スマート カード証明書を使用した PIX と Cisco VPN クライアント間の IPSec 設定例

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 PIXの登録と設定

 設定

 Cisco VPN Client証明書の登録

 PIXへの接続用に証明書を使用するためのCisco VPN Clientの設定

 eTokenスマートカードドライバのインストール

 確認

 トラブルシュート

 関連情報

<u>概要</u>

このドキュメントでは、PIX FirewallとCisco VPN Client 4.0.xの間にIPSec VPNトンネルを設定す る方法について説明します。このドキュメントの設定例では、Cisco IOS®ルータとCisco VPN Clientの両方の認証局(CA)登録手順と、証明書ストレージとしてのスマートカードの使用につい ても説明します。

Entrust証明書を使用したCisco IOSルータとCisco VPN Client間のIPSecの設定の詳細は、『 <u>Entrust証明書を使用したCisco IOSルータとCisco VPN Client間のIPSecの設定</u>』を参照してくだ さい。

Cisco IOSルータでの複数ID認証局の設定の詳細については、『<u>Cisco IOSルータでの複数ID認証</u> <u>局の設定</u>』を参照してください。

前提条件

<u>要件</u>

このドキュメントに特有の要件はありません。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

・ソフトウェアバージョン6.3(3)が稼働するCisco PIX Firewall

• Windows XPを実行しているPC上のCisco VPN Client 4.0.3

•このドキュメントでは、Microsoft Windows 2000 CAサーバをCAサーバとして使用します。

• Cisco VPN Clientの証明書は、<u>Aladdin</u> e-Token Smartcardを使用して保存さ れます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細は、「<u>シスコ テクニカル ティップスの表記法</u>」を参照してください。

PIXの登録と設定

ここでは、このドキュメントで説明する機能を設定するための情報を示します。

注:このドキュメントで使用されているコマンドの詳細を調べるには、<u>Command Lookup</u> <u>Tool(</u>登録ユーザ<u>専用)を使用</u>してください。

<u>設定</u>

このドキュメントでは次の設定を使用します。

- <u>PIX Firewallでの証明書登録</u>
- <u>PIX ファイアウォールの設定</u>

PIX Firewallでの証明書登録 !--- 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 !--- 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
PIX ファイアウォールの設定
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>Cisco VPN Client証明書の登録</u>

Cisco VPN Clientで使用するPCに、スマートカードデバイスに付属の必要なドライバとユーティリティをすべてインストールしてください。

次の手順は、MS証明書用のCisco VPN Clientの登録に使用する手順を示しています。証明書は Aladdin e-Token Smartcardストア<u>に保存さ</u>れています。

- 1. ブラウザを起動し、証明書サーバのページ(この例ではhttp://CAServeraddress/certsrv/)に移動します。
- 2. [Request a certificate]を選択し、[Next]をクリックします。

ddress	Attp://209.1	.65.201.21/certsrv/
--------	--------------	---------------------

Microsoft Certificate Services -- kobe

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- O Retrieve the CA certificate or certificate revocation list
- Request a certificate
- O Check on a pending certificate

Next >

3. <u>「要求タイプの選択」ウィンドウで「拡張要求」を選択し、「次へ」をクリックします。</u>

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. [Submit a certificate request to this CA using a form]を選択し、[Next]をクリックします。

📑 Go Lir

Home

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

5. [Advanced Certificate Request]フォームのすべての項目に入力します。部門(OU)または組織 単位(OU)が、PIX vpngroup名で設定されているCisco VPN Clientグループ名に対応している ことを確認します。セットアップに適した正しい証明書サービスプロバイダー(CSP)を選択 します。

Advanced Co	ertificate Request	
dontifying Info	rmation	
identifying into	imauon.	
Name	ericetoken	
⊏-iviaii		
Company	: cisco	
Department	vpncert	
City	: ctd	
State	nsw	
Country/Region	AU	
Intended Purpo	se:	
	Client Authentication Certificate 😒	
Kev Options:		
CSP	eToken Base Cryptographic Provider	
Key Usage	: OExchange OSignature Both	
Key Size	: 512 Min: 384 (common key sizes: 512 1024)	
	Max 1024	
	Create new key set	
	OUse existing key set	
	Enable strong private key protection	
	🗌 Mark keys as exportable	
	🔲 Use local machine store	
Additional Optic	You must be an administrator to generate	
Hash Algorithm:	SHA-1	$\approx 24^5$
	Only used to sign request.	
	Save request to a PKCS #10 file	
Attributes:		
		Submit >

6. Potential Scripting Validation警告が表示されたら、**Yes**を選択してインストールを続行します。

Potential Scripting Violation	
This Web site is requesting a new certificate on your behalf. You should allow only trusted certificate for you. Do you want to request a certificate now?	Web sites to request a
Yes No	
7. 証明書の登録に <mark>より、eTokenストアが呼び出されます。パスワードを入</mark> 力)し、「 OK 」をク
eToken Base Cryptographic Provider 🛛 🛛	
eToken	
Input eToken password	
eToken: [eToken [AKS itdh 0]	
Password: *******	
Login to your eToken to enable using/creating/removing your private key.	
Less << OK Cancel	
8. [Install this certificate] をクリックします。	
Microsoft Certificate Services kobe	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	

