ASA/PIX 8.x:Microsoft CA 컨피그레이션과 함께 디지털 인증서를 사용하는 사이트 간 IPSec VPN 인증 예

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>관련 제품</u> <u>표기 규칙</u> <u>구성</u> <u>네트워크 다이어그램</u> <u>구성</u> <u>ASA-1 컨피그레이션 요약</u> <u>ASA-1 컨피그레이션 요약</u> <u>ASA-2 컨피그레이션 요약</u> <u>다음을 확인합니다.</u> <u>문제 해결</u> <u>관련 정보</u>

<u>소개</u>

이 문서에서는 Microsoft CA(Certificate Authority) 서버를 사용하여 IPSec 피어를 인증하기 위해 Site-to-Site VPN에서 Cisco Security Appliance(ASA/PIX) 8.x에 서드파티 벤더 디지털 인증서를 수 동으로 설치하는 방법에 대해 설명합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서를 사용하려면 인증서 등록을 위해 CA(인증 기관)에 액세스할 수 있어야 합니다.지원되는 타사 CA 공급업체는 Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, VeriSign입니다.

이 문서에서는 ASA/PIX에 기존 VPN 컨피그레이션이 없다고 가정합니다.

참고: 이 문서에서는 시나리오의 CA 서버로 Windows 2003 서버를 사용합니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• 소프트웨어 버전 8.0(2) 및 ASDM 버전 6.0(2)을 실행하는 Cisco ASA 5510 Adaptive Security Appliance

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>관련 제품</u>

ASA 컨피그레이션은 소프트웨어 버전 8.x를 실행하는 Cisco 500 Series PIX와 함께 사용할 수도 있습니다.

<u>표기 규칙</u>

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

<u>구성</u>

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환 경에서 사용된 RFC 1918 주소입니다.

<u>구성</u>

이 문서에서는 다음 구성을 사용합니다.

• <u>ASA-1 단계별 구성</u>

• <u>ASA-1 컨피그레이션 요약</u>

<u>ASA-1 컨피그레이션</u>

ASA에 타사 공급업체 디지털 인증서를 설치하려면 다음 단계를 완료하십시오.

- 1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.
- <u>2단계. 인증서 서명 요청 생성</u>
- <u>3단계. 신뢰 지점 인증</u>
- <u>4단계. 인증서 설치</u>
- 5단계. 새로 설치된 인증서를 사용하도록 IPSec(Site-to-Site VPN)을 구성합니다.

1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.

ASDM 절차

- 1. Configuration(컨피그레이션)을 클릭한 다음 Device Setup(디바이스 설정)을 클릭합니다.
- 2. System Time(시스템 시간)을 확장하고 Clock(시계)을 선택합니다.
- 3. 나열된 정보가 정확한지 확인합니다.올바른 인증서 검증이 이루어지려면 날짜, 시간 및 표준 시간대 값이 정확해야 합니다

File View Tools Wizards Window H	elp
Home 🦓 Configuration 📴 Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🤗 Help
Device Setup are + ×	Configuration > Device Setup > System Time > Clock
Startup Wizard	Configure the ASA date and clock.
Device Name/Password	Time Zone: (GMT+05:30) Calcutta
	Date
	Apr 14, 2009
	Time: 14 : 50 : 27 hh:mm:ss (24-hour)
	Update Displayed Time
	Update Displayed Time

명령줄 예

ASA-1	
ASA-1# sn clock	
14:53:15.943 IST Tue Apr 14 2009	

<u>2단계. 인증서 서명 요청 생성</u>

서드파티 CA가 ID 인증서를 발급하려면 CSR(Certificate Signing Request)이 필요합니다.CSR에는 생성된 공개 키와 함께 ASA의 DN(Distinguished Name) 문자열이 포함됩니다.ASA는 생성된 개인 키를 사용하여 CSR에 디지털 서명을 합니다.

ASDM 절차

1. Configuration(구성) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동한 다음 Add(추가)를 클릭합니다

File View Tools Wizards Window	oring Save & Refresh & Back O Forward ? Help	End ·
Device Monogement	Configuration > Device Monogement > Certificate Monogement > Issued To Issued By Expiry Date Usage	Identity Certificates
Engling Engling Engline Engline Engline Certificate Management CA Certificates		Show Details Delete
B-∰ DHCP B-∰ DNS B-∰ Advanced		Export Install

2. Add a **new identity certificate** 라디오 버튼**을** 클릭합니다

Decryption Passphrase: File to Import From:			Browse	ſ
Add a new identity certi	ficate:			
Key Pair:	my.CA.key	•	Show	New
Certificate Subject DN:	CN=CiscoASA		Select	
	1			
Generate self-signer	d certificate ficate authority and issi	ue dynamic cer!	tificates to TLS	-Proxy
Generate self-signer 🕞 Generate self-signer	d certificate	Je dynamic cerl	tificates to TLS	-Proxy Advanced

Name:	🔿 Use default key	y pair name	
	Enter new key	pair name: my.CA	A.key
5ize:	1024	¥	
Jsage:	 General purpos 	e O Sp	ecial

- 4. Enter new key pair name(새 키 쌍 이름 입력) 라디오 버튼을 클릭합니다.인식 목적으로 키 쌍 이름을 명확하게 식별해야 합니다.
- 5. Generate Now(**지금 생성)를 클릭합니다**.이제 키 쌍을 만들어야 합니다.

.

6. 인증서 주체 DN을 정의하려면 Select(선택)를 클릭하고 이 표에 나열된 특성을 구성합니다

File to Import From:			
	1	Browse	
Add a new identity cert	ificate:		
Key Pair:	my.CA.key	Show	New
Certificate Subject DN:	CN=CiscoASA	Select)
🔲 Generate self-signe	d certificate		
F Act as local cert	ificate authority and issue dyr	namic certificates to TLS-I	Proxy
			Advanced.

		Attribute	Value
DN Attribute to be Added	l	Common Name(CN) Department (OU)	CiscoASA.cisco TSWEB
Attribute: Select Attribute 💌	Add>>	Company Name (O)	Cisco Systems
		Country (C)	US
Value:	Delete	State (St)	North Carolina
		Location (L)	Raleigh

참고: 일부 타사 공급업체는 ID 인증서를 발급하기 전에 특정 특성을 포함해야 합니다.필요한 특성을 잘 모르는 경우 공급업체에 자세한 내용을 확인하십시오.

