ASA 8.x Anyconnect 인증(벨기에 eID 카드 사용)

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 배경 정보 로컬 PC 설정 운영 체제 카드 리더기 eID 런타임 소프트웨어 인증 인증서 AnyConnect 설치 ASA 요구 사항 ASA 컨피그레이션 1단계. 외부 인터페이스를 활성화합니다. 2단계. 도메인 이름, 비밀번호 및 시스템 시간을 구성합니다. <u>3단계. 외부 인터페이스에서 DHCP</u>서버를 활성화합니다. 4단계. eID VPN 주소 풀 구성 5단계. 벨기에 루트 CA 인증서 가져오기 6단계. Secure Sockets Laver 구성 7단계. 기본 그룹 정책 정의 8단계. 인증서 매핑 정의 9단계. 로컬 사용자 추가 10단계. ASA를 재부팅합니다. 미세 조정 1분 구성 관련 정보

<u>소개</u>

이 문서에서는 벨기에 eID 카드를 사용하도록 ASA 8.x Anyconnect 인증을 설정하는 방법에 대해 설명합니다.

<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.

- 적절한 ASA 8.0 소프트웨어가 포함된 ASA 5505
- AnyConnect 클라이언트
- ASDM 6.0

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 Cisco 기술 팁 표기 규칙을 참고하십시오.

<u>배경 정보</u>

eID는 사용자가 원격 Windows PC에서 인증하기 위해 사용해야 하는 벨기에 정부가 발급한 PKI(Public Key Infrastructure) 카드입니다. AnyConnect 소프트웨어 클라이언트는 로컬 PC에 설치 되며 원격 PC에서 인증 자격 증명을 받습니다. 인증이 완료되면 원격 사용자는 전체 SSL 터널을 통 해 중앙 리소스에 액세스할 수 있습니다. 원격 사용자는 ASA에서 관리하는 풀에서 가져온 IP 주소 로 프로비저닝됩니다.

<u>로컬 PC 설정</u>

<u>운영 체제</u>

로컬 PC의 운영 체제(Windows, MacOS, Unix 또는 Linux)는 모든 필수 패치가 설치된 최신 상태여 야 합니다.

<u>카드 리더기</u>

eID 카드를 사용하려면 로컬 컴퓨터에 전자 카드 판독기를 설치해야 합니다. 전자카드 리더기는 컴 퓨터의 프로그램과 ID 카드의 칩 사이에 통신 채널을 만드는 하드웨어 장치입니다.

승인된 카드 판독기 목록은 다음 URL을 참조하십시오. http://www.cardreaders.be/en/default.htm

참고: 카드 리더를 사용하려면 하드웨어 공급업체에서 권장하는 드라이버를 설치해야 합니다.

eID 런타임 소프트웨어

벨기에 정부가 제공하는 eID 런타임 소프트웨어를 설치해야 합니다. 이 소프트웨어를 사용하면 원 격 사용자가 eID 카드의 내용을 읽고, 검증하고, 인쇄할 수 있습니다. 이 소프트웨어는 Windows, MAC OS X 및 Linux용 프랑스어 및 네덜란드어로 제공됩니다.

자세한 내용은 다음 URL을 참조하십시오.

<u>http://www.belgium.be/zip/eid_datacapture_nl.html</u>

<u>인증 인증서</u>

로컬 PC의 Microsoft Windows 저장소로 인증 인증서를 가져와야 합니다. 인증서를 저장소로 가져 오지 못하면 AnyConnect 클라이언트가 ASA에 대한 SSL 연결을 설정할 수 없습니다.

절차

.

Windows 저장소로 인증 인증서를 가져오려면 다음 단계를 완료하십시오.

1. eID를 카드 판독기에 삽입하고, eID 카드의 내용에 액세스하려면 미들웨어를 실행합니다.eID 카드의 내용이 나타납니다

🖏 Carte d'identité					
🗧 🗆 🖨 🖉 🗶		T WERTHER STREET	Section 2	a koko ko ja koko ko	
Identité Certificats Carte & PIN Option	is Info				
BELGIQUE	BELGIË	BELGIEN	BE	LGIUM	
CARTE D'IDENTITE	IDENTITEITSKAART	PERSONALAUSWEIS	IDE	NTITY CARD	
	Identité				
	Nom				
	Prénoms				F
	Lieu de naissance	Date de naissance	Sexe	Nationalité	
		14/04/1963	м	be	
	Titre		Numéro national		
Cat	A.4		03.04.14-033.25		
Numéro de la cause	Adresse				
534C494E336600296CFF2715071	82C36				
Numéro de la carte	Code postal Commune			Pays	-
590.5942800.24				pe	
07/06/2007 07/06/2012	Statut spécial			-	
Commune d'émission	Canne blanche				
	Canne jaune				
	Minorité étendue		1	-	
			den.		
				12 M	
				- 1	
		24		the state of the	
			123.	1 1	
The second s				AND TO POST	
Fini	en la cara a	a construction and a second second	STATISTICS TOTAL		

2. Certificates (FR) 탭을 클릭합니다.인증서 계층 구조가 표시됩니다

📾 Carte d'identité		
6 🗖 🖙 🖬 🚳 🛪 Identité Certificats Carte & PIN Options Info		
Certificats		
BELPIC	Propriétaire	- Hard Star
Belgium Root CA	(Autrie	entication)
Citizen CA	Citizen CA	
(Signature)	Longueur de clé 1024 bits	
	Valide du	Au
	15/06/2007	08/06/2012
	Statut du certificat Non validé	
	Les certificats de la carte utiliser la carte d'identité (OpenOffice.org, Adobe P sélectionnez-le et cliquez	eID doivent être enregistrés dans Windows pour pouvoir électronique dans Internet Explorer, Microsoft Office, leader, Outlook, Pour enregistrer un certificat, sur le bouton « Enregistrer ». Enregistrer Détails >>
Fini		

- 3. 벨기에 **루트 CA**를 확장한 다음 Citizen CA를 확장합니다.
- 4. 명명된 인증서의 인증 버전을 선택합니다.
- 5. Enregister (FR) 버튼을 클릭합니다.인증서가 Windows 저장소에 복사됩니다.

