AAA & 인증서 인증을 사용하여 ASDM에서 보안 클라이언트 IKEv2/ASA 구성

목차

소개 <u>사전 요구 사항</u> 요구 사항 <u>사용되는 구성 요소</u> 네트워크 다이어그램 설정 ASDM의 컨피그레이션 <u>1단계. VPN 마법사 열기</u> 2단계. 연결 프로파일 식별 3단계. VPN 프로토콜 4단계. 클라이언트 이미지 <u>5단계. 인증 방법</u> <u>6단계. SAML 컨피그레이션</u> 7단계. 클라이언트 주소 할당 8단계. 네트워크 이름 확인 서버 <u>9단계. NAT 제외</u> 10단계. 보안 클라이언트 구축 <u>11단계. 설정 저장</u> 12단계. 보안 클라이언트 프로파일 확인 및 내보내기 13단계. 보안 클라이언트 프로파일 세부 정보 확인 <u>14단계. ASA CLI에서 설정 확인</u> 15단계. 암호화 알고리즘 추가 <u>Windows Server의 구성</u> ISE의 컨피그레이션 <u>1단계. 장치 추가</u> <u>2단계. Active Directory 추가</u> <u>3단계. ID 소스 시퀀스 추가</u> 4단계. 정책 집합 추가 5단계. 인증 정책 추가 6단계. 권한 부여 정책 추가 <u>다음을 확인합니다.</u> 1단계. Win10 PC1에 보안 클라이언트 프로필 복사 <u>2단계. VPN 연결 시작</u> <u>3단계. ASA의 Syslog 확인</u> 4단계. ASA에서 IPsec 세션 확인 5단계. Radius 라이브 로그 확인 문제 해결 <u>1단계. VPN 연결 시작</u> <u>2단계. CLI에서 Syslog 확인</u>

<u>참조</u>

소개

이 문서에서는 ASDM과 AAA 및 인증서 인증을 사용하여 ASA에서 IKEv2를 통한 보안 클라이언트 를 구성하는 데 필요한 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ・ Cisco ISE(Identity Services Engine) 구성
- Cisco ASAv(Adaptive Security Virtual Appliance) 컨피그레이션
- Cisco ASDM(Adaptive Security Device Manager) 구성
- VPN 인증 흐름

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Identity Services Engine Virtual 3.3 패치 1
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.

Windows Server 2016에 구성된 도메인 이름은 ad.rem-system.com이며 이 문서의 예제로 사용됩니다.



네트워크 다이어그램

설정

ASDM의 컨피그레이션

1단계. VPN 마법사 열기

Wizards(마법사) > VPN Wizards(VPN 마법사)로 이동하고 Secure Client VPN Wizard(보안 클라이 언트 VPN 마법사)를 클릭합니다.



Next(다음)를 클릭합니다.

Secure Client VPN Conne	ction Setup Wizard	×
Secure Client VPN Connect VPN Wizard	Introduction Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device when a VPN connection is established. VPN Remote Access	× ed
	< Back Next > 現初 Help	

Next(다음) 버튼 클릭

2단계. 연결 프로파일 식별

연결 프로파일에 대한 정보를 입력합니다. 연결 프로파일 이름: vpn-ipsec-tunnel-grp VPN 액세스 인터페이스: 외부

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Connection Profile Identification	
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN	
2. Connection Profile	connections.	
3. VPN Protocols	Connection Profile Name: vpn-ipsec-tunnel-grp	
4. Client Images	UTM Access TokerFaces	
5. Authentication Methods	VPN Access aren ace.	
6. SAML Configuration		
7. Client Address Assignme		
 Network Name Resolutio Servers 		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	< Back Next > It if Help	

연결 프로파일 식별

3단계. VPN 프로토콜

IPsec을 선택하고 Add(추가) 버튼을 클릭하여 새 자체 서명 인증서를 추가합니다.

