# 스마트 카드 인증서를 사용하는 PIX와 Cisco VPN 클라이언트 간 IPSec 구성 예

## 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 PIX 등록 및 구성 구성 Cisco VPN 클라이언트 인증서 등록 PIX에 연결하기 위해 인증서를 사용하도록 Cisco VPN 클라이언트 구성 eToken 스마트 카드 드라이버 설치 다음을 확인합니다. 문제 해결 관련 정보

## <u>소개</u>

이 문서에서는 PIX 방화벽과 Cisco VPN Client 4.0.x 간에 IPSec VPN 터널을 구성하는 방법을 보여 줍니다. 이 문서의 컨피그레이션 예제에서는 Cisco IOS® 라우터와 Cisco VPN Client 모두에 대한 CA(Certification Authority) 등록 절차뿐만 아니라 Smartcard를 인증서 스토리지로 사용하는 방법도 중점적으로 설명합니다.

Cisco IOS 라우터<u>와 Cisco VPN 클라이언트</u> 간<u>에서</u> Entrust 인증서를 사용하여 IPSec을 구성하는 방법에 대한 자세한 내용은 <u>Cisco IOS 라우터</u>와 Cisco VPN 클라이언트 간 IPSec 구성을 참조하십 시오.

Cisco IOS 라우터<u>에서 다중 ID 인증 기관 구성에 대한 자세한 내용은 Cisco IOS 라우터</u>에서 다중 ID 인증 기관 구성을 참조하십시오.

## <u>사전 요구 사항</u>

### <u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

### <u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.3(3)을 실행하는 Cisco PIX Firewall
- Windows XP를 실행하는 PC의 Cisco VPN Client 4.0.3
- 이 문서에서는 Microsoft Windows 2000 CA 서버를 CA 서버로 사용합니다.

• Cisco VPN Client의 인증서는 Aladdin e-Token Smartcard를 사용하여 저장됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

## <u>PIX 등록 및 구성</u>

이 섹션에서는 이 문서에 설명된 기능을 구성하기 위한 정보가 제공됩니다.

**참고:** 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용합니다.

### <u>구성</u>

이 문서에서는 이러한 구성을 사용합니다.

- <u>PIX 방화벽의 인증서 등록</u>
- PIX 방화벽 컨피그레이션

### PIX 방화벽의 인증서 등록 !--- 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 방화벽 컨피그레이션

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 클라이언트 인증서 등록

Cisco VPN Client와 함께 사용할 수 있도록 PC에 스마트 카드 장치와 함께 제공되는 모든 필수 드 라이버 및 유틸리티를 설치해야 합니다.

다음 단계는 MS 인증서에 대해 Cisco VPN 클라이언트를 등록하는 데 사용되는 절차를 보여줍니다. . 인증서는 Aladdin <u>e</u>-Token 스마트 카드 저장소에 저장됩니다.

- 1. 브라우저를 시작하고 인증서 서버 페이지(이 예에서는 http://CAServeraddress/certsrv/)으로 이동합니다.
- 2. Request a certificate(인증서 요청)를 선택하고 Next(다음)를 클릭합니다

ddress	Attp://209.165.201.21/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. 요청 유형 선택 창에서 **고급 요청**을 선택하고 **다음**을 클릭합니다

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

4. Submit a certificate request to this CA using a form(양식을 사용하여 이 CA에 인증서 요청 제 출)을 선택하고 Next(다음)를 클릭합니다

🔁 Go Lir

Home

Microsoft Certificate Services kobe	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a compute following methods. Note that the policy of the certification authority ( the certificates that you can obtain.	er using one of the CA) will determine
<ul> <li>Submit a certificate request to this CA using a form.</li> </ul>	
<ul> <li>Submit a certificate request using a base64 encoded PKCS #1 renewal request using a base64 encoded PKCS #7 file.</li> </ul>	0 file or a
Request a certificate for a smart card on behalf of another user Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another	using the Smart
Tou musc have an enrollment agent certificate to submit a request for anot	Next >