참고: Details(세부사항) 버튼을 클릭하면 인증서에 대한 세부사항이 표시되는 창이 나타납니다. Details(세부사항) 탭에서 Subject(제목) 필드를 선택하여 Serial Number(일련 번호) 필드를 표시합 니다. Serial Number 필드에는 사용자 권한 부여에 사용되는 고유한 값이 포함됩니다. 예를 들어, 일 련 번호 "56100307215"는 출생 일자가 1956년 10월 3일 순번이 072이고 수표 번호가 15인 사용자 를 나타냅니다. 이러한 번호를 저장하려면 연방 당국의 승인 요청을 제출해야 합니다. 벨기에 시민 의 데이터베이스 유지와 관련된 적절한 공식 선언을 하는 것은 여러분의 책임입니다.

다음을 확인합니다.

인증서를 성공적으로 가져왔는지 확인하려면 다음 단계를 완료하십시오.

- 1. Windows XP 컴퓨터에서 DOS 창을 열고 mmc 명령을 **입력합니다**.Console 애플리케이션이 나타납니다.
- 2. [**파일] > [스냅인 추가/제거]를** 선택하거나 Ctrl+M을 누릅니다.스냅인 추가/제거 대화 상자가 나타납니다.
- 3. Add 버튼을 클릭합니다.독립형 스냅인 추가 대화 상자가 나타납니다.
- 4. Available Standalone Snap-ins(사용 가능한 독립형 스냅인) 목록에서 **Certificates(인증서**)를 선택하고 Add(**추가)**를 클릭합니다.
- 5. **내 사용자 계정** 라디오 버튼을 클릭하고 **마침**을 클릭합니다.Add/Remove Snap-in 대화 상자 에 Certificate 스냅인이 나타납니다.
- 6. Close(**닫기)**를 클릭하여 Add Standalone Snap-in(독립형 스냅인 추가) 대화 상자를 닫은 다음 Add/Remove Snap-in(스냅인 추가/제거) 대화 상자에서 OK(확인)를 클릭하여 변경 사항을 저 장하고 Console 애플리케이션으로 돌아갑니다.

- 7. Console Root(콘솔 루트) 폴더에서 Certificates(인증서) Current User(현재 사용자)를 확장합 니다.
- 8. Personal(**개인**)을 확장한 다음 Certificates(인증서)를 **확장합니다**.가져온 인증서는 다음 이미 지와 같이 Windows 저장소에 나타나야 합니다

🐞 Console1 - [Console Root\Certific	ates - Current User/Personal/Ce	rtificates]			X			
🚡 File Action View Favorites Wind	File Action View Favorites Window Help							
Console Root	Issued To /	Issued By	Expiration Date	Intended Purposes	Frier			
Certificates - Current User Personal Certificates Trusted Root Certification Author Enterprise Trust Intermediate Certification Author Active Directory User Object Trusted Publishers Untrusted Certificates Trusted People Other People Other Certificate Enrollment Requests	(Authentication)	Citizen CA	8/06/2012	Client Authentication	Clé c			
	<				>			
Personal store contains 1 certificate.								

<u>AnyConnect 설치</u>

.

원격 PC에 AnyConnect 클라이언트를 설치해야 합니다. AnyConnect 소프트웨어는 사용 가능한 게 이트웨이 목록을 미리 설정하기 위해 편집할 수 있는 XML 구성 파일을 사용합니다. XML 파일은 원 격 PC의 이 경로에 저장됩니다.

C:\Documents and Settings\%USERNAME%\Application Data\Cisco\Cisco AnyConnect VPN Client

여기서 %USERNAME%은(는) 원격 PC에 있는 사용자의 이름입니다.

XML 파일의 이름은 preferences.xml입니다. 다음은 파일 내용의 예입니다.

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectPreferences> <DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences> 여기서 192.168.0.1은 ASA 게이트웨이의 IP 주소입니다.



ASA가 다음 요구 사항을 충족하는지 확인합니다.

• AnyConnect 및 ASDM은 플래시에서 실행해야 합니다.이 문서의 절차를 완료하려면 적절한 ASA 8.0 소프트웨어가 설치된 ASA 5505를 사용하십시오. AnyConnect 및 ASDM 애플리케이 션은 플래시에 미리 로드해야 합니다. flash의 내용을 보려면 show flash 명령을 사용합니다. ciscoasa#show flash:

- #	length	date/time	- path
66	14524416	Jun 26 2007 10:24:0	2 asa802-k8.bin
67	6889764	Jun 26 2007 10:25:2	8 asdm-602.bin
68	2635734	Jul 09 2007 07:37:0	6 anyconnect-win-2.0.0343-k9.pkg

• ASA는 공장 기본값으로 실행해야 합니다.이 문서의 절차를 완료하기 위해 새 ASA 섀시를 사용 하는 경우 이 요구 사항을 건너뛸 수 있습니다. 그렇지 않으면 ASA를 공장 기본값으로 재설정 하려면 다음 단계를 완료하십시오.ASDM 애플리케이션에서 ASA 섀시에 연결하고 File(파일) > Reset Device to the Factory Default Configuration(공장 기본 컨피그레이션으로 디바이스 재설 정)을 선택합니다



템플릿에 기본값을 그대로 둡니다.이더넷 0/1 내부 인터페이스에서 PC를 연결하고 ASA의 DHCP 서버에서 프로비저닝될 IP 주소를 갱신합니다.**참고:** 명령줄에서 ASA를 공장 기본값으 로 재설정하려면 다음 명령을 사용합니다.

ciscoasa#conf t

ciscoasa#config factory-default 192.168.0.1 255.255.255.0

ASA 컨피그레이션

ASA 공장 기본값을 재설정한 후에는 이더넷 0/1 내부 인터페이스에서 ASA에 연결하기 위해 ASDM을 192.168.0.1으로 시작할 수 있습니다.

참고: 이전 비밀번호는 보존됩니다(또는 기본적으로 비어 있을 수 있음).

기본적으로 ASA는 서브넷 192.168.0.0/24에 소스 IP 주소가 있는 수신 관리 세션을 수락합니다. ASA의 내부 인터페이스에서 활성화된 기본 DHCP 서버는 192.168.0.2-129/24 범위의 IP 주소를 제 공하며 ASDM을 사용하여 내부 인터페이스에 연결할 수 있습니다.