Secure Client VPN Conn	ection Setup Wizard X	C Manage Identity Certificates
Steps	VPN Protocols	Terried To Terried By Evniry Date Associated Trustmonts Usane Dublic Ley Type Add
1. Introduction	Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you	Show hat ale
2. Connection Profile Identification	would like this connection profile to support.	Palata
3. VPN Protocols		u uesece
4. Client Images	IPsec	Export
5. Authentication Methods	Device Certificate	Install
5. SAML Configuration	Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IXEV2) require that valid device certificate be	Re-Enroll
8. Network Name Resolutio	available on the ASA.	
Servers	Device Certificate: None V Manage	
 NAT Exempt Secure Client Deployme 		
1. Summary		
		End: O O Match Case
		Certificate Expiration Alerts
		Send the first alert before : 60 (days) Set Default
	<back next=""> 現初 Help</back>	Repeat Alert Interval : 7 (days)
		Weak Crypto Configurations
		Permit Weak key sizes and Hash Algorithms
		Duble CA Foundment
		Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust
		offers Cisco customers a special promotional price for certificates and trial certificates for testing.
		Enroll ASA SSL certificate with Entrust
		Using a previously saved certificate signing request, enrol with Entrust.
		ASDM Identity Certificate Wizard
		The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.
		Launch ASDM Identity Certificate Wizard
		OK Cancel Help

자체 서명 인증서에 대한 정보를 입력합니다.

신뢰 지점 이름: vpn-ipsec-trustpoint

키 쌍: ipsec-kp

Ta Add Identity Certificate X	Ta Add Key Pair	×	
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: ORSA OECDSA OEDDSA		
Decryption Passphrase:	Name: Use default key pair name	_	
File to Import From: Browse O Add a new identity certificate:	Size: 4096		
Key Pair: ipsec-lip V Show New	Usage: O General purpose O Special		
Certificate Subject DN: CN=ciscoasa Select Generate self-signed certificate Act as local certificate authority and issue dynamic certificates to TLS-Proxy	Generate Now Cancel Help		
Advanced			
Enable CA flag in basic constraints extension			
Add Certificate Cancel Help			

자체 서명 인증서의 세부 정보

VPN 프로토콜의 설정을 확인하고 Next(다음) 버튼을 클릭합니다.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocol would like this connection profile to support. SSL Pervice Certificate Device Certificate Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/B:Ev2) require that valid device certificate be available on the ASA. Device Certificate Vpn-ipsec-trustpoint:unstructuredNamv Manage	you
	< Back Next > It in H	slp

VPN 프로토콜 설정 확인

4단계. 클라이언트 이미지

보안 클라이언트 이미지를 추가하려면 Add(추가) 버튼을 클릭하고 Next(다음) 버튼을 클릭합니다.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest Secure Client package to	the client device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a br You can also minimize connection setup time by moving the image	owser to an image. used by the most commonly encountered operation system to
3. VPN Protocols	the top of the list.	
4. Client Images	A	
5. Authentication Methods	Add Areplace Delete 7 +	
6. SAML Configuration	Image	Regular expression to match user-agent
7. Client Address Assignme	disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg	
8. Network Name Resolutio Servers		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	You can download Secure Client packages from Cisco by searchin	g 'Secure Mobility Client' or <u>click here</u> ,
	< gack Next >	Riff Help

클라이언트 이미지

5단계. 인증 방법

새 aaa 서버를 추가하려면 New 버튼을 클릭하고 Next 버튼을 클릭합니다.

서버 그룹 이름 : radius-grp

인증 프로토콜 : RADIUS

서버 IP 주소: 1.x.x.191

인터페이스 : 내부

Secure Client VPN Conn	ection Setup Wizard	×	The New Authentication Server Gr	roup	×	Secure Client VPN Conne	ection Setup Wized	×
Dawn 1. Drividution 2. Connection finalitie 2. Connection finalitie 3. Unit Protection 4. Carl Langest 5. Additional Restartion 1. Static Addition Antipole C. Static Conference S. Natt Compt 10. Secure Carl Deployment 11. Summary	Athetic score Heliode This cay but you you have hold from a three schemes proce- tions can do and the "Beam"- but to the scheme to the scheme scheme proce- Load there backees banks Date to Adder Parsword		Create a new authentication se To add more servers to the gr Corrigut adds - Device Manage Server Group Name: Authentication Protocol: Server IP Address: Interface:	erver group containing one authentication ser up or change other AdA server Group. reduce-grp RADEUS 1.::*.5.191 inside	rver. to	2015 1. Jerodatton 2. Connotion Publis Jeneficianon 3. URIV Intracia 4. Osel Tanges 5. Anthonica Alampine 6. Safet Configuration 7. Oser Address Alampine 8. Natos Alampi Pesukito Servers 9. Nat Compti 10. Server Centr Delayere 11. Sammary	Authoritation Methods This step ists up optify the location of the authoritation server. Two concide into the Security of the server grave. AAA form Grage Table The security of the securi	
	(b4) (b42) (b43)	Hib	Server Secret Key: Confirm Server Secret Key:	••••••			< gad get>	6
			OK	Cancel Help				