5. 고급 인증서 요청 양식의 모든 항목을 입력합니다.부서 또는 OU(조직 구성 단위)가 PIX vpngroup 이름에 구성된 대로 Cisco VPN 클라이언트 그룹 이름과 일치하는지 확인하십시오. 설정에 적합한 올바른 CSP(Certificate Service Provider)를 선택합니다

interoson contine	Late Delvices Kobe	
Advanced Ce	rtificate Request	
dentitying infor	mation:	
Name:	ericetoken	
E-Mail:		
Company:	cisco	
Department:	vpncert	
City:	ctd	
State:	nsw	
Country/Region:	AU	
ntended Purpos	e:	
	Client Authentication Certificate 💌	
(ev Options:		
CSP:	eToken Base Cryptographic Provider	<b>v</b>
Kev Usage:	O Exchange O Signature   Both	
Kev Size:	512 Min: 384 (common key sizes: 512 1024)	
<i></i>	Max:1024	
	Create new key set	
	O Use existing key set	
	Enable strong private key protection	
	Mark keys as exportable	
	Use local machine store	
dditional Option	You must be an administrator to generate ns:	
Hach Algorithm	SHA.1	2.01
nash Aigunthin. [	Only used to sign request.	
	Save request to a PKCS #10 file	
Attributes:	< × × ×	
		Submit >

6. Potential Scripting Validation 경고가 표시될 때 설치를 계속하려면 Yes를 선택합니다

	Potential S	cripting Violation
		his Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a ertificate for you. o you want to request a certificate now?
		Yes No
7.	인증서 등록	록이 eToken 저장소를 호출합니다. 비밀번호를 입력하고 <b>확인</b> 을 클릭합니다
	eToken	Base Cryptographic Provider
		1
	eTo	oken
	Input eT	oken password
	eToken:	eToken [AKS ifdh 0]
	Passwor	rd: ******
	1.7.	
	Login to your priv	your eToken to enable using/creating/removing /ate key.
	Less	<< OK Cancel

8. 이 인증서 설치를 클릭합니다

.



9. Potential Scripting Validation 경고가 표시될 때 설치를 계속하려면 Yes를 선택합니다

#### Potential 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.

No

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



Sut	ject : kobe, vpn,	ant unn std			
T		apt-ypn, ttu	, nsw, AU		
155	Issuer : Self Issued				
Tim	e Validity : Monda	iy, 25 August	: 2003 throu	gh Thursday, 25 August :	
Ser	al Number : 43C2	EE28 43CE56	5A6 4457F2E	2 23EDFED2	
	moprint (shal) : :	304/08-6 2/	1038888D C28	04F68 /85300A0 3A92/	
110	moprine (mos) : A	AIE23E01 005	000FA4 0004	F10/ 49EC//4F	

Yes

11. Certificate Installed(설치된 인증서) 창이 나타나고 설치에 성공했는지 확인합니다

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

12. 스마트 카드에 저장된 인증서를 보려면 eToken Application Viewer를 사용합니다

🚍 eToken Prop	erties	
eToken		
	Advanced 🕗 Refresh 🛛 🔭 Help	
Local Machine	eToken [PRO] Details Settings Certificates & keys ericetoken Exchange key <beb2b14a-e935-4476-bfb3-8e22c< th=""><th>195</th></beb2b14a-e935-4476-bfb3-8e22c<>	195
	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         Valid to       Thursday, 14 October 2004 2:34:56         Subject       AU, nsw, ctd, cisco, vpncert, ericet         Key container       beb2b14a-e935-4476-bfb3-8e22d9	AM 8 AM token 5a3d19
		More

## <u>PIX에 연결하기 위해 인증서를 사용하도록 Cisco VPN 클라이언</u> <u>트 구성</u>

다음 단계는 PIX 연결에 인증서를 사용하도록 Cisco VPN 클라이언트를 구성하는 데 사용되는 절차 를 보여줍니다.