ASA를 구성하려면 다음 단계를 완료합니다.

- 1. <u>외부 인터페이스 활성화</u>
- 2. <u>도메인 이름, 비밀번호 및 시스템 시간 구성</u>
- 3. <u>외부 인터페이스에서 DHCP 서버 활성화</u>
- 4. <u>eID VPN 주소 풀 구성</u>
- 5. <u>벨기에 루트 CA 인증서 가져오기</u>
- 6. <u>Secure Sockets Layer 구성</u>
- 7. <u>기본 그룹 정책 정의</u>
- 8. <u>인증서 매핑 정의</u>
- 9. <u>로컬 사용자 추가</u>
- 10. <u>ASA 재부팅</u>

1단계. 외부 인터페이스를 활성화합니다.

이 단계에서는 외부 인터페이스를 활성화하는 방법을 설명합니다.

- 1. ASDM 애플리케이션에서 Configuration(컨피그레이션)을 클릭한 다음 Device Setup(디바이스 설정)을 클릭합니다.
- 2. Device Setup(디바이스 설정) 영역에서 Interfaces(인터페이스)를 선택한 다음 Interfaces(인터 페이스) 탭을 클릭합니다

🛍 Cisco ASDM 6.0 for ASA - 192.168.0.	1								
File View Tools Wizards Window Help					Look	For:		Find +	ahaha
Home 🖧 Configuration 📴 Monitoring	Save	📿 Refresh 🔇	Back 🕐 Poresard	? Help					CISCO
Device List an a × co	onfiguratio	n > Device Setup > In	terfaces						0
Add 1 Delete S Connect	Interfaces	Switch Ports							
192.160.0.1	Name	Switch Ports	Enabled	Security	IP Address	Subnet Mask	Restrict	VLAN	
	inside	Ethernet0/1, Ethernet0	(2, Et Yes	100	192.168.0.1	255.255.255.0	Tramic noer	viant	A00
	outside	Ethernet0/0	Yes	0	197.0.100.1	255.255.255.0		vlan2	EdR
									Delete
Device Setup									
g ⁹ Startup Wizard									
Scherlages Scherlages									
Device Name/Password									
a O system ize									
B. Device Setup									
P. Frewal									
03	<			dina di					
in the Access with	Enable b	raffic between two or m	ore interfaces which	are configur	ed with same sec	unity levels			
Ste-to-Ste VPN	Enable t	raffic between two or m	ore hosts connected	to the same	interface				
Device Management									
				A	sply Re	eset			
Device configuration loaded successfully.					<admin></admin>	15		20	/07/07 8:35:14 UTC

- 3. 외부 인터페이스를 선택하고 Edit를 클릭합니다.
- 4. General(일반) 탭의 IP address(IP 주소) 섹션에서 Use Static IP(고정 IP 사용) 옵션을 선택합니다.
- 5. IP 주소에 197.0.100.1을 입력하고 서브넷 마스크에 255.255.255.0을 입력합니다.
- 6. Apply를 클릭합니다.

.

2단계. 도메인 이름, 비밀번호 및 시스템 시간을 구성합니다.

이 단계에서는 도메인 이름, 비밀번호 및 시스템 시간을 구성하는 방법에 대해 설명합니다.

1. Device Setup 영역에서 Device Name/Password를 선택합니다

🛍 Cisco ASDM 6.0 for ASA - 192.168	10.1 ···· ·	
File Wew Tools Wizards Window H	Hip Look For: Find	ahaha
Home 🖧 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🥜 Help	CISCO
Device List d P ×	Configuration > Device Setup > Device Hame/Pessword	0
Add Delete S Connect	Hostname and Domain Name	
B1192100.01	Hostname: ciscoase	
	Domain Name: cisco.be	
	Enable Password	
	Change the privleged mode password.	
Desice Setup	Old Password:	
3 ⁹ Sartup Wizard	New Password: *******	
Interfaces	Confirm New Password: *******	
Privice Name/Password		
🛞 🧿 System Time	Telnet Password	
	Change the password to access the conside or the security appearce.	
	Old Password:	
	New Password:	
	Confirm New Password:	
S Design Settion		
and and and		
🐑 Frewal		
Remote Access VPN		
Ste-to-Site VPN		
Device Management		
:	Apply Reset	
Device configuration loaded successfully.	<admin> 15 🔯 🛃 🔂</admin>	27/07/07 8:36:04 UTC

- 2. 도메인 이름에 cisco.be를 입력하고 Enable Password(비밀번호 활성화) 값에 cisco123을 입 력합니다.**참고:** 기본적으로 비밀번호는 비어 있습니다.
- 3. Apply를 클릭합니다.
- 4. Device Setup(디바이스 설정) 영역에서 System Time(시스템 시간)을 선택하고 클럭 값을 변 경합니다(필요한 경우).
- 5. Apply를 클릭합니다.

.

<u>3단계. 외부 인터페이스에서 DHCP 서버를 활성화합니다.</u>

이 단계에서는 테스트를 용이하게 하기 위해 외부 인터페이스에서 DHCP 서버를 활성화하는 방법 에 대해 설명합니다.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
- 2. Device Management(디바이스 관리) 영역에서 DHCP를 확장하고 DHCP Server(DHCP 서버)를 선택합니다

G Cisco ASDM 6.0 for ASA - 192.168	.0.1						
File Wew Tools Wizards Window He	elp		Look	For:		Find +	ababa
Home Configuration D Monitori	ing 🔚 Save 💽 Refresh	Sack 🕐 Formard 🖓 Hel	p				CISCO
Device List an Q ×	Configuration > Device Ma	nagement > DHCP > DHCP Server					
Add Delete S Connect	Interface DHCP Enabled	d Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout L	e Edk
S. Contraction	outside Yes	192.168/0.2 - 192.168/0.129					
Device Management & P ×							
Management Access System Image/Configuration							
🗉 🙀 High Availability							
E Logging	<					-	<u>1</u>
Certificate Management	Global DHCP Options						
P DHCP Relay	Enable auto-configurat	ion from interface: outs 💌 📃	Allow VPN override				
EHCP Server	Enabling auto-configuration take precedence over the	n causes the DHOP server to automatic auto-configured values.	ally configure DNS	, WINS and the d	efault domain na	me. The values in th	ve fields below
B B Advanced	DNS Server 1:	Primary WINS	Server:				
	DNS Server 2:	Secondary WD	IS Server:				
	Domain Name:						
	Lease Length:	secs					
Device Setup	Ping Timeout:	ns					
🕄 Firewal						l	Advanced
Remote Access VPN	Dynamic DNS Settings fo	r DHCP Server					
CA Ste-to-Ste VPN	Update DNS Server						
	Update Both Record	ds Override Client Settings					
B Levice Banagement							
\$			R	esec			
Running configuration successfully saved to flas	sh memory.		<admin></admin>	15	😼 🛃	2	7/07/07 8:48:04 UTC