9. Potential Scripting Validation警告が表示されたら、**Yes**を選択してインストールを続行しま

9 。 Potentia	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. ルート証明書をルートストアに追加するには、[Yes]を選択します。

0



11. [Certificate Installed]ウィンドウが表示され、正常にインストールされたことを確認します

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

12. eToken Application Viewerを使用して、スマートカードに保存されている証明書を表示します。

🚍 eToken Prope	erties		
eToken			
	🔊 Advanced 🕗 Ref	resh 김 Help	
	eToken [PRO]		
Local Machine	Details Settings Left	incates & keys	
	🖳 ericetoken		Delete
	端 Exchange ke	y <beb2b14a-e935-4476-bfb3-8e22d95< td=""><td></td></beb2b14a-e935-4476-bfb3-8e22d95<>	
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	- 11
	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

<u>PIXへの接続用に証明書を使用するためのCisco VPN Clientの設</u> <u>定</u>

次の手順は、PIX接続に証明書を使用するようにCisco VPN Clientを設定する手順を示しています。

1. Cisco VPN Client を起動します。[Connection Entries]で[**New**]をクリック**し**、新しい接続を 作成します。

Connection Entries Status	Certificates Log	Options 1	<u>H</u> elp	
<u>Connect to to_pix</u>	Ctrl+O		M	CISCO SYSTEMS
Disconnect	Ctrl+D	E.	Delete	يال يال
Create Shortcut		DONY	Delete	
Modify		_	Host	Trans
D <u>e</u> lete			1100	Trace
Dyplicate				
Set as Default Connection	on Entry			
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			
<		-		•

2. 接続の詳細を入力し、[Certificate Authentication]を指定し、登録から取得した証明書を選択 します。[Save] をクリックします。

VPN Client Create New VPN Connection Entry
Connection Entry: to_pix
Description: connection to pix
Host: 209.165.201.20
Authentication Transport Backup Servers Dial-Up
C Group Authentication
Name:
Password:
Confirm Password:
 Certificate Authentication <u>Name:</u> ericetoken (Microsoft) Send CA Certificate Chain
, olina a roominado onan
Erase <u>U</u> ser Password <u>Save</u> Cancel

3. PIXへのCisco VPN Client接続を開始するには、目的の接続エントリを選択し、[Connect]を

クリックします。

🕹 VPN Client - Version	4.0.3 (Rel)				
Connection Entries Status	C <u>e</u> rtificates <u>L</u> og	Options	Help		
Connect to to_pix	Ctrl+O	-	×4	Cisco Sys	TEMS
Disconnect	: Ctrl+D		2 Delete	ale	iho
C <u>r</u> eate Shortcut <u>M</u> odify		pairy			
D <u>e</u> lete Dyplicate			209.165.201	.20	I ran IPSe
<u>S</u> et as Default Connection	on Entry				
<u>N</u> ew <u>I</u> mport					
Exit VPN Client	Ctrl+Q	-			
•		- ¢			•
Not connected.					

eTokenスマートカードドライバのインストール

次の手順は、<u>Aladdin</u> eToken Smartcardドライバのイ<u>ンストールを</u>示しています。

1. eToken Run time Environment 3.51セットアップウィザードを開きます。



2. 使用許諾契約書に同意し、[次へ]をクリックします。

🛃 eToken Run Time Environment 3.51 Setup	
End-User License Agreement Please read the following license agreement carefully	eToken Your Key to eSecurity RT
ALADDIN KNOWLEDGE SYSTE	MS LTD.
ETOKEN ENTERPRISE END USER LIC	CENSE AGREEMENT
IMPORTANT INFORMATION - PLEASE I 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 KBac	k Next > Cancel

3. [INSTALL] をクリックします。

Token Run Time Environment 3.51 Setup			
	eTotk	en Security	RT
Please click	Next to begin in:	stallation	<u>.</u>
			<u> </u>
	t 3.51 Setup	t 3.51 Setup	Decee click Next to begin installation

4. eToken Smartcardドライバがインストールされました。[**Finish**]をクリックして、セットア ップウィザードを終了します。



<u>確認</u>

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供し ています。

ー部の show コマンドは<u>アウトプット インタープリタ ツールによってサポートされています(登</u> <u>録ユーザ専用)。このツールを使用することによって、show コマンド出力の分析結果を表示で</u> <u>きます。</u>

• show crypto isakmp sa: ピアにおける現在の Internet Key Exchange (IKE; インターネット鍵 交換) Security Association (SA; セキュリティ アソシエーション)をすべて表示します。 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 : 現在のセキュリティアソシエーションで使用されている設定を表示し

ます。

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): (0.0.0.0/0.0.0.0/0/0)
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:

<u>トラブルシュート</u>

この設定のトラブルシューティング<u>の詳細は、『確立されたIPSecトンネルでデータトラフィッ</u> <u>クを通過させるPIXのトラブルシューティン</u>グ』を参照してください。

<u>関連情報</u>

- <u>Cisco Secure PIX ファイアウォール コマンド リファレンス</u>
- <u>Requests for Comments (RFCs)</u>
- IPSec (IP セキュリティ プロトコル)に関するサポート ページ
- <u>Cisco VPN Client に関するサポート ページ</u>
- <u>PIX 500 シリーズ ファイアウォールに関するサポート ページ</u>
- <u>テクニカルサポート Cisco Systems</u>