- 7. 적절한 값을 추가한 후 **확인**을 클릭합니다.Add Identity Certificate 대화 상자가 나타나고 Certificate Subject DN 필드가 채워집니다.
- 8. Advanced(고급)를 **클릭합니다**

Desmustice Desert		Q		
Decryption Passphrase:	·			
File to Import From:	1		Browse,	
Add a new identity cert	ificate:			
Key Pair:	my.CA.key	•	Show	New
Certificate Subject DN:	CN=CiscoASA		Select	
		- 23		
Generate self-signe	d certificate			
Generate self-signe	d certificate	ue dynamic cer	tificates to TLS-	Proxy
Generate self-signe	d certificate	ue dynamic cer	tificates to TLS-	Proxy
Generate self-signe	d certificate	ue dynamic cer	tificates to TLS-	Proxy Advanced

CN(Common Name)에 사용한 FQDN과 같아야 합니다

Enrollment mode par	ns ameters and SCEP challenge password are not available for self-signed certificate
Certificate Parame	ters Enrollment Mode SCEP Challenge Password
EODN: Cisc	nASA.cisco.com
E-mail:	
IP Address:	
🔽 Include serial	number of the device
	OK Cancel Help
10. OK(확인)를 클릭한 CSR을 저장하라는	다음 Add Certificate(인증서 추가)를 클릭합니다 .로컬 시스템의 파일에 메시지가 표시됩니다
🚮 Identity Cert	ificate Request 🔀
To complete th request (CSR)	e enrollment process, please save the PKCS10 enrollment and send it to the CA.
You will then no clicking the Ins	ed to install the certificate that is returned from the CA by all button in the Identity Certificates panel.
Save CSR to fil	e: c:/cert_client.txt Browse
	OK Cancel Help

11. Browse(**찾아보기**)를 클릭하고 CSR을 저장할 위치를 선택하고 확장자가 .txt인 파일을 저장 합니다.**참고:** .txt 확장자로 파일을 저장하면 텍스트 편집기(예: 메모장)로 파일을 열고 PKCS#10 요청을 볼 수 있습니다

<u>File E</u> dit	F <u>o</u> rmat	Help							
MIICKZ IENhcm MCIGA1 TVgwOT Bgkqhk XgKoH2 XgKoH2 MI6XLY QX8JP6 A1UdEQ 3tZYAD bsxSv1 j89/Y4 End	CCAZQC) 9saW5hM UEAXMb(M1SZA1) iG9w0B) PcelcG2 KrGo7b(qcZE0C) qcZE0C) qcZE0C) qcZE0C) qcZE0C) gsSX0S(58XhQ7) - Thi:	AQAwga(MQswCQ) Q21zY29 NDAfBgl AQEFAA(Z9dUXn- DPASLP(AWEAAa) EkNpc21 j9EW7E Q1Sb84 9fvBWbf s line	DXEDAOB (DVQQGB BUOEu (qhkiG DBjQAw PY09Qjr 20Bx1/L 9MDSG VVQVNBL 14BfcX 2D6MEG 8UX9er NOT pa	BGNVBA EWJVUZ 721ZY2 DWOBCC GYKCGY nOKrj6 LVLTY3 ISqGSI LMNPC2 d20LCb 5cU7BX nhFHPG art of	CTB1J EWMBQ(8uY291 IWEKN EAUOII 8L6KX ORQCY b3DQE NVLMN XAOP5I J/K1Z HNQ/M HNQ/M	hbGVp: SA1UE TIE9VI C2NV (QDMj 71PgN, 72QP3 70JEU 70DJEU 7	Z2gxFz ChMNQ2 PVRTV0 QVNBLm VrdbZg AaFMwB Ir1BSw MCwwCW Bgkqhk aEeaCk UVCHr0 dQ== ficate	AVBGN 12Y280 VCMTUN Npc2N BZUAj1 2YSTIC OyBaOF YDVROF iG9w0E fN/Pp PYWVU PYWVU	/BAGTI gU31zc vEGYDV /LMNVI FC10j: Dn+hJE FPSRE: PBAQD/ BAQQF/ BAQQF/ SMATAS LWGRJC
어장된 CS 아격 증명	····································	osoft CA 받아 CA	와 같은 티 서버 172	사 공급 16.5.1℃	업체에 지 네 웹 로그	해출합니 1인을 イ	│다.VPN ≥행합니□	서버에 7 나	제공된/
File Ed	lit View	Favorite	es Tools	Help					
A Pole	$\cdot \rightarrow \cdot$	8	3 Q	Search	🗼 Favo	orites	Media	3	
Man Dark							1.117	and the second	214

)	Please type y	our user name and	d password.		
	Site:	172.16.5.1			
	User Name	vpnuser			
L	Password	******			
	Domain				
	🔲 Save this	password in your	password list		
			OK	Ca	incel

버와 함께 ASA(VPN 서버)에 대한 사용자 계정이 있는지 확인하십시오.Request a certificate(인증서 요청) > advanced certificate request(고급 인증서 요청)를 클릭하여 Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file(base-64 인 코딩 CMC 또는 PKCS#10 파일을 사용하여 인증서 요청 제출)을 선택하거나 base-64 인코딩 PKCS#7 파일을 사용하여 갱신 요청을 제출합니다

Address 🛃 http://172.16.5.1/certsrv/certrqad.asp

Microsoft Certificate Services - CA1

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file,

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

인코딩된 정보를 복사하여 Saved **Request** 상자에 붙여넣은 다음 Submit(제출)을 **클릭합니** 다

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded (source (such as a Web server) in the Saved Request box.

Saved Request:

l l	VQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAO
Base-64-encoded	4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8
certificate request	D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+
(CMC or	8Ux9emhFHpGHnQ/MpSfUOdQ==
PKCS #10 or	
PKCS #7):	not part of the certificate request 🌾
54 C	

Browse for a file to insert.