- 3. Interface 목록에서 외부 인터페이스를 선택하고 Edit를 클릭합니다. Edit DHCP Server 대화 상 자가 나타납니다.
- 4. Enable DHCP Server(DHCP 서버 활성화) 확인란을 선택합니다.
- 5. DHCP Address Pool(DHCP 주소 풀)에 197.0.100.20~197.0.100.30의 IP 주소를 입력합니다.
- 6. Global DHCP Options(전역 DHCP 옵션) 영역에서 Enable auto-configuration from interface(인터페이스에서 자동 컨피그레이션 활성화) 확인란의 선택을 취소합니다. 7. Apply를 클릭합니다.

4단계. elD VPN 주소 풀 구성

이 단계에서는 원격 AnyConnect 클라이언트를 프로비저닝하는 데 사용되는 IP 주소 풀을 정의하는 방법에 대해 설명합니다.

- 1. Configuration(컨피그레이션)을 클릭한 다음 Remote Access VPN(원격 액세스 VPN)을 클릭 합니다.
- 2. Remove Access VPN(액세스 VPN 제거) 영역에서 Network (Client) Access(네트워크(클라이 언트) 액세스)를 확장한 다음 Address Assignment(주소 할당)를 확장합니다.
- 3. Address Pools(주소 풀)를 선택한 다음 Configure named IP Address pools(명명된 IP 주소 풀 구성) 영역에 있는 Add(추가) 버튼을 클릭합니다 Add IP Pool 대화 상자가 나타납니다

Gisco ASDM 6.0 for ASA - 192.168	.0.1					
File View Tools Wizards Window He	de de	an da anna an tao bar gan bhailtean an an	Alex Constant of the second of the	Look For:	Find +	advada.
Home 🔏 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refre	sh 🔇 Back 🚫 Forwa	a 🦿 Help			cisco
Device List d7 & ×	Configuration > Remote	Access VPN > Hetwork (Client) Access > Add	tress Assignment >	Address Pools	
Add 👔 Delete 🔊 Connect	Configure named IP Add	dress pools.				
192.160.0.1	This assumption is apple	and in other a title many one			and a section and in a	
	mo parameter o entre	Counterrainer a tres process	CELEBRATE AND	a contraction proved of	COLUMN CONSUMEROUS	
	Add 📑 Edt 📋	Delete				
	Pool Name	Starting Address		Ending Address	Subnet Mask	
	_					
Remote Access VPN 2 P ×		Add IP Pool		×		
😑 🗃 Network (Client) Access 🔺						
SSL VPN Connection Profiles						
IPsec Connection Profiles				-		
Group Policies		Namec	eID-VPNPOOL			
Oynamic Access Policies						
Assignment Policy		Starting IP Address:	192.168.10.100			
Address Pools						
🗉 🔯 Advanced	1	Ending IP Address:	192.168.10.110	1000000		
Clentless SSL VPN Access						
Easy VPN Remote		Subnet Mask:	255.255.255.0	~		
E AAA Setup				1000 Bala		
Certificate Management						
P DHCP Server						
Contraction of the Owner of the		OK	Cancel Help			
Bevice Setup				_		
Frewal						
Bamote Access VPN						
Ste-to-Site VPN						
Device Management						
			Annh	(Beert		
\$			etba.	Keset		
			<8	imin> 15	🔯 🚰 🔰 🙆 2	7/07/07 8:53:04 UTC

- 4. Name 필드에 eID-VPNPOOL을 입력합니다.
- 5. Starting IP Address(시작 IP 주소) 및 Ending IP Address(종료 IP 주소) 필드에 192.168.10.100~192.168.10.110 범위의 IP 주소를 입력합니다.
- 6. Subnet Mask(서브넷 마스크) 드롭다운 목록에서 255.255.255.0을 선택하고 OK(확인)를 클릭 한 다음 Apply(적용)를 클릭합니다.

<u>5단계. 벨기에 루트 CA 인증서 가져오기</u>

이 단계에서는 벨기에 루트 CA 인증서로 가져오는 방법에 대해 설명합니다.

- 1. 정부 웹 사이트에서 벨기에 루트 CA 인증서(벨기에 umrca.crt 및 벨기에 umrca2.crt)를 다운로 드하여 설치하고 로컬 PC에 저장합니다.벨기에 정부 웹 사이트는 다음 URL에 있습니다. <u>http://certs.eid.belgium.be/</u>
- 2. Remote Access VPN(원격 액세스 VPN) 영역에서 **Certificate Management(인증서 관리**)를 확 장하고 **CA Certificates(CA 인증서)를** 선택합니다.
- 3. Add(**추가**)를 클릭한 다음 Install from file(파일에서 설치)을 클릭합니다.
- 4. 벨기에 루트 CA 인증서(벨기에umrca.crt) 파일을 저장한 위치를 찾아 Install Certificate(인증서 설치)를 클릭합니다.
- 5. Apply를 클릭하여 변경 사항을 저장합니다.
- 이 그림에서는 ASA에 설치된 인증서를 보여 줍니다.



<u>6단계. Secure Sockets Layer 구성</u>

이 단계에서는 보안 암호화 옵션의 우선 순위를 지정하고, SSL VPN 클라이언트 이미지를 정의하고, 연결 프로파일을 정의하는 방법에 대해 설명합니다.