6단계. SAML 컨피그레이션

Next(다음) 버튼을 클릭합니다.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	SAML Configuration	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	This step allows you to configure a SAML and the authenticaion method. Authentication Method: AAA Server Group: radus-grp Manage Use LOCAL if Server Group fails SAML Identity Provider SAML Server : None Manage	
	< gack Next > Rin H	elp

SAML 컨피그레이션

7단계. 클라이언트 주소 할당

새 IPv4 풀을 추가하려면 New 버튼을 클릭하고 Next 버튼을 클릭합니다.

이름: vpn-ipsec-pool

시작 IP 주소: 172.16.1.20

종료 IP 주소: 172.16.1.30

서브넷 마스크: 255.255.255.0

Steps	Client Address Assignment		Steps	Client Address Assignment
Introduction Connection Profile Identification VPN Protocols VPN Protocols Configuration Configuration Configuration Configuration Configuration Configuration Configuration Notework Name Resolutio Servers NAT Exempt Secure Client Deployme Summary	This step allows you to create a new address pool or select an existr be asigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool Address Pool: Select V New Details of the selected address pool Stating IP Submet Mill	2 address pool for IP+4 and IP+6. The Secure Clerts will Pool X Address 172.16.1.20 - 172.16.1.20 - 172.16.1.30 - 0K Cancel Help	Introduction Connection Profile Identification VPN Protocols Clent Images Authentication Methods SAML Configuration Clent Address Assignment Notevork Name Resolutio Servers NAT Exempt Io. Secure Clent Deployme II. Summary	This step allows you to create a new address pool or select an existing address pool for IP-4 and IP-6. The Secure Clerks to be assigned addresses from the pools when they connect. IP-4 address pool is only supported for SSL connection.
	< Back Next >	Rcifi Help		<gack next=""> Rifl Help</gack>

클라이언트 주소 할당

8단계. 네트워크 이름 확인 서버

DNS 및 도메인에 대한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

DNS 서버: 1.x.x.57

도메인 이름: ad.rem-system.com

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Network Name Resolution Servers	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolution Servers NAT Exempt Secure Client Deployme Summary 	This step lets you specify how domain names are resolved for the remote user when accessing the internal network. DNS Servers: Domain Name: ad.rem-system.com	
	< gack Next > Ikin He	lp .

네트워크 이름 확인 서버

9단계. NAT 제외

Next(다음) 버튼을 클릭합니다.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	NAT Exempt	
I. Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme I. Summary	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
	< Back Next > 単初	Help

NAT 제외

10단계. 보안 클라이언트 구축

Allow Web Launch(웹 실행 허용)를 선택하고 Next(다음) 단추를 클릭합니다.

Secure Client VPN Conne	ction Setup Wizard X
Steps	Secure Client Deployment
1. Introduction	Secure Client program can be installed to a client device by one of the following two methods:
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed; Pre-deployment - Manually install the Secure Client package.
3. VPN Protocols	
4. Client Images	
5. Authentication Methods	Allow Web Launch
6. SAML Configuration	Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will
7. Client Address Assignme	NUT WORK FIELS CARREND OFF.
8. Network Name Resolutio Servers	For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA
9. NAT Exempt	in your Secure Client package, otherwise IPsec connection will NOT work.
10. Secure Client Deployment	
11. Summary	
	< gack Next > Rifl Help

11단계. 설정 저장

Finish(마침) 버튼을 클릭하고 설정을 저장합니다.



설정 저장

12단계. 보안 클라이언트 프로파일 확인 및 내보내기

Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Client Profile(보안 클라이언트 프로파일)로 이동하 고 Edit(편집) 버튼을 클릭합니다.