Certificate Template:

IPSEC	•
IPSEC	

Additional Attributes:

Attributes:	
	Submit >

64 인코딩 라디오 버튼을 클릭하고 인증서 다운로드를 클릭합니다

@Go Lin

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

Download certificate Download certificate chain · anjin 파일 다운로드 창 이 나타납니다.cert_client_id.cer 이름으로 저장합니다. ASA에 설치할 ID 인증서입니다 File Download X Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file. File name: certnew.cer File type: Security Certificate 172.16.5.1 From: 1 This type of file could harm your computer if it contains malicious code. Would you like to open the file or save it to your computer? Save Cancel Open More Info Always ask before opening this type of file

명령줄 예



trustpoint)#keypair my.CA.key
crusepoint/# Reypair my.cr.Rey
I Specifies key pair generated in Step 3 ASA-
1(config-ca-trustpoint)# fadn CiscolS1 cisco com
$I_{}$ Specifies the FODN (DNS:) to be used as the subject
alternative name ASA-1(config-ca-trustpoint) #enrollment
terminal
I Specifies manual enrollment ASA-1(config-ca-
trustpoint)# exit
ASA-1(config)# crypto ca enroll CA1
I Initiates certificate signing request This is the
request to be ! submitted via Web or Email to the
third party wonder & Start gertificate enrollment
The subject neme in the certificate will be:
The subject name in the certificate will be.
CHECISCOASA.CISCO.COM OUEISWEB, UECISCO Systems,
demoin news in the neutrificate will be
domain name in the certificate will be:
CiscoASA.cisco.com % include the device serial number in
the subject name? [yes/no]: no
<i>! Do not include the device's serial number in the</i>
<i>subject</i> . Display Certificate Request to terminal?
[yes/no]: y
! Displays the PKCS#10 enrollment request to the
terminal. You will need to ! copy this from the
terminal to a text file or web text field to submit to
<i>! the third party CA</i> . Certificate Request follows:
MIICKzCCAZQCAQAwga0xEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEk
MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOn+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBx1/LVLTy3ORqcyy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJDjEuMCwwCwYDVR0PBAQD
AgWqMB0G
A1UdEOOWMBSCEkNpc2NvQVNBLmNpc2NvLmNvbTANBqkqhkiG9w0BAOOF
AAOBqOBM
JtzvAD7o6R5ei9EW7Ei4BfcXd20LCbXAoP5LlKbPaEeaCkfN/Pp5mATA
sG832TBm
bsxSvljSSXOsOlSb842D6MEG6cu7Bxj/Kl76MxafUvCHrOPYWVU1waRJ
Gh+ndCZK $i89/Y4S8XhO79fvBWbR8IIx9emhFHpGHnO/MpSfII0dO==$
-End - This line not part of the certificate request
Redisplay enrollment request? [ves/nol: n
$\Lambda S_{\lambda-1}(aonfig) $ #
APA-1(CONTIG)#

<u>3단계. 신뢰 지점 인증</u>

서드파티 벤더로부터 ID 인증서를 받은 후에는 이 단계를 진행할 수 있습니다.

ASDM 절차

1. 로컬 컴퓨터에 ID 인증서를 저장합니다.

- 2. 기본 64로 인코딩된 인증서가 파일로 제공되지 않은 경우 base 64 메시지를 복사하여 텍스트 파일에 붙여넣어야 합니다.
- 3. 확장명이 .cer인 파일 이름을 바꿉니다.참고: 파일 이름이 .cer 확장명으로 변경되면 파일 아이



타사 공급업체 또는 CA 관리자에게 문의하십시오.

- 5. Certificate Path 탭을 클릭합니다.
- 6. 발급된 ID 인증서와 연결된 CA 인증서를 클릭하고 View Certificate(인증서 보기)를 클릭합니

참고: Windows에 메시

Certificate	? >
General Details Certification Path	
┌ Certification path	
CA1	EB
	View Certificate
Certificate <u>s</u> tatus:	
This certificate is OK.	
자세하 정보가 나타난니다	

7. ID 인증서에 대한 자세한 내용을 보려면 Details를 클릭합니다

Version V3 Serial number 611E E59B 0000 0000 0007 Signature algorithm sha1RSA Issuer CA1, TSWeb, cisco, com Valid from Saturday, December 15, 2007 Valid to Monday, December 14, 2009	
Serial number 611E E59B 0000 0000 0007 Signature algorithm sha1RSA Issuer CA1, TSWeb, cisco, com Valid from Saturday, December 15, 2007 Valid to Monday, December 14, 2009	
Signature algorithm SharkSA Issuer CA1, TSWeb, cisco, com Valid from Saturday, December 15, 2007 Valid to Monday, December 14, 2009	1.1
Valid from Saturday, December 15, 2007	
Valid from Saturday, December 13, 2007	
	1
Subject CiscoASA.cisco.com OU=TSW	
Public key RSA (1024 Bits)	-

8. ID 인증서를 설치하기 전에 CA 서버에서 CA 인증서를 다운로드하여 ASA에 설치해야 합니다 (그림 참조).**CA1**이라는 CA 서버에서 CA 인증서를 다운로드하려면 다음 단계를 **완료합니다** .VPN 서버에 제공된 자격 증명의 도움을 받아 CA 서버 172.16.5.1에 웹 로그인을 수행합니다

Eile	Edit	⊻ie	w F	avorites	Tools	<u>H</u> elp			
G Ba	ack 👻	Θ	- 💌	2	<u>م ا</u> (Search	☆ Favorites	0	1

1918	
Connecting to 17	2.16.5.1
<u>U</u> ser name:	🖸 vpnserver
Password:	•••••
	Remember my password

.

certificate, certificate chain or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)을 클릭하여 창을 엽니다(그림 참조).인코딩 방법으로 Base 64 라디오 버튼을 클릭하고 CA 인증서 다운로 드를 클릭합니다

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA cert

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:

Current	[CA1]
ļ	

Encoding method:

9.

ODER
• Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRI
Download latest delta CRI
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.64 KB
From: 172.16.5.1
Upen Save Cancel
Ave. Ave. And a first the between the second data for the second
potentially harm your computer. If you do not trust the source, do not
open or save this software. <u>What's the risk?</u>
CA 인증서를 저장한 위치를 찾습니다. - 레코자리 가유 테스트 퍼지리그 코이유 어니티 코이유 라우스 우르퍼 내트우

10. 메모장과 같은 텍스트 편집기로 파일을 엽니다.파일을 마우스 오른쪽 버튼으로 클릭하고 Send To(보내기) > Notepad(메모장)를 선택합니다.

