。 Cisco Systems
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version ©onnection Entries Status ©onnect to to_pix Disconnect Create Shortcut Modify Delete	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>Save</u> 所需的連線條目 tions <u>H</u> elp fy Delete Host	Canc 1,然後按一 5,201,20	eel 下連線。 Cisco Systems
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version © onnection Entries Status © onnect to to_pix © isconnect Create Shortcut Modify Delete Duplicate	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>S</u> ave 所需的連線條目 tions <u>H</u> elp fy Delete Host 209.1	Canc 1,然後按一 55.201.20	eel 下連線。 Cisco Systems Liliumilium Trans IPSe
「Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN系 ② VPN Client - Version ② Onnection Entries Status © Connect to to_pix © Disconnect Create Shortcut Modify Delete Duplicate Set as Default Connecti	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>S</u> ave 所需的連線條目 tions Help fy Delete Host 209.10	Canc 3 , 然後按一 65.201.20	eel 下連線。 Cisco Systems Lilling of the second secon
☐ Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version ©onnection Entries Status ©onnect to to_pix ©isconnect Create Shortcut Modify Delete Duplicate Set as Default Connecti New	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>Save</u> 所需的連線條目 tions Help fy Delete Host 209.10	Canc ,然後按一	eel 下連線。 Cisco Systems Luluuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
☐ Send CA Certificate Erase User Password 要啟動與PIX的Cisco VPN ② VPN Client - Version ©onnection Entries Status ©onnect to to_pix ©isconnect Create Shortcut Modify Delete Duplicate Set as Default Connecti New Import	Chain 客戶端連線,請選擇 n 4.0.3 (Rel) Certificates Log Op Ctrl+O Ctrl+D	<u>Save</u> 所需的連線條目 tions Help fy Delete <u>Host</u> 209.10	Canc ,然後按一 65.201.20	eel 下連線。 Cisco Systems Lullium dine Trans IPSe

安裝eToken智慧卡驅動程式

以下步驟演示如何安裝<u>Aladdin</u> eToken智慧卡驅動程式。



2. 接受許可協定條款,然後點選下**一步**。

🛃 eToken Run Time Environment 3.51 Setup		×
End-User License Agreement Please read the following license agreement carefully	eToken Your Key to eSecurity R	ГЕ
ALADDIN KNOWLEDGE SYSTE	MS LTD.	^
ETOKEN ENTERPRISE END USER LIC	CENSE AGREEMENT	
IMPORTANT INFORMATION - PLEASE H CAREFULLY BEFORE OPENING THE PA THE CONTENTS THEREOF AND/OR BEFO INSTALLING THE SOFTWARE PROGRAM. USE OF THE ETOKEN ENETERPRISE PRO limitation, libraries, utilities, diskettes, CD_ROM, Guide) (hereinafter "Product") SUPPLIED BY	READ THIS AGREEMENT CKAGE AND/OR USING ORE DOWNLOADING OR ALL ORDERS FOR AND ODUCTS (including without eToken® keys and the User ALADDIN KNOWLADGE	
 I accept the license agree I do not accept the license 	ment e agreement	
Reset Kac	k Next > Cancel	

3. 按一下「Install」。

eToken Run Time Environment	t 3.51 Setup
Ready to Install the Application	Toton
Click Next to begin installation.	Your Key to eSecurity RTE
	Please click Next to begin installation.
	<back next=""> Cancel</back>

4. 現在已安裝eToken智慧卡驅動程式。按一下完成以退出安裝嚮導。



<u>驗證</u>

本節提供的資訊可用於確認您的組態是否正常運作。

<u>輸出直譯器工具(</u>僅供<u>註冊</u>客戶使用)支援某些show命令,此工具可讓您檢視<u>show</u>命令輸出的分析。

 show crypter 	o isakmo sa	— 顯示對等	≦體上的所有	當前網際網	路金鑰交換(IK	F)安全關聯(SA)。
SV2-11 (conf	ia)# show cr	voto isa sa				
Total :	1	1600 -20 20				
Embryonic :	0					
dst		src	state	pending	created	
209.165.2	01.20 209	.165.201.19	QM_IDLE	0	1	
 show crypter 	o ipsec sa -	– 顯示當前努	R 全關聯使用	目的設定。		
SV1-11(conf	ig)# show cr	ypto ipsec s	a			
interface:	outside					
Crypto	map tag: my	map, local a	ddr. 209.16	5.201.20		
local ident	(addr/mask	/prot/port):	(0.0.0.0/0	.0.0.0/0/0)		
remote iden	t (addr/mas	k/prot/port)	: (10.0.0.1)	0/255.255.25	55.255/0/0)	
current_pee	er: 209.165.	201.19:500				
dynamic all	ocated peer	ip: 10.0.0.	10			
PERMIT, fla	gs={}					
#pkts encap	s: 4, #pkts	encrypt: 4,	#pkts diges	st 4		
#pkts decap	s: 7, #pkts	decrypt: 7,	#pkts veri:	fy 7		
#pkts compr	essed: 0, #	pkts decompr	essed: 0			
#pkts not c	ompressed:	0, #pkts com	pr. failed:	0, #pkts de	ecompress faile	d: 0
#send error	s 0, #recv	errors O				
local crypt	o endpt.: 2	09.165.201.2	0, remote c	rypto endpt.	: 209.165.201.	19
path m	tu 1500, ip	sec overhead	56, media m	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:

<u>疑難排解</u>

如需此配置故障排除的詳細資訊,請參閱排除PIX故障以在已建立的IPSec隧道上傳遞資料流量。

相關資訊

- Cisco Secure PIX防火牆命令參考
- <u>要求建議 (RFC)</u>
- IPSec (IP 安全通訊協定)支援頁面
- Cisco VPN使用者端支援頁面
- PIX 500系列防火牆支援頁面
- 技術支援 Cisco Systems