File View Iools Wigards Window Help	e 💽 Refresh 🔇 Back 💭 Forward 🦻 Help			Type topic to search Go	cisco
Device List Boolmarks	Configuration > Remote Access VPN > Network (Client) Acce	ess > Secure Client Profile			
Boolmarks and a page, right-click on a node in the navigation tree and select: "Add to boolemarks". Go Go Toelete	This panel is used to manage Secure Client Profiles and perform gro upload and download of client profiles between local machine and do The profile Usage field is introduced with the Secure Mobility Solutio	up assignment for Secure Client version 2.5 or later. You can select a pr evice. n. This field contains different profile usage in Secure Client version 3.0	offe to edit, change group or to delete. You can select the 'Add' butto and later.	in to add a new profile. Pressing the Import or Export bu	tton is for
Remote Access VPN 🗗 🖗	🗣 Adc 📝 Edit 🔀 Change Group Policy 📋 Delete 🛃 Impor	t 🖏 Export 🔊 Valdate			
Introduction Introduction Introduction Introduction	Profile Name	Profile Usage	Group Policy	Profile Location	
Secure Clent Connection Profiles Secure Clent Customization(Localization Secure Clent Profile Secure Clent Software	von-ipsec-tunnel-grp_clent_profile	AnyConnect VPN Profile	GroupPolicy_upn-ipsec-tunnel-grp	disk0;/vpn-ipsec-tunnel-grp_client_profile.xml	

보안 클라이언트 프로파일 편집

프로필의 세부사항을 확인합니다.

- 표시 이름(필수): ciscoasa (IPsec) IPv4
- FQDN 또는 IP 주소: 192.168.1.1
- 기본 프로토콜: IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	p_client_profile					Server List Entry					×
Profile: vpn-ipsec-tunne	l-grp_client_pr	rofile					Primary Server	gServers SCIP M	ble Certificate Pinning	Connection Information	n	
- (3) Preferences (Part 1) 	Gerrer List						Display Name (r	equired) [ciscolese (Psec) Pv4	Primary Protocol	Рис 🗸	
- Centricate Priving - Centricate Matching	Hostname	Host Address	User Group	Backup Server List	SCEP	Noble Setting	FQDN or IP Add	-	User Group	ASA gateway		
Muble Polcy Server Lat							192.168.1.1	1	1	B II Identity (305	ing D.E. Negotiation	[LAP-AnyConnect. ~
							Group CPL					
	Note: it is highly i	recommended that at	least one server be	defined in a profile.		udd		Backup Servers				
						LOK-IN		Host Address			Add	
											Move Down	
											Delete	
									l			
									OK	Cancel		

보안 클라이언트 프로파일 확인

프로필을 로컬 PC로 내보내려면 Export(내보내기) 버튼을 클릭합니다.



보안 클라이언트 프로파일 내보내기

13단계. 보안 클라이언트 프로파일 세부 정보 확인

Secure Client Profile by browser(브라우저별 보안 클라이언트 프로파일)를 열고 호스트의 기본 프 로토콜이 IPsec인지 확인합니다.

```
\u00ed 
\u00ed <
```

보안 클라이언트 프로파일 세부 정보

14단계. ASA CLI에서 설정 확인

ASA CLI에서 ASDM에 의해 생성된 IPsec 설정을 확인합니다.

// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0

// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5

// Define the transform sets that IKEv2 can use crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES192 protocol esp encryption aes-192 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal 3DES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal DES protocol esp encryption aes protocol esp integrity sha-256 sha-1

```
// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
```

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
crl configure

// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b

ac76f984 efd41d13 073d0be6 f923a9c6 7b quit

// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10

encryption aes-192 integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 20 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 40 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 // Enabling client-services on the outside interface crypto ikev2 enable outside client-services port 443 // Specifiies the certificate the ASA uses for IKEv2 crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint // Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside enable anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml anyconnect enable tunnel-group-list enable // Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes wins-server none dns-server value 1.x.x.57 vpn-tunnel-protocol ikev2 default-domain value ad.rem-system.com webvpn anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user // Ties the pool of addressess to the vpn connection tunnel-group vpn-ipsec-tunnel-grp type remote-access tunnel-group vpn-ipsec-tunnel-grp general-attributes address-pool vpn-ipsec-pool authentication-server-group radius-grp default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes group-alias vpn-ipsec-tunnel-grp enable

15단계. 암호화 알고리즘 추가

ASA CLI에서 IKEv2 정책에 그룹 19를 추가합니다.