11. 이 이미지의 인증서와 유사한 기본 64로 인코딩된 메시지가 나타납니다

🌌 certnew.cer - Notepad

File Edit Format Help

----BEGIN CERTIFICATE----

MIIEnTCCA4wgAwIBAgIQcJnxmUdk4JxGUdqAowt0nDANBgkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT Bqojkiajk/IszAEZFqVUU1dlyjEMMAoGA1UEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 M1oxDTEyMTIxNDA2MTAxNVowUTETMBEGCqmSJomT8ixkARkWA2NvbTEVMBMGCqmS JOMT8ixkARkWBWNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuVvyiLmA9 BSGZMz3sCtR9TCMw0x7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMijcQnwdOq+ Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4db0I y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2V uBwCsptW7c1akTqfm5×K/d//z2eUu×rHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDh×x wPXR018CAwEAAaoCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ pAP1wDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWM]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJ2aWN]cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD PWNvbT9jZXJ0aWZpYŹF0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 Y1JMRGlzdHJpYnV0aw9uUG9pbnSGNwh0dHA6Ly90cy13MmszLwFjcy50c3dlYi5j aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHqHUCD9/BZWAqfmGUm++HMljnW8liyIF DCNwxlqxsDT+n9Y0k6bnG6u0f4SgETNrN8EyYVrSGK0lE+0C5L+ytJvw19GZhlzE lovufpa+pt47dmar6uo2v2zbw5kGavLu8GsrFd8wZbpBvMkCqFwNcNItcufu0x1b 1xxc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1vD+p85at ----END CERTIFICATE----

- 12. ASDM에서 Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
- 13. Certificate Management(인증서 관리)를 확장하고 CA Certificates(CA 인증서)를 선택합니다.
- 14. Add(추가)를 클릭합니다.
- 15. Paste certificate in **PEM Format(PEM 형식으로 인증서 붙여넣기**) 라디오 버튼을 클릭하고 서드파티 벤더가 제공한 기본 64 CA 인증서를 텍스트 필드에 붙여넣습니다.
- 16. Install Certificate를 클릭합니다

Paste certificate in PEM for	rmat:
PVRTLVcySzMtQUNTLENOF Tj1TZXJ2aWNlcyxDTj1Db2 PWNvbT9jZXJ0aWZpY2F02 Y1JMRGlzdHJpYnV0aW9uL aXNjby5jb20vQ2VydEVucn CSqGSIb3DQEBBQUAA4IB L6Z86JGW1Rbf5VYnlTrqRy DcNwxlQxsDT+n9YOk6bn(IOVUfPA+PT47dmAR6Uo2 1XXc68DKoZY09pPq877uT	PUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD 25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD 2VJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 JG9pbn5GNWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j m9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G)AQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr y6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMljnW8liyIF G6uOf4SgETNrN8EyYVr5GKOIE+OC5L+ytJvw19GZhlzE V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNItcufu0xlb 'aou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE	-
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE	
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE Use SCEP:	
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE Use SCEP: SCEP URL: http://	
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE Use SCEP: SCEP URL: http:// Retry Period: 1	-
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE Use SCEP: SCEP URL: http:// Retry Period: Retry Count: 0	-
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE Use SCEP: SCEP URL: http:// Retry Period: 1 Retry Count: 0	-
9Ms7ABAu+pRIoi/EfjQgMS END CERTIFICATE ■ Use SCEP: SCEP URL: http:// Retry Period: Retry Count: 0	minutes Use 0 to indicate unlimited retri More Options

명령줄 예

ASA-1
ASA-1(config)#crypto ca authenticate CA1
! Initiates the prompt for paste-in of base64 CA
intermediate certificate. ! This should be provided by
the third party vendor. Enter the base 64 encoded CA
certificate. End with the word "quit" on a line by
itselfBEGIN CERTIFICATE
$\tt MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B$
AQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK

BgNVBAMT
${\tt A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu}$
VvyiLmA9
BSGzMz3sCtR9TCMW0x7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4db0I
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwgYBXWKh4uC04xxQmr//Sct1t
dWOcvk2V
uBwCsptW7C1akTgfm5XK/d//z2eUuXrHYvS0CfoFvk1vE6/0lo+f0eSS
z+TlDhXx
wPXR018CAwEAAaOCAW8wggFrMBMGCSsGAOOBgicUAgOGHgOAOwBBMAsG
A1UdDwOE
AWIBD APBGNVHRMBAf8EBTADAOH/MB0GA1UdDgOWBBTZrb818ig18RRD
L3mYfNOJ
DAP1WDCCAOMGA1UdHwSB+zCB+DCB9aCB8gCB74aBtWxkYXA6Lv8v0049
00ExLENO
PVRTLVcvSzMtOUNTLENOPUNEUCxDTi10dWJsaWM1MiBLZXk1MiBTZXJ2
aWNlcvxD
Ti1TZXJ2aWN1cvxDTi1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYn1TrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlj
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
19GZhlzE
10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
END CERTIFICATE
quit
Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
<pre>% Certificate successfully imported</pre>
ASA-1(config)#

<u>4단계. 인증서 설치</u>

ASDM 절차

다음 단계를 완료하려면 서드파티 벤더가 제공한 ID 인증서를 사용하십시오.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
- 2. Certificate Management(인증서 관리)를 확장한 다음 Identity Certificates(ID 인증서)를 선택합

니다.

- 3. <u>2단계</u>에서 생성한 ID 인증서를 <u>선택합니다</u>.참고: 만료 날짜가 보류 *중으로 표시됩니다*.
- 4. Install(**설치)을 클릭합니다**

155060 10	Issued By	Expiry Date	Usage	
A.cisco.com OU=TS	[Not Available]	Pending	Unknown	
💼 Install Identity	y certificate		×	
Identity Certificate	·			
C Install from a	a file:	Brows	0	C
Paste the ce	rtificate data in base-64 form	nat:		-
VZZEM7368 NSLsYWqjkC	ECUSEMedFb+KYpAFy3PPy41 Bg+aUO+WPFk4jICr23UOK 9up2PEH2L/O34wm/dpuLuHi	8EHe4MJbdjUpjb9USI6J2QPSI51YBUy 74oWTPFNpfv2x4VFI/Mpcs87ychngKB+8 rnvWnF1zCnqfcyHcETie2tSt1nwLpsc	×	

Paste the certificate data in base-64 format 라디오 버튼을 클릭하고 서드파티 벤더가 제공한 ID 인증서를 텍스트 필드에 붙여넣습니다.

	informat	ion	×
	i	Certificate import succeeded.	
		ОК	
5. Install Certificate 클릭입니다.			가셔오
기가 성공했는지 확인하는 대화	상자가 나타닙	[니다.	