1. 가장 안전한 암호화 옵션의 우선 순위를 지정합니다.Remote Access VPN(원격 액세스 VPN) 영역에서 **Advanced(고급**)를 확장하고 **SSL Settings(SSL 설정)**를 **선택합니다**. Encryption(암 호화) 섹션에서 Active Algorithms(활성 알고리즘)는 다음과 같이 누적, 하향식으로 누적됩니다 .AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1

🖀 Cisco ASDM 6.0 for ASA - 192.168	8.0.1	An address of the second structure of the second seco	en en entre desacente des la sedecte desta anon se server especiel estas de	
File View Tools Wizards Window H	telp		Look For: Find +	ahaha
Home Configuration 🕖 Monitor	ring 🔚 Save 🔇 Refresh 🔇 Back	C Forward ? Help	and a set of the data of the set	CISCO
Device List d ¹ 4 ×	Configuration > Remote Access VPH	> Advanced > SSL Settings		0
🗣 Add 📋 Delete 🖋 Connect	Configure SSL parameters. These parame	ters affect both ASDM and SSL VPN acc	ess.	
D 192.168.0.1				
	Server SSL Version: Any	Client SSL Version: Any		
	Encryption			
	Avaiable Algorithms	AMAN	Active Algorithms	Movello
	RC4-MD5		AE5256-5HA1	Li tore op
	DES-SHA1	<< Remove	AE5128-5HA1	Move Down
Remote Access VPN 🗗 🕈 🗡			30E5-SHA1	A STATE OF STATE OF STATE
🗄 🌃 Clientless SSL VPN Access 📃 🔺			RC4-SHA1	
Easy VPN Remote			L	
🗄 💼 AAA Setup	Certificates			1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
Secure Desitop Manager Cartificate Management	Specify which certificates, if any, should	the used for SSL authentication on eac	h interface. The fallback certificate will be used on interfa	ces not
P DHCP Server	associated with a certificate of their ow	n.		
3 DNS	Tehnelsen	ID Continue		
🖃 🐻 Advanced	inside	to Certaica		EdR
 Connection Gateway 	outside			1202000000000
SSL Settings				
Certificate to SSL VPN Conne				
HTTP Redrect				
Final Provy				
< s				
A Device Setup				
Frowal				
Remote Access VPN				
Ste-to-Site VPN				
Device Management	Falkark Cartificatas (
\$		Apply	Reset	
Running configuration successfully saved to fla	sh memory.	cadmir	> 15 😡 🔐 🙆	27/07/07 8:57:34 UTC

2. AnyConnect 클라이언트에 대한 SSL VPN 클라이언트 이미지를 정의합니다.Remote Access VPN(원격 액세스 VPN) 영역에서 Advanced(고급)를 확장하고 SSL VPN을 확장한 다음 Client Settings(클라이언트 설정)를 선택합니다.SSL VPN Client Images(SSL VPN 클라이언트 이미 지) 영역에서 Add(추가)를 클릭합니다.플래시에 저장된 AnyConnect 패키지를 선택합니다 .AnyConnect 패키지는 다음 이미지에 표시된 대로 SSL VPN Client Images 목록에 나타납니 다

.

📫 Cisco ASDM 6.0 for ASA - 192.	168,100,254	
File View Tools Wizards Window	r Help Look For: Frid -	ahaha
Home 🖧 Configuration 📴 Mo	intoring 🔚 Save 🔃 Refresh 🔇 Back 🚫 Forward 🧳 Help	cisco
Device List 51 & X	Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings	0
🗣 Add 📋 Delete 🖋 Connect	Identify SSL VPN Client (SVC) related files.	
A 192.168.0.1	SSI VIN Client Images	
A DESTRUCTION	Mininge connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.	
	🔶 Add 17 Replace 🗊 Delete 🛧 Move LP 🕹 Move Down	
	Add Investment also 3 & 03/3 (0 also	
	devia gang connect with a success gives pag	
Remote Access VPN 🔗 🔍		
Network (Client) Access		
SSL VPN Connection Profiles		
Group Policies		
Dynamic Access Policies	SSL WPN Client Profiles	
Accress Assignment	Add I Call Collector	
Address Pools	Name Parlame	
B S Advanced	Taking Taking	
B SS. VPN		
Client Settings		
Dypass Interface Ac		
C International S		
9		
Device Setup		
🐔 Frewal	SSL VPN Client Localization File	
Remote Access VPN	To set the Localization file go to Language Localization.	
Ste-to-Site VPN	Cache File System (to hold CSD and SVC images)	
Device Management	Maximum Size: 20 MB	
:	Acoly	
	(admin) 15 📴 😭 🍙 25/	07/07 23:20:54 UTC
🍠 start 🔰 🖬 🕹 🕹 😣	🛐 🦈 🚘 a Wind 🛐 200(Pro 📷 C.(WIRD 👩 Caso A5 🏪 a Infan 💽 TextPad 🤞	S 10 10.00

3. DefaultWEBVPNGroup 연결 프로파일을 정의합니다.Remote Access VPN(원격 액세스 VPN) 영역에서 Network (Client) Access(네트워크(클라이언트) 액세스)를 확장하고 SSL VPN Connection Profiles(SSL VPN 연결 프로파일)를 선택합니다.Access Interfaces(액세스 인터페 이스) 영역에서 Enable Cisco AnyConnect VPN Client(Cisco AnyConnect VPN 클라이언트 활 성화) 확인란을 선택합니다.외부 인터페이스의 경우 다음 이미지에 표시된 대로 Allow Access(액세스 허용), Require Client Certificate(클라이언트 인증서 필요) 및 Enable DTLS(DTLS 활성화) 확인란을 선택합니다