참고: IKEv2/IPsec 연결의 경우 Cisco Secure Client는 버전 4.9.00086부터 DH(Diffie-Hellman) 그룹 2, 5, 14, 24를 더 이상 지원하지 않습니다. 이러한 변경으로 인해 암호화 알 고리즘 불일치로 인해 연결 실패가 발생할 수 있습니다.

ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#

Windows Server의 구성

VPN 연결을 위해 도메인 사용자를 추가해야 합니다. Active Directory 사용자 및 컴퓨터로 이동한 다음 사용자를 클릭합니다. vpnuser를 도메인 사용자로 추가합니다.

? X t for administering the computer/domain s group can have their passwords replicat s group are permitted to publish certificat s group are permitted to publish certificat s group cannot have their passwords replicat s group cannot have their passwords replicat s group cannot have their passwords replicat s group cannot have their passwords replication o are permitted to perform dynamic upd ninistrators of the domain s and servers joined to the domain trollers in the domain sts s group can perform administrative action s group can access remote access properties s group are Read-Only Domain Controlla ninistrators of the schema	in ted to the to be cl dicate lates o ers in t domain ain ons on ers in t
	? × Sessions s group can have their passwords replicated s group are permitted to publish certific s group that are domain controlliers may managed by the system. s group cannot have their passwords replaced to perform dynamic upd ninistrators of the domain trollers in the domain trollers in the domain states in the domain states in the domain states in the domain states in the domain diministrative actives group can perform administrative actives group can access remote access properties s group are Read-Only Domain Controllent inistrators of the schema Help

```
도메인 사용자 추가
```

Domain Admins 및 Domain Users의 구성원에 도메인 사용자를 추가합니다.

on user Properties				?	\times	vpn user Pr	operties				?	×
Remote control	Remote I	Desktop Services I	Profile	CO	M+	Remote	control	Remote	Desktop S	ervices Profile	CO	M+
Member Of	Dial-in	Environmen	t	Sessio	ns	General	Address	Account	Profile	Telephones	Organiz	zation
General Address	Account	Profile Teles	phones	Organi	zation	Membe	er Of	Dial-in	En	vironment	Session	ns
User logon name:						Member of	of:					
vpnuser		@ad.rem-syste	m.com		\sim	Name		Active Direct	tory Domai	n Services Folde		٦
User logon name (pre-)	Windows 200	0):				Domain	Admins	ad.rem-syste	m.com/Us	ers		
AD\		vpnuser				Domain	Users	ad.rem-syste	m.com/Us	ers		
Account gotions:	je password a inge passwori expires using reversib	at next logon d le encryption			~	Add Primary g	roup: D	Remove Iomain Users There is r	no need to	change Primary	aroup unle	
Never End of:	Monday ,	June 10, 202	4]	<u>S</u> et Pr	mary Group	you have application	Macintosi ons.	h clients or POSI	(-complian	t
0												

도메인 관리자 및 도메인 사용자

ISE의 컨피그레이션

1단계. 장치 추가

Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)button을 클릭 하여 ASAv 디바이스를 추가합니다.

Network Devices	Network Device Grou	ps Network D	evice Profiles	External RADIU	JS Servers	RADIUS Server Sequences
Network Devices Default Device Device Security Settings	Network Network Name Descr	Devices List > ASAv ork Devices ASAv iption				
	IP	Address 🗸 * IP :	1,070,061	/ 32 @)	
	Devic	e Profile 🗰 Cisco		× 0		
	Mode	I Name		~		
	Softw	are Version		~		
	Netwo	ork Device Group				
	Locat	ion All Locat	tions	~	Set To Defau	it
	IPSEC	No		~	Set To Defau	lt
	Devic	e Type All Devic	e Types	~	Set To Defau	ilt
		RADIUS Au	thentication Se	ettings		
		RADIUS UDP S	ettings			
		Protocol	RADIUS			
		Shared Secret	cisco123		Hid	e

장치 추가

2단계. Active Directory 추가

Administration(관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동하고 Connectiontab(연결 탭)을 클릭한 다음 Active Directory를 ISE에 추가합니다.