명령줄 예

ASA-1
ASA-1(config)#crypto ca import CA1 certificate
! Initiates prompt to paste the base64 identity !
certificate provided by the third party vendor. %The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself ! Paste the base 64 certificate provided by
the third party vendorBEGIN CERTIFICATE
MIIFpzCCBI+gAwIBAgIKYR71mwAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoXDTA5
$\tt MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRointer the the state of $
IENhcm9s

aW5hMRAwDgYDVQQHEwdSYWx1aWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0
ZW1zMSQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZIhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxq0
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDg0WBB0sJC3bS0zeGv4tY+MeH7KM10xCFiAf
Banvhsme
GDAWgBTZrb818ig18RRDL3mYfNOJpAP1WDCCAOMGA1UdHwSB+zCB+DCB
9aCB8aCB
Tindwie
LERDPVRTVZVILERDPWNDCZNVLERDPWNVDT9JZXJUAWZDIZFUZVJIAM9J
IXRD25M
axN0P2Jnc20/b2Jq2wN0Q2xnc3M9Y1JMRG1ZdHJpYnV0aw9u0G9pbnSG
LY90CY13MmszLWFJCY50C3d1Y15JaXNJbY5Jb20VQ2VydEVuCm9sbC9D
QTEUY3JS
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
O18vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZm1jYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1d1Yi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
${\tt zRq4dxAL111JkIjhfeQY+7VSkZ1GEpuBnENTohdhthz5vBjG1cROXIs8}$
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc
1L5nuPsd8MaexBc=
END CERTIFICATE
quit
INFO: Certificate successfully imported
ASA-1(config)#

5단계. 새로 설치된 인증서를 사용하도록 IPSec(Site-to-Site VPN)을 구성합니다.

VPN 터널을 생성하려면 다음 절차를 완료합니다.

.

- 1. 브라우저를 열고 ASDM Access용으로 구성된 ASA 인터페이스의 https://<IP_Address>를 입 력하여 ASA의 ASDM에 액세스합니다.
- 2. ASDM 애플리케이션 **설치** 프로그램을 다운로드하려면 **Download ASDM Launcher and Start ASDM(ASDM 시작** 시작 **시**작)을 클릭합니다.
- 3. ASDM Launcher가 다운로드되면, 소프트웨어를 설치하고 Cisco ASDM Launcher를 실행하기 위해 프롬프트에 의해 지시된 단계를 완료합니다.
- 4. http 명령으로 구성한 인터페이스의 IP 주소와 사용자 이름 및 비밀번호를 입력합니다(지정 된 경우).
- 5. ASDM 애플리케이션이 ASA에 연결되면 IPsec VPN **마법사**를 실행합니다

File	View	Tools	Wizard	ds Window	Help	inga nga ng					
Ci) Home	og Con	St	artup Wizard	l		9.99		3	Back 🚫 For	ward 🤶 Help
Ho	ome			sec VPN Wiza	ard						
/	🔡 Dev	rice Dasht	SS	SL VPN Wizar	d						
	Device : Genera	Informat	Pa	gh Availability acket Captur	and S Wizar	calabili d	ity Wizar	d			
	Host	Name:	ASA-	1.default.do	main.in	valid					
	ASA '	Version:	8.0(2))			C	evice Upt	ime:	7d 23h 40m	65
	ASDN	1 Version:	6.0(2))			C	evice Typ	e:	ASA 5510	
	Firew	all Mode:	Route	ed			C	Context Mo	ode:	Single	
	Total	Flash:	64 MB	}			Т	otal Mem	ory:	256 MB	
	/PN Tur	nnels									
	IKE: 0			IPsec: 0		(Clientless	SSL VPN	: 0		SSL VPN Client: 0
	auctom	Docours	oe Sta	ture							

6. Site-to-Site IPSec VPN 터널 유형을 선택하고 표시된 대로 Next(다음)를 클릭합니다

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Branch	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
	Site-to-Site
	Remote Access Remote Access
6	VPN Tunnel Interface: outside 🗸
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help
 원격 피어의 외부 IP 주	

7. 원격 피어의 외부 IP 주소를 지정합니다.이 예에서 사전 공유 키인 사용할 인증 정보를 입력합 니다.이 예에서 사용되는 사전 공유 키는 cisco123입니다. L2L VPN을 구성하는 경우 기본적 으로 터널 그룹 이름은 외부 IP 주소입니다.Next(다음)를 클릭합니다

🖆 VPN Wizard		X
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Branch Branch Branch Hama Corporate Network	Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 172.17.1.1 Authentication Method Pre-shared key Pre-Shared Key: © Certificate Certificate Signing Algorithm: rsa-sig Certificate Name CA1 Challenge/response authentication (CRACK)	
	Tunnel Group For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity. Tunnel Group Name: 172.17.1.1	
	Sack Next > Finish Cancel Help	

8. 1단계라고도 하는 IKE에 사용할 특성을 지정합니다. 이러한 특성은 ASA와 IOS 라우터 모두에 서 동일해야 합니다.Next(**다음)를 클릭합니다**

•

🕵 VPN Wizard				×
VPN Wizard	IKE Policy	(Step 3 of 6)		
Branch Frankh Frankh Horne	Select t group fi security connect	he encryption algori or the devices to use association betwee ion must match exa	thm, authentication algorithm, and Diffie-Hellman e to negotiate an Internet Key Exchange (IKE) n them. Configurations on both sides of the ctly.	
Corporato Network		Encryption: Authentication:	3DES 🖌	
		DH Group:	2	
			< Back Next > Finish Cancel He	þ

9. 2단계라고도 하는 IPSec에 사용할 특성을 지정합니다. 이러한 특성은 ASA와 IOS 라우터 모 두에서 일치해야 합니다.Next(**다음)를 클릭합니다**

🖆 VPN Wizard		3
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)	
PPN WIZZERO	IPsec Encryption and Authentication (Step 4 of 6) Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly. Encryption: Image: Configuration content is a content of the connection must match exactly. Authentication: Image: Configuration content of the connection must match exactly.	
	< Back Next > Finish Cancel Help	

10. VPN 터널을 통과하도록 트래픽을 허용해야 하는 호스트를 지정합니다.이 단계에서는 VPN 터널에 **로컬** 및 **원격 네트워크**를 제공해야 합니다.여기 표시된 대로 Local Networks(로컬 네 트워크) 옆의 버튼을 클릭하여 드롭다운 목록에서 로컬 네트워크 주소를 선택합니다

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks ((Step 5 of 6)
Branch Branch ISP	An IPsec tunnel protects remote sites. Please ider	entify hosts and networks to be used in the IPsec tunnel.
Home	HOUDIL (
	Local Networks: a	any
Network	Remote Networks: a	any 💮
	✓ Exempt ASA side ho	nost/network from address translation:
		< Back Next > Finish Cancel Help