🕼 Cisco ASDM 6.0 for ASA - 192.168	8.100.254	a da palaka menaka salak seberah 2014 s			en en fan de ser en fan de	
File View Tools Wizards Window H	elp		the second second	Look For:	Find +	alada
Home 🖧 Configuration [Monitor	ng 🔚 Save 🔇	Refresh 🚫 Back (💭 Porward 🧳 Help			cisco
Device List 라우×	Configuration > Re	emote Access VPH >	Network (Client) Access > SS	L VPN Connection Profile	5	0
◆ Adj ① Delete Ø Connect	The security appl deployment requi Security (DTLS) to (More client-related	iance automatically dep ires end-user administra unneling options. ted parameters, such a	loys the Cisco AnyConnect VPN Cl Rive rights. The Cisco AnyConnect s client images and client profiles,	ient or legacy SSL VPN Client VPN Client supports the HT can be found at sternt Settor	to remote users upon connection. IPS/TCP (SSL) and Datagram Trans	The initial client sport Layer
	Access Interdentia					
	Access Incertace					
E D Network (Clerit) Access	Enable Cisco	AnyConnect VPN Clent	or legacy SSL WIN Client access of	n the interfaces selected in t	ne table below	
SSL VPN Connection Profiles	Interface	Allow Access	Require Client Certificate	Enable DTLS		
IPsec Connection Profiles	locide					
Group Policies	1000					
Bio Dynamic Access Policies						
Advanced	100					
Clentless SSL VPN Access	Access Port: 44	3 DTLS P	ort: 443			
Connection Profiles						
Portal	Click here to Ass	ion Certificate to Interfa	<u>808</u> ,			
the Extranic Access Policies	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1					
🖃 🚼 Advanced	Connection Profi	les				
🛅 Encoding 🛛 💌	Connection profile	e (tunnel group) table b	elow contains records that determ	nine connection policies. A re	cord identifies a default group polic	cy for the
< >>	connection and c	oricaris prococor-specific	connection parameters.			
S Desize Setue	Add 🛃 Ed	Celece				
20	Name	Alases	SSL VPN	Client Protocol	Group Policy	
Firewall	Defaultivesweisen	20up	Enabled		Dittorprotoy	
OR Daniela burary USM	Deradorskaroop		Chabled		cricaproicy	
0.0 Ganges were and						
Ste-to-Site VPN						
Device Management	Allow user to	select connection. iden	tified by alias in the table above.	at login page		
:			Apply	Reset		
			<	idmin> 15	😡 🚱 🛛 🙆 2	6/07/07 0:20:25 UTC

Connection Profiles(연결 프로파일) 영역에서 Default(기본)WEBVPNGroup**을** 선택하고 Edit(편집)를 **클릭합니다**.Edit SSL VPN Connection Profile 대화 상자가 나타납니다

🛍 Edit SSL VPN Connecti	on Profile: DefaultWE	BVPNGroup	
Basic	Name: Aliases:	DefaultWEBVPNGroup	
	Authentication		
	Method:	○ AAA	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL If Server Group fails	
	Client Address Assign	ent	
	DHCP Servers:		
	Client Address Pools:		Select
	Default Group Policy -		
	Group Policy:	DfltGrpPolicy	Manage
	SSL VPN Client Protocol:	C Enabled	
L			
	ОК	Cancel Help	

탐색 영역에서 **기본**을 선택합니다.Authentication(인증) 영역에서 Certificate(인증서) 라디오 버튼을 클릭합니다.Default Group Policy(기본 그룹 정책) 영역에서 **SSL VPN Client Protocol(SSL VPN 클라이언트 프로토콜**) 확인란을 선택합니다.Advanced(**고급**)를 확장하고 Authentication(**인증)을** 선택합니다.Add(**추가**)를 클릭하고 다음 이미지에 표시된 대로 로컬 서 버 그룹이 있는 외부 인터페이스를 추가합니다

📬 Edit SSL VPN Connecti	ion Profile: Default	WEBVPNGroup		×
Basic Advanced General	Interface-Specific A	Authentication Server Group	15	
Client Addressing Authentication Authorization Accounting SSL VPN	Interface outside	Server Group LOCAL	Fallback to LOCAL	
	ОК	Cancel Hel	P	

탐색 영역에서 Authorization을 **선택합니다**.Default Authorization Server Group(기본 권한 부 여 서버 그룹) 영역의 Server Group(서버 그룹) 드롭다운 목록에서 LOCAL(로컬)을 선택하고 Users must exist in the authorization database to connect(연결할 권한 부여 데이터베이스에 사용자가 존재해야 함) 확인란을 선택합니다.User Name Mapping(사용자 이름 매핑) 영역의 Primary DN Field(기본 DN 필드) 드롭다운 목록에서 SER (Serial Number)를 선택하고 Secondary DN Field(보조 DN 필드)에서 None(없음)을 선택한 다음 OK(확인)를 클릭합니다

🖆 Edit SSL VPN Connectio	on Profile: DefaultWEBVPNGroup	×
Basic Advanced General Client Addressing Authentication Authorization Accounting SSL VDM	Default Authorization Server Group Server Group: LOCAL Ulsers must exist in the authorization database to connect Interface-specific Authorization Server Groups Add C Edit Polete	
	Interface Server Group	
	User Name Mapping Use the entire DN as the username Specify individual DN fields as the username Primary DN Field: SER (Serial Number) Secondary DN Field: None OK Cancel Help	

<u>7단계. 기본 그룹 정책 정의</u>

.

이 단계에서는 기본 그룹 정책을 정의하는 방법에 대해 설명합니다.

1. Remote Access VPN(원격 액세스 VPN) 영역에서 **Network (Client) Access(네트워크(클라이 언트) 액세스**)를 확장하고 **Group Policies(그룹 정책)를** 선택합니다

🖆 Cisco ASDM 6.0 for ASA - 192.168	3.0.1				
File View Tools Wizards Window H	ыþ		Look For:	Find	ahaha
Home 🔏 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 I	Back 🚫 Forward 💡 Hel	P		CISCO
Device List and A ×	Configuration > Remote Access	/PH > Network (Client) Acce	ss > Group Policies		
Add Delete S Connect	Manage VPN group policies. A VPN	group policy is a collection of u	ser-oriented attribute/value pairs that m	ay be stored internally on the d	evice or
A LEAST CALL	Add - T Edt 1 Faller	er. The group poicy information	n is renerenced by very curinel groups and	user accounts.	
	Name	Tura	Turnalina Destoral	AAA Secure Genue	
	DRGrpPolicy (System Default)	Internal	L2TP-IPSec, svc, IPSec, webvpn	N/A	
Remote Access VPN & Q ×					
B Network (Client) Access					
 SS, VPN Connection Profiles IPsec Connection Profiles 					
Group Policies					
Dynamic Access Policies					
E G Advanced					
Chendless SSL VPN Access Easy VPN Remote					
🗄 📸 AAA Setup					
Secure Desktop Manager Secure Desktop Manager Secure Desktop Manager					
P DHCP Server					
B Advanced					
0					
Device Setup					
En Prowal					
Remote Access VPN					
Ste-to-Ste VPN					
Device Management					
:			Apply Reset		
			cadmin> 15	27	/07/07 15:23:14 UTC

- 2. 그룹 정책 목록에서 **DfltGrpPolicy**를 선택하고 Edit를 **클릭합니다**. 3. Edit Internal Group Policy 대화 상자가 나타납니다

.