- 조인 지점 이름: AD_Join_Point
- Active Directory 도메인: ad.rem-system.com



Active Directory 추가

그룹 탭으로 이동하여 디렉터리에서 그룹 선택 드롭다운 목록을 선택합니다.디렉터리에서 그룹

=	dentity Services	s Engine Administration / identity Management
j.	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
1 ¹ 2	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
. %	Operations	Cartificate Authenticat
	Policy	C Active Directory
<u> </u>	O Administration	AD_Join_Point 🗋 Add Group Control Assist ad.rem-system.com/S-1-5-32-579
_ 선택협	합니다	

그룹 검색(Retrieve Groups)시작(From) 드롭다운 목록을 누릅니다. Checkad.rem-

system.com/Users/Domain Computersandad.rem-system.com/Users/Domain 사용자를 클릭한 다 음 OK를 클릭합니다.

≡		Engine		×	🔺 Evolus
н	Bookmarks	Identities Groups E	Select Directory Groups This dialog is used to select groups from the Directory.		
52	Dashboard	Active Directo	Dormain ad rem-system.com		
넝	Context Visibility	AD_Join_Poin	Name SID Type ALL		
*	Operations	C LDAP			
0	Policy	COBC	Remeve Groups		
10	Administration	C RADIUS Token	Name Group SID Group Type		
3	Work Centers	SAM IN Provide	ad rem-system.com/Users/DisAdmins 5-1-5-21-4193742415-4133520028-20462399 DOMAIN LOCAL	•	
-		Social Login	ad.rem-system.com/Users/DnsUpdateProxy 5-1-5-21-4193742415-8133520026-20462399 GLOBAL		
(3)	Interactive Male		ad.rem-system.com/Users/Domain Admins S-1-5-21-4193742415-4133520026-20462399 GLOBAL		
6	interactive help		ad /em-system.com/Users/Domain Computers 5-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			ad./em-system.com/Users/Domain Controllers 5+1+5+21+4193742415+4133520026+20462399 GLOBAL		
			ad.rem-system.com/Users/Domain Guests 5-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			ad.rem-system.com/Users/Domain Users 5-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			ad.rem-system.com/Usersi@nterprise.Admins 5-1-5-21-4193742415-4133520026-20462399 UNIV@ASAL		
			ad.rem-system.com/Users/Enterprise Key Admins 5-1-5-21-4193742415-4133520026-20462399 UNIVERSAL		
			ad.rem-system.com/Users/Enterprise Read-only 5-1-5-21-4193742415-4133520026-20462399 UNIVERSAL		
			ad.rem-system.com/Users/Group Policy Creator 5-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			<		
			Cancel	×	

도메인 컴퓨터 및 사용자 추가

3단계. ID 소스 시퀀스 추가

Administration(관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동하여 ID 소스 시퀀스를

추가합니다.

- 이름: Identity_AD
- 인증 검색 목록: AD_Join_Point

≡	alada Identity Services I	Engine		Administration / Id	dentity Management
н	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
55	Dashboard	Identity Source Sequences	List > Identity_AD		
명	Context Visibility	Identity Source Se	quence		
*	Operations				
-0	Policy	 Identity Source Name 	Sequence		
a 0	Administration	lde	entity_AD		
d.	Work Centers	Description			
?	Interactive Help	✓ Certificate Bas ☐ Select Certifica	sed Authentication	~	
		Authentication	Search List		
		A set of identi	ity sources that will be accessed	in sequence until first authentication s	ucceeds
		Available		Selected	
		Internal En	idpoints ^	AD_Join_Point ^	
		Internal Us Guest Lise	iers		
		All_AD_Jo	in_Points		2
				č	
			>	E E	
					<u>-</u>

ID 소스 시퀀스 추가

4단계. 정책 집합 추가

Policy(정책) > Policy Sets(정책 세트)로 이동하고 +를 클릭하여 정책 세트를 추가합니다.