11. 로컬 **네트워크** 주소를 선택한 다음 **OK**(확인)를 클릭합니다

🖆 Browse Local Netwo	orks			×
🗣 Add 👻 🌠 Edit 🏛	Delete 0			
	beece 4			Ethan I change
Filter:				Filter Clear
Name ^	1 IP Address	Netmask	Description	
Network Objects				
- 🌑 any	0.0.0.0	0.0.0		
🚽 🚮 dmz-network	10.77.241.64	255.255.255.192		
🚽 🚅 inside-network	10.10.10.0	255.255.255.0		
····· 🚮 outside-network	k 172.16.1.0	255.255.255.0		
Selected Local Networks -				
Local Networks ->	any			
				Cancel
		시 큰 시 태 된 기 더 ㅠ /		

12. 드롭다운 목록에서 원격 네트워크 주소를 선택하려면 표시된 대로 Remote Networks(원격 네트워크) 옆에 있는 버튼을 클릭합니다

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Brench Brench	An IPsec tunnel protect remote sites. Please ide	s data exchanged by selected hosts and networks at the local and ntify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Horne	Local Networks:	inside-network/24
Corporativ	Remote Networks:	any
	Evernt ASA side b	oct (network from address translation:
	Compensation and the	
		< Back Next > Finish Cancel Help

13. **원격 네트워크** 주소를 선택한 다음 **확인**을 클릭합니다.**참고:** 목록에 원격 네트워크가 없으면 네트워크를 목록에 추가해야 합니다.Add를 **클릭합니다**

🖆 Browse Remote Net	works			×
🗣 Add 🝷 🗹 Edit 📋	Delete 🔍			
Filter:				Filter Clear
Name ^	1 IP Address	Netmask	Description	
Network Objects				
	0.0.0.0	0.0.0.0		
📑 dmz-network	10.77.241.64	255.255.255.192		
- 🚮 inside-network	10.10.10.0	255.255.255.0		
📑 🚮 outside-networ	k 172.16.1.0	255.255.255.0		
i- 🛃 10.20.10.0	10.20.10.0	255.255.255.0		
Remote Networks ->	any			
			L CK	Cancel

14. Exempt ASA side host/network from address translation(ASA 측 호스트/네트워크에서 주소 변환 제외) 확인란을 선택하여 터널 트래픽이 Network Address Translation(네트워크 주소 변환)을 받지 않도록 합니다.Next(다음)를 클릭합니다

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protec remote sites. Please id	ts data exchanged by selected hosts and networks at the local and lentify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks:	inside-network/24
Network	Remote Networks:	10.20.10.0/24
	▼ Exempt ASA side	host/network from address translation:
		Rack Next > Finish Cased Hale
		Cancel Hep

15. VPN 마법사에서 정의한 특성이 이 요약에 표시됩니다.구성이 올바른지 확인한 후 Finish(마 침)를 클릭합니다

🖆 VPN Wizard		×
VPN Wizard	Summary (Step 6 of 6)	
Branch Branch Branch Branch Hanne Comportate Notwork	You have created a Site-to-Site VPN tunnel with the following attributes: VPN Tunnel Interface: outside Peer IP Address: 172.17.1.1 IPSsec authentication uses certificate:CA1 Tunnel Group Name: 172.17.1.1 IKE Policy Encryption / Authentication / DHGroup: 3DES / SHA / Group 2 IPsec ESP Encryption / ESP Authentication: 3DES / SHA Traffic flow to be protected by this tunnel: (local) 10.10.10.0/24 (remote) 10.20.10.0/24	
	< Back Next > Finish Cancel Hel	p

<u>ASA-1 컨피그레이션 요약</u>

ASA-1	

```
ASA-1#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ASA-1
domain-name cisco.comenable password 8Ry2YjIyt7RRXU24
encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 192.168.1.5 255.255.255.0!
interface Ethernet0/1
nameif inside
security-level 100
ip address 10.2.2.1 255.255.255.0!
interface Ethernet0/2
nameif DMZ
security-level 50
ip address 10.77.241.142 255.255.255.192
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
encryptedftp mode passive dns server-group DefaultDNS
domain-name cisco.com access-list inside_nat0_outbound
extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0
255.255.255.0 access-list outside_1_cryptomap extended
```

permit ip 10.2.2.0 255.255.255.0 10.5.5.0 255.255.255.0 pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.2.2.0 255.255.255.0 nat (inside) 0 access-list inside_nat0_outbound route outside 0.0.0.0 0.0.0.0 192.168.1.3 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact ! crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto map outside_map 1 match address outside_1_cryptomap crypto map outside_map 1 set peer 172.17.1.1 crypto map outside_map 1 set transform-set ESP-3DES-SHA crypto map outside_map interface outside ! crypto ca trustpoint CA1 enrollment terminal subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems, C=US, St=North Carolina,L=Rale serialnumber keypair my.CA.key crl configure crypto ca certificate chain CA1 certificate 611ee59b000000000007 308205a7 3082048f a0030201 02020a61 lee59b00 00000000 07300d06 092a8648 86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31 15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689 93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 le170d30 37313231 35303833 3533395a 170d3039 31323134 30383335 33395a30 76310b30 09060355 04061302 55533117 30150603 55040813 0e4e6f72 74682043 61726f6c 696e6131 10300e06 03550407 13075261 6c656967 68311630 14060355 040a130d 43697363 6f205379 7374656d 73312430 22060355 0403131b 43697363 6f415341 2e636973 636f2e63 6f6d204f 553d5453 57454230 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 b8e20aa8 332356b7 5b660073 5008d373 5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754 5e7f98d3 d4239b42 ab8faf0b e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a b94b18ef 308eb12f 22ab1a8e db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9 03f722bd 414b0a32 05aa053e c45e2464 80606f8e 417f09a7 aa9c644d 02030100 01a38202 de308202 da300b06 03551d0f 04040302 05a0301d 0603551d 11041630 14821243 6973636f 4153412e 63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cdela fe2d63e3 le1fb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f 79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081 ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143 532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 25323053 65727669 6365732c 434e3d53 65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e 2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966 69636174 65526576 6f636174 696f6e4c 6973743f 62617365 3f6f626a 65637443 6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 74863568 7474703a 2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 01050507 01010482 010f3082 010b3081 a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e 3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143 65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274 69666963 6174696f 6e417574 686f7269