1. Cisco VPN Client를 시작합니다. Connection Entries(연결 항목)에서 **New(새로 만들기**)를 클 릭하여 새 연결을 생성합니다

onnection Entries Status	Certificates Log	Options	Help	
<u>Connect to to_pix</u>	Ctrl+O	-	M	CISCO SYSTEMS
Disconnect	Ctrl+D	- Selifu	Delete	مناند منابذ
Create Shortcut		Daily	Delete	
<u>M</u> odify			Host	Tran
D <u>e</u> lete			11000	1100
Dyplicate				
Set as Default Connectio	on Entry			
<u>N</u> ew				
Import				
Evit VPN Cliept	Ctrl+O	1		

2. 연결 세부 정보를 입력하고 인증서 인증을 지정하고 등록에서 얻은 인증서를 선택합니다. 저 장을 **클릭합니다** 

Ø 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
G Group Authentication
Name:
Password:
C <u>o</u> nfirm Password:
<ul> <li>Certificate Authentication</li> <li><u>N</u>ame: ericetoken (Microsoft)</li> </ul>
Send CA Certificate Chain
Erase User Password Cancel

3. PIX에 대한 Cisco VPN Client 연결을 시작하려면 원하는 Connection Entry(연결 항목)를 선택

### 하고 Connect(연결)를 클릭합니다

👌 VPN Client - Versio	n 4.0.3 (Rel)				
Connection Entries Status	Certificates Log	Options	Help		
Connect to to_pix	Ctrl+O	-	×4	Cisc	O SYSTEMS
Disconnect	: Ctrl+D		Delete		e álio
Create Shortcut Modify		pany	Delete		
Delete		-	Host 209.165.201	.20	Trans IPSe
Set as Default Connect	ion Entry	-			
<u>N</u> ew <u>I</u> mport					
E <u>x</u> it VPN Client	Ctrl+Q				-
Not connected.					1

# eToken 스마트 카드 드라이버 설치

다음 단계에서는 Aladdin <u>eToken</u> 스마트 카드 드라이버를 설치하는 방법을 보여 줍니다.

1. eToken 런타임 환경 3.51 설치 마법사를 엽니다



2. 라이센스 계약 약관에 동의하고 Next(**다음**)를 클릭합니다

🛃 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
<ul> <li>I accept the license agree</li> <li>I do not accept the license</li> </ul>	ment e agreement
Reset KBac	k Next > Cancel

3. Install(**설치)을 클릭합니다** 

3.51 Setup	🖗 eToken Run Time Environmen
eToken Your Key to eSecurity RTE	Ready to Install the Application Click Next to begin installation.
Please click Next to begin installation.	
< Back Next > Cancel	
< Back Next > Cance	

4. 이제 eToken 스마트 카드 드라이버가 설치되었습니다. **마침**을 클릭하여 설치 마법사를 종료 합니다 .



# <u>다음을 확인합니다.</u>

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 show 명령은 <u>출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면</u> show 명 령 출력의 분석 결과를 볼 수 있습니다.

• show crypto isakmp sa - 피어의 현재 IKE(Internet Key Exchange) 보안 연결(SA)을 모두 표시 합니다.

```
SV2-11(config)#show crypto isa sa
 Total
         : 1
 Embryonic : 0
                                     state
                                               pending
         dst
                          src
                                                           created
   209.165.201.20
                    209.165.201.19
                                     OM IDLE
                                                     0
                                                                 1
• show crypto ipsec sa - 현재 보안 연결에서 사용하는 설정을 표시합니다.
 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:
```



이 컨피그레이션 <u>트러블슈팅에 대한 자세한 내용은 Troubleshooting the PIX to Pass Data Traffic</u> <u>on an Established IPSec Tunnel(설정된 IPSec 터널에서 데이터 트래픽 전달</u>을 위한 PIX 트러블슈 팅)을 참조하십시오.

## <u>관련 정보</u>

- <u>Cisco Secure PIX Firewall 명령 참조</u>
- <u>RFC(Request for Comments)</u>
- IPSec(IP Security Protocol) 지원 페이지
- <u>Cisco VPN 클라이언트 지원 페이지</u>
- PIX 500 Series 방화벽 지원 페이지
- Technical Support Cisco Systems