- 정책 집합 이름: VPN_Test
- 조건: 장치 장치 유형이 모든 장치 유형과 같음
- 허용되는 프로토콜/서버 시퀀스: 기본 네트워크 액세스

≡	dentity Services Engi	ne	Policy / Policy Set	s	🔺 Evaluatio	an Mode 🖬 Days 🛛 Q	۵	0 🗘	A
Щ	Bookmarks	Policy Sets			Reset	Reset Policyset Hit	counts	Sav	re -
51	Dashboard	+ Status Policy Set Name	Description	Conditions	Allowed Protocols	Server Sequence	Hits A	ctions V	iew
15	Context Visibility	Q Search							
×	Operations	VPN Test		DEVICE-Device Type EQUALS All	Default Network Ac	cess 🦯 🔟	30	ń.	
0	Policy	V N _a tur	L	Device Types				1%r	

정책 집합 추가

5단계. 인증 정책 추가

Policy Sets(정책 집합)로 이동하고 VPN_Test를 클릭하여 인증 정책을 추가합니다.

- 규칙 이름: VPN_Authentication
- 조건: 네트워크 액세스 디바이스 IP 주소가 1.x.x.61과 같음
- 사용: Identity_AD

∨Authentication Policy(2)				
🕂 Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
		Identity_AD		
VPN_Authentication	Retwork Access-Device IP Address EQUALS 1.171.1.61	> Options	10	\$ <u>\$</u>
인증 정책 추가				

6단계. 권한 부여 정책 추가

Policy Sets(정책 집합)로 이동하고 VPN_Test를 클릭하여 권한 부여 정책을 추가합니다.

- 규칙 이름: VPN_Authorization
- 조건: Network_Access_Authentication_Passed
- 결과: PermitAccess

∨Authorization Policy(2)						
		Results				
(+) Status Rule Name	Conditions	Profiles	Security Groups		Hits	Actions
Q Search						
VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	0+	10	ŝ
권한 부여 정책 추가						

다음을 확인합니다.

1단계. Win10 PC1에 보안 클라이언트 프로필 복사

보안 클라이언트 프로파일을 C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile 디렉토리에 복사합니다.



2단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client를 실행하고 사용자 이름과 비밀번호를 입력한 다음 Cisco Secure Client가 성공적으로 연결되었는지 확인합니다.

Sisco Secure Client – 🗆 🗙	S Cisco Secure Client ciscoasa (IPsec) IPv4 X	S Cisco Secure Client − □ ×
AnyConnect VPI: Please enter your username and password. ciscoasa (IPsec) IPv4 < Connect	Please enter your username and password. Group: vpn-ipsec-tunnel-grp Username: vpnuser	AnyConnect VPI: Connected to discoasa (IPsec) IPv4. discoasa (IPsec) IPv4 V Disconnect
	Password:	00:00:05 IPv4
	OK Cancel	

연결 성공

3단계. ASA의 Syslog 확인

syslog에서 IKEv2 연결이 성공했는지 확인합니다.

<#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
New Connection Established
```

```
May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

4단계. ASA에서 IPsec 세션 확인

run show vpn-sessiondb detail anyconnect 명령을 사용하여 ASA의 IKEv2/IPsec 세션을 확인합니다.

<#root>

ciscoasa#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnuser Index : 23 Assigned IP : 172.16.1.20 Public IP : 192.168.1.11 Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent License : AnyConnect Premium Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp Tunnel Group : vpn-ipsec-tunnel-grp Login Time : 08:13:20 UTC Tue May 28 2024 Duration : 0h:10m:10s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 01aa003d0001700066559220 Security Grp : none IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 AnyConnect-Parent Tunnels: 1 AnyConnect-Parent: Tunnel ID : 23.1 Public IP : 192.168.1.11 Encryption : none Hashing : none Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : 5.1.3.62 IKEv2: Tunnel ID : 23.2 UDP Src Port : 50982 UDP Dst Port : 4500 Rem Auth Mode: userPassword Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA256 Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds PRF : SHA256 D/H Group : 19 Filter Name : Client OS : Windows Client Type : AnyConnect IPsecOverNatT: Tunnel ID : 23.3 Local Addr : 0.0.0.0/0.0.0.0/0/0 Remote Addr : 172.16.1.20/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA256 Encapsulation: Tunnel Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307

5단계. Radius 라이브 로그 확인

ISE GUI에서 Operations(운영) > RADIUS > Live Log(라이브 로그)로 이동하여 vpn 인증을 위한 라이브 로그를 확인합니다.