7479305d	06082b06	01050507	30028651	68747470	3a2f2f74
732d7732	6b332d61	63732e74	73776562	2e636973	636f2e63
6f6d2f43	65727445	6e726f6c	6c2f5453	2d57324b	332d4143
532e5453	5765622e	63697363	6f2e636f	6d5f4341	312e6372
74302106	092b0601	04018237	14020414	1e120057	00650062
00530065	00720076	00650072	300c0603	551d1301	01ff0402
30003013	0603551d	25040c30	0a06082b	06010505	07030130
0d06092a	864886f7	0d010105	05000382	0101008a	82680£46
fbc87edc	84bc45f5	401b3716	0045515c	2c81971d	0da51fe3
96870627	b41b4319	23284b30	5eafcedb	10c1ef05	d0686a61
cd1ab877	100b965d	499088e1	7de418fb	b5529199	46129b81
9c4353a2	1761b61c	f9bc18c6	95c44e5c	8b3cfb71	a183c872
61964433	bddef040	b4b0431e	7456fe29	8a40172d	cf3f2e25
f041dee0	c25b7635	29fdbf74	97997a23	340fe65e	75601d32
3522ec61	6aa39020	60f9a50e	£963c593	88c80abd	9750e2bb
e285933c	53697efd	ble15148	fcca5cb3	cef27219	e0281fbc
acf1c285	2b19b30f	6ea733c4	lf62ff3b	7e309bf7	69b8bb87
8abaf05a	7175cc29	ea7dcc87	7044e279	9b52b759	f02e9b1c
94be67b8	fb1df0c6	9ec417 qu	uit certif	Eicate ca	
7099f1994	4764e09c46	551da80a16	5b749c 308	32049d 308	320385
a0030201	02021070	99£19947	64e09c46	51da80a1	6b749c30
0d06092a	864886£7	0d010105	05003051	31133011	060a0992
268993£2	2c640119	1603636f	6d311530	13060a09	92268993
£22c6401	19160563	6973636f	31153013	060a0992	268993£2
2c640119	16055453	57656231	0c300a06	03550403	13034341
31301e17	0d303731	32313430	36303134	335a170d	31323132
31343036	31303135	5a305131	13301106	0a099226	8993£22c
64011916	03636±6d	31153013	060a0992	268993±2	2c640119
16056369	73636±31	15301306	0a099226	8993122c	64011916
05545357	6562310c	300a0603	55040313	03434131	30820122
300d0609	2a864886	±70d0101	01050003	82010±00	3082010a
02820101	00ea8iee	c/ae56fc	a22e603d	05216333	3dec0ad4
7d4c2316	3bleea33	C9a6883d	28ece906	0290219a	dleb2b8d
1588CD9a	/8a069a3	965de133	6036a8a7	bedeyccd	aleyubec
88D32a19	38653536	6CUU32e8	8CUU3IA6	21022a40	bydda2c2
5ICDD621	8/6006/8	C8a3/109	10/4eabe	2011aC59	a/8d0a3D
35all/ae	08/44805	3D9a34e7	24D9e054	063C60a4	90803009
551DC030	03169357	1455209197	10/5D400	CD/14014	09411331
20071426	00409443	14550210		ayous/so	$a_{878D820}$
50C/1420	alliuz/z	duou/504	10De4095	62240000	9D56ec2d
5d915d91	9D95Calu		94D97aC7	05249009	Ef020201
0001-3282	016f3082	01663013	060022006	01040182	37140204
061_0400	43004130	01003013	1d0f0404	01010102	300f0603
55121301	13004130 01ff0405	30030101	ff301d06	03551202	04160414
d9adbf08	f23a88f1	14432f79	987cd409	a403e558	30820103
0603551d	1f0481fb	3081f830	81f5a081	f2a081ef	8681b56c
6461703a	2f2f2f43	4e3d4341	312c434e	3d54532d	57324b33
2d414353	2c434e3d	4344502c	434e3d50	75626c69	63253230
4b657925	32305365	72766963	65732c43	4e3d5365	72766963
65732c43	4e3d436f	6e666967	75726174	696f6e2c	44433d54
53576562	2c44433d	63697363	6f2c4443	3d636f6d	3£636572
74696669	63617465	5265766f	63617469	6f6e4c69	73743£62
6173653f	6f626a65	6374436c	6173733d	63524c44	69737472
69627574	696f6e50	6f696e74	86356874	74703a2f	2f74732d
77326b33	2d616373	2e747377	65622e63	6973636f	2e636f6d
2f436572	74456e72	6f6c6c2f	4341312e	63726c30	1006092b
06010401	82371501	04030201	00300d06	092a8648	86f70d01
01050500	03820101	001abc5a	40b32112	22da80fb	bb228bfe
4bf8a515	df8fc3a0	4e0c89c6	d725e2ab	2fa67ce8	9196d516
dfe55627	953aea47	2e871289	6b754e9c	1e01d408	3f7f0595
8081f986	526fbelc	c9639d6f	258b2205	0dc370c6	5431b034
fe9fd60e	93a6e71b	ab8e7f84	a011336b	37c13261	5ad218a3
a513e382	e4bfb2b4	9bf0d7d1	99865cc4	94e5547c	f03e3d3e

3b766011 e94a3657 6cc35b92 860152d4 f06b2b15 df306433		
c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196		
34f693ea f3beee4d aa2ef1c2 edba288f 3a678ecb 3809d0df		
b1699c76 13018f9f 5e3dce95 efe6da93 f4cb3b00 102efa94		
48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad		
quit ! crypto isakmp enable outside crypto isakmp policy		
10 authentication rsa-sig encryption 3des hash sha group		
1 lifetime 86400 telnet timeout 5 ssh timeout 5 console		
timeout 0 threat-detection basic-threat threat-detection		
statistics access-list ! class-map inspection_default		
match default-inspection-traffic ! ! Output		
<i>suppressed!</i> tunnel-group 172.17.1.1 type ipsec-121		
tunnel-group 172.17.1.1 ipsec-attributes trust-point CA1		
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end		

<u>ASA-2 컨피그레이션</u>

ASA-2 보안 어플라이언스에 대해 유사한 <u>구성</u>을 따릅니다.