💕 Edit Internal Group Po	licy: DfltGrpPolicy		
General	Name: DfltGrpP	blicy	
 Advanced Split Tunneling 	Banner:		
IE Browser Proxy SSL VPN Client Login Setting	Address Pools: eID-VP	NPOOL	Select
Key Regeneration Dead Peer Detecti	Tunneling Protocols:	Clientless SSL VPN 🕑 SSL VPN Client 🗌 IPsec	L2TP/IPsec
Customization IPsec Client	Filter:	None	Manage
	NAC Policy:	None	Manage
	Access Hours: Simultaneous Logins:	Unrestricted	Manage
	Restrict access to VLAN	Unrestricted	
	Maximum Connect Time:	Unlimited minutes	
	Idle Timeout:	Unlimited 30 minutes	
<			
	ОК	Cancel Help	

- 4. 탐색 영역에서 **일반**을 선택합니다.
- 5. 주소 풀의 경우 **선택**을 클릭하여 주소 풀을 선택하고 elD-**VPNPOOL을** 선택합니다.
- 6. More Options(추가 옵션) 영역에서 **IPsec** 및 **L2TP/IPsec** 확인란의 선택을 취소하고 **OK(확인**)**를 클릭합니다**.

<u>8단계. 인증서 매핑 정의</u>

이 단계에서는 인증서 매핑 기준을 정의하는 방법을 설명합니다.

- 1. Remote Access VPN(원격 액세스 VPN) 영역에서 Advanced(고급)를 클릭하고 Certificate to SSL VPN Connection Profile Maps(SSL VPN 연결 프로파일 맵에 인증서)를 선택합니다.
- 2. Certificate to Connection Profile Maps(인증서-연결 프로파일 맵) 영역에서 Add(추가)를 클릭 하고 맵 목록에서 DefaultCertificateMap을 선택합니다.이 맵은 Mapped to *Connection Profile(*연결 프로파일에 매핑됨) 필드의 DefaultWEBVPNProfile과 일치해야 합니다.
- 3. Mapping Criteria(매핑 조건) 영역에서 Add(추가)를 클릭하고 다음 값을 추가합니다.필드: 발급 자, 국가(C), 같음, "be"필드: 발급자, CN(Common Name), Equals, "citizen ca"매핑 기준은 다 음 이미지에 표시된 대로 나타납니다

💼 Cisco ASDM 6.0 for ASA - 192.168	.100.254	1998 - Lagrid Admir 1998 I. Stader 1998 1	ta parta atra tata da pondo	e de la company de la comp		nenara processione	
File View Tools Wizards Window He	de de			Look	For:	Find +	alada
Home 🔓 Configuration 📴 Monitori	ng 🔚 Save Q	Refresh 🔇 Back 🤇	Porward ? H	elp			cisco
Device List d ^a P ×	Configuration > R	emote Access VPH > A	dvanced > Certific	vie to SSL VPH Co	enection Profile Maps		0
Add Delete Ø Connect 192.168.0.1 192.168.100.251	Define rules to m matching criteria Certificate to Co	ap certificates to desired for the selected rule. mection Profile Maps It Delete	connection profiles (t	unnel groups). Use t	he bottom table to configure certific	ate fields togethe	r with their
	Map Name	al Marc	Rule Priority	Mapped to C	onnection Profile		
Remote Access VPN D A × Contribute Management Code Signer Code Sig	Mapping Criteria Add C Ed Field Issuer Ssuer	t Delete Component Country (C) Common Name (CN)		Operator Equals Equals Equals	Volue De citizen ca		
Configuration changes saved successfully.				<admin></admin>	15 🔯 🚰 🔂	@ 24	07/07 23:20:54 UTC

4. Apply를 클릭합니다.

<u>9단계. 로컬 사용자 추가</u>

이 단계에서는 로컬 사용자를 추가하는 방법을 설명합니다.

- 1. Remote Access VPN(원격 액세스 VPN) 영역에서 AAA Setup(AAA 설정)을 확장하고 Local Users(**로컬 사용자)를** 선택합니다.
- 2. Local Users(로컬 사용자) 영역에서 Add(추가)를 클릭합니다.
- 3. 사용자 이름 필드에 사용자 인증서의 일련 번호를 입력합니다. 예를 들어, 56100307215(이 문 서의 <u>인증 인증서</u> 섹션에 설명 참조
).

Gisco ASDM 6.0 for ASA - 192.168.	100.254	o do solo antinana ang ipang na ang ing ipang		hildi i Grenz par para mana		
File Wew Tools Wizards Window He	\$p			Look For:	Find +	ahaha
Home 🖧 Configuration 🗾 Monitoria	ng 🔚 Save 🔇	Refresh 🜔 Back 🜔 R	rward 🦿 Help			cisco
Device List 라우×	Configuration > R	emote Access VPH > AAA S	etup > Local Users			0
🕈 Add 📋 Delete 🖋 Connect	Create entries in	the ASA local user database.				
A 192.168.0.1	Constant and a			and the second reach		
- Childheathannaidh	Command autro	rización music de enabled in oro	er for die user account privie	ges to be enrorced. To enab	e commano autrionzación, go o	Transferrate
	AAA authentical	tion console commands must be	enabled in order for certain a	ccess restrictions to be enfo	rced. To enable AAA authentica	tion command
	go to Authentic	800.				
	Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
Remote Access VPN 🗗 🔍 🗙	enable_15	15	Full	N/A	N/A	
Application Helper	63041403325	6	rui -	- anex aroup Polcy	 In prioric Group Policy ** 	Eak
Single Signon Servers						Delete
Easy VPN Remote						ALCONTRACTOR IN
🗄 🚰 AAA Setup	1000					
AAA Server Groups						
Sig LDAP Attribute Map						
Secure Desktop Manager						
🗷 🛅 Certificate Management						
CHCP Server	2.2					
B R Advanced	199					
+5+ Connection Gateway 🛛 🗹	Sec. 1					
< >						
S. Device Setup						
Ø	35					
E Frewal	32					
Bemote Access VPN						
🙀 ste-to-Ste VPN						
Device Management						
			Apply	Reset		
Running configuration successfully saved to flash	h memory.		<adm< td=""><td>in> 15</td><td>🕼 🍘 🔰 🔂 2</td><td>5/07/07 0:22:25 UTC</td></adm<>	in> 15	🕼 🍘 🔰 🔂 2	5/07/07 0:22:25 UTC

4. Apply를 클릭합니다.

<u>10단계. ASA를 재부팅합니다.</u>

모든 변경 사항이 시스템 서비스에 적용되도록 ASA를 재부팅합니다.