<u>다음을 확인합니다.</u>

ASA에서는 인증서의 상태를 확인하기 위해 명령줄에서 여러 show 명령을 실행할 수 있습니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

```
• show crypto ca trustpoint 명령은 구성된 신뢰 지점을 표시합니다.
 ASA-1#show crypto ca trustpoints
 Trustpoint CA1:
     Subject Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
           Serial Number: 7099f1994764e09c4651da80a16b749c
     Certificate configured.
• show crypto ca certificate 명령은 시스템에 설치된 모든 인증서를 표시합니다.
 ASA-1# show crypto ca certificate
 Certificate
   Status: Available
   Certificate Serial Number: 3f14b70b0000000001f
   Certificate Usage: Encryption
   Public Key Type: RSA (1024 bits)
   Issuer Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   Subject Name:
     cn=vpnserver
     cn=Users
     dc=TSWeb
     dc=cisco
     dc=com
   PrincipalName: vpnserver@TSWeb.cisco.com
   CRL Distribution Points:
     [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
     CN=Services, CN=Configuration, DC=TSWeb, DC=cisco,
     DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
   Validity Date:
     start date: 14:00:36 IST Apr 14 2009
     end date: 14:00:36 IST Apr 15 2010
   Associated Trustpoints: CA1
 CA Certificate
   Status: Available
   Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
   Certificate Usage: Signature
   Public Key Type: RSA (2048 bits)
   Issuer Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   Subject Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   CRL Distribution Points:
     [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
     CN=Services, CN=Configuration, DC=TSWeb, DC=cisco,
     DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
     [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
   Validity Date:
     start date: 06:01:43 IST Apr 14 2009
     end date: 06:10:15 IST Apr 14 2014
   Associated Trustpoints: CA1
 Certificate
   Subject Name:
     Name: CiscoASA.cisco.com
   Status: Pending terminal enrollment
   Key Usage: General Purpose
   Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
   Associated Trustpoint: CA1
• show crypto ca cris 명령은 캐시된 CRL(certificate revocation list)을 표시합니다.
• show crypto key mypubkey rsa 명령은 생성된 모든 암호화 키 쌍을 표시합니다.
 ASA-1# show crypto key mypubkey rsa
 Key pair was generated at: 01:43:45 IST Apr 14 2009
 Key name: <Default-RSA-Key>
  Usage: General Purpose Key
  Modulus Size (bits): 1024
  Key Data:
   30819f30 0d06092a 864886f7 0d010101
    05000381 8d003081 89028181 00d4a509
   99e95d6c b5bdaa25 777aebbe 6ee42c86
    23c49f9a bea53224 0234b843 1c0c8541
   f5a66eb1 6d337c70 29031b76 e58c3c6f
    36229b14 fefd3298 69f9123c 37f6c43b
   4f8384c4 a736426d 45765cca 7f04cba1
    29a95890 84d2c5d4 adeeb248 a10b1f68
   2fe4b9b1 5fa12d0e 7789ce45 55190e79
    1364aba4 7b2b21ca de3af74d b7020301 0001
 Key pair was generated at: 06:36:00 IST Apr 15 2009
 Key name: my.CA.key
  Usage: General Purpose Key
  Modulus Size (bits): 1024
  Key Data:
```

```
30819f30 0d06092a 864886f7 0d010101
    05000381 8d003081 89028181 00b8e20a
   a8332356 b75b6600 735008d3 735d23c5
    295b9247 2b5e02a8 1f63dc7a 570667d7
   545e7f98 d3d4239b 42ab8faf 0be8a5d3
    94f80d01 a14cc01d 98b1320e 9fe84905
   5ab94b18 ef308eb1 2f22ab1a 8edb38f0
    2c2cf78e 07197f2d 52d3cb73 91a9ccb2
   d903f722 bd414b0a 3205aa05 3ec45e24
    6480606f 8e417f09 a7aa9c64 4d020301 0001
 Key pair was generated at: 07:35:18 IST Apr 16 2009
 ASA-1#
• show crypto isakmp sa 명령은 피어의 모든 현재 IKE SA를 표시합니다.
 ASA#show crypto isakmp sa
    Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active
    and 1 Rekey SA during rekey)
 Total IKE SA: 1
     IKE Peer: 172.17.1.1
 1
     Type : L2L
                               Role
                                      : initiator
                               State : MM ACTIVE
     Rekey
             : no

    show crypto ipsec sa 명령은 피어의 모든 현재 IPSec SA를 표시합니다.

 ASA#show crypto ipsec sa
 interface: outside
     Crypto map tag: outside_map, seq num: 1,
    local addr: 192.168.1.1
       local ident (addr/mask/prot/port):
    (10.2.2.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port):
    (10.5.5.0/255.255.255.0/0/0)
       current_peer: 172.17.1.1
      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
       #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 9, #pkts comp failed:
    0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures:
    0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0,
    #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 192.168.1.1,
    remote crypto endpt.: 172.17.1.1
       path mtu 1500, ipsec overhead 58, media mtu 1500
       current outbound spi: 434C4A7F
     inbound esp sas:
       spi: 0xB7C1948E (3082917006)
          transform: esp-3des esp-sha-hmac none
          in use settings ={L2L, Tunnel, PFS Group 2, }
          slot: 0, conn_id: 12288, crypto-map: outside_map
          sa timing: remaining key lifetime (kB/sec): (4274999/3588)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0x434C4A7F (1129073279)
```

```
transform: esp-3des esp-sha-hmac none
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 12288, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/3588)
IV size: 8 bytes
replay detection support: Y
```

Output <u>Interpreter 도구(등록된</u> 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력 의 분석을 보려면 OIT를 사용합니다.

<u>문제 해결</u>

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 show 명령을 지원합니다.OIT를 사용하여 show 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전<u>에 Debug 명령</u> 및 <u>IP 보안 문제 해결 - Understanding and Using</u> <u>debug Commands(디버그 명령 이해 및 사용</u>)에 <u>대한 중요 정보를</u> 참조하십시오.

• debug crypto ipsec 7 - 2단계의 IPSec 협상을 표시합니다.debug crypto isakmp 7 - 1단계의 ISAKMP 협상을 표시합니다.

Site-to-<u>Site</u> VPN 트러블슈팅 방법에 대한 자세한 내용은 <u>Most Common L2L and Remote Access</u> <u>IPSec VPN Troubleshooting Solutions(가장 일반적인 L2L 및 원격 액세스 IPSec VPN 트러블슈팅</u> <u>솔루션</u>)를 참조하십시오.

<u>관련 정보</u>

- <u>Cisco Adaptive Security Appliance 지원 페이지</u>
- <u>Cisco VPN 클라이언트 지원 페이지</u>
- <u>기술 지원 및 문서 Cisco Systems</u>