<u>미세 조정</u>

테스트하는 동안 일부 SSL 터널이 제대로 닫히지 않을 수 있습니다. ASA는 AnyConnect 클라이언 트가 연결을 끊고 다시 연결할 수 있다고 가정하므로 터널이 삭제되지 않으므로 다시 돌아올 수 있 습니다. 그러나 기본 라이센스(기본적으로 2개의 SSL 터널)로 랩 테스트를 수행하는 동안 SSL 터 널이 제대로 닫히지 않으면 라이센스가 낭비될 수 있습니다. 이 문제가 발생하면 vpn-sessiondb logoff <*option*> 명령을 사용하여 모든 활성 SSL 세션을 로그오프합니다.

<u>1분 구성</u>

작업 컨피그레이션을 신속하게 생성하려면 ASA를 공장 기본값으로 재설정하고 컨피그레이션 모드에서 이 컨피그레이션을 붙여넣습니다.

ciscoasa
ciscoasa# conf t
ciscoasa# clear configure all
ciscoasa# domain-name cisco.be
ciscoasa# enable password 9jNfZuG3TC5tCVH0 encrypted
1

interface Vlan1 nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 interface Vlan2 nameif outside security-level 0 ip address 197.0.100.1 255.255.255.0 interface Ethernet0/0 switchport access vlan 2 no shutdown interface Ethernet0/1 no shutdown 1 passwd 2KFQnbNIdI.2KYOU encrypted dns server-group DefaultDNS domain-name cisco.be ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110 mask 255.255.255.0 asdm image disk0:/asdm-602.bin no asdm history enable global (outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 dynamic-access-policy-record DfltAccessPolicy http server enable http 192.168.0.0 255.255.255.0 inside crypto ca trustpoint ASDM_TrustPoint0 enrollment terminal crl configure crypto ca certificate map DefaultCertificateMap 10 issuer-name attr c eq be issuer-name attr cn eq citizen ca crypto ca certificate chain ASDM_TrustPoint0 certificate ca 580b056c5324dbb25057185ff9e5a650 30820394 3082027c a0030201 02021058 0b056c53 24dbb250 57185ff9 e5a65030 0d06092a 864886f7 0d010105 05003027 310b3009 06035504 06130242 45311830 16060355 0403130f 42656c67 69756d20 526f6f74 20434130 1e170d30 33303132 36323330 3030305a 170d3134 30313236 32333030 30305a30 27310b30 09060355 04061302 42453118 30160603 55040313 0f42656c 6769756d 20526f6f 74204341 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101 00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d c720eb30 915a75f5 e2d2cfc8 4c149842 58adc711 c540406a 5af97412 2787e99c e5714e22 2cd11218 aa305ea2 21b9d9bb fff674eb 3101e73b 7e580f91 164d7689 a8014fad 226670fa 4b1d95c1 3058eabc d965d89a b488eb49 4652dfd2 531576cb 145d1949 b16f6ad3 d3fdbcc2 2dec453f 093f58be fcd4ef00 8c813572 bff718ea 96627d2b 287f156c 63d2caca 7d05acc8 6d076d32 be68b805 40ae5498 563e66f1 30e8efc4 ab935e07 de328f12 74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf 6ce3841d de872e33 0b3c74e2 21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b a7210687 1d27d3c4 a1c94cb0 6f020301 0001a381 bb3081b8 300e0603 551d0f01 01ff0404 03020106 300f0603

551d1301 01ff0405 30030101 ff304206 03551d20 043b3039 30370605 60380101 01302e30 2c06082b 06010505 07020116 20687474 703a2f2f 7265706f 7369746f 72792e65 69642e62 656c6769 756d2e62 65301d06 03551d0e 04160414 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609 60864801 86f84201 01040403 02000730 1f060355 1d230418 30168014 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 300d0609 2a864886 f70d0101 05050003 82010100 c86d2251 8a61f80f 966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59 48a74c49 37d773a1 6a01655e 32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9 5d0f37ba 76d240bd cc2d3fd3 4441499c fd5b29f4 0223225b 711bbf58 d9284e2d 45f4dae7 b5634544 110d2a7f 337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1 60f2d787 f6572e7a 7e6a1380 1ddce3d0 631e3d71 31b160d4 9e08caab f094c748 755481f3 1bad779c e8b28fdb 83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636 ba218c97 1a21d4ea 2d3bacba eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297 fff26e87 7d46c974 d6efeb3d 7de6596e 069404e4 a2558738 286a225e e2be7412 b004432a quit no crypto isakmp nat-traversal dhcpd address 192.168.0.2-192.168.0.129 inside dhcpd enable inside dhcpd address 197.0.100.20-197.0.100.30 outside dhcpd enable outside ! service-policy global_policy global ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4sha1 ssl certificate-authentication interface outside port 443 webvpn enable outside svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 svc enable certificate-group-map DefaultCertificateMap 10 DefaultWEBVPNGroup group-policy DfltGrpPolicy attributes vpn-tunnel-protocol svc webvpn address-pools value eID-VPNPOOL username 63041403325 nopassword tunnel-group DefaultWEBVPNGroup general-attributes authentication-server-group (outside) LOCAL authorization-server-group LOCAL authorization-required authorization-dn-attributes SER tunnel-group DefaultWEBVPNGroup webvpn-attributes authentication certificate exit copy run start



- <u>Cisco PIX 방화벽 소프트웨어</u>
- Cisco Secure PIX Firewall 명령 참조
- <u>보안 제품 필드 알림(PIX 포함)</u>
- <u>RFC(Request for Comments)</u>
- <u>기술 지원 및 문서 Cisco Systems</u>