=	ence Identity Services Engine					Operations / RADIUS						A ***	duation Mode 💭 Days	۵ ۵	0	4 ۹
н	Bookmarks	Live Logs Live Sessions														
	Dashboard															
N	Context Visibility	Misconfigured Supplicants	Miss	configured Ne	twork Device	es 😳	RADIUS Drops 🕓		Client Stopped Responding 📀			Repeat Counter 💿				
*	Operations	0			0				0		0			0		
Ð	Policy											Defresh	Show		Victor	
2.	Administration											Never	V Latest 20 re	cords 🗸	Last 3 ho	urs v
ส์เ	Work Centers	C for Reset Repeat Counts	₫ Export To ∨												Filter 🗸	۰
		Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Por	t Ider	ntity Grou
	Interactive Help	×				Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	V Network Devic	Device Port	Ider	sity Group
		May 28, 2024 05:13:42	•	ō.	0	00.50.5	vpruser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess					
		May 28, 2024 05:13:42	•	0		00:50:5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		World	station

Radius 라이브 로그

Status(상태)를 클릭하여 라이브 로그의 세부사항을 확인합니다.

	Cisco ISE				
,					
	Overview		Steps		
	Event	5200 Authentication succeeded	Step ID 11001	Description Received RADIUS Access-Request	Latency (ms)
	Username	vpnuser	11017	RADIUS created a new session	1
	Endpoint Id	00:50:56:98:77:A4 ⊕	15049	Evaluating Policy Group	36
	Endpoint Profile	Windows 10-Workstation	15008	Evaluating Service Selection Policy	1
	Endpoint Prome	WIRdows I C-WORkstation	15048	Queried PIP - DEVICE.Device Type	6
	Authentication Policy	VPN_Test >> VPN_Authentication	15041	Evaluating Identity Policy	20
	Authorization Policy	VPN_Test >> VPN_Authorization	15048	Queried PIP - Network Access.Device IP Address	2
	Authorization Result	PermitAccess	22072	Selected identity source sequence - Identity_AD	6
			15013	Selected Identity Source - AD_Join_Point	1
			24430	Authenticating user against Active Directory - AD_Join_Point	4
	Authentication Details		24325	Resolving identity - vpnuser	38
	Source Timestamp	2024-05-28 17:13:42.897	24313	Search for matching accounts at join point - ad.rem- system.com	0
	Received Timestamp	2024-05-28 17:13:42.897	24319	Single matching account found in forest - ad.rem- system.com	0
	Policy Server	ise33-01	24323	Identity resolution detected single matching account	0
	Event	5200 Authentication succeeded	24343	RPC Logon request succeeded - vpnuser@ad.rem- system.com	23
	Username	vpnuser	24402	User authentication against Active Directory succeeded - AD_Join_Point	3
	Enapoint la	00.50.56.96.77.44	22037	Authentication Passed	1
	Calling Station Id	192.168.1.11	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
	Endpoint Profile	windows10-workstation	15036	Evaluating Authorization Policy	1
	Authentication Identity	AD_Join_Point	24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
	3000		24211	Found Endpoint in Internal Endpoints IDStore	9
	Identity Group	Workstation	15048	Queried PIP - Network Access.AuthenticationStatus	2
	Audit Session Id	01aa003d0001700066559220	15016	Selected Authorization Profile - PermitAccess	7
	Authentication Method	PAP_ASCII	22081	Max sessions policy passed	6
			22080	New accounting session created in Session cache	0
	Authentication Protocol	PAP_ASCII	11002	Returned RADIUS Access-Accept	2
	Network Device	ASAv			

라이브 로그 세부 정보

문제 해결

암호화 알고리즘이 일치하지 않으면 연결 오류가 발생할 수 있습니다. 알고리즘 불일치 문제가 발생하는 경우의 예입니다. ASDM에 서 섹션 구성의 15단계를 실행하면 문제가 해결될 수 있습니다.

1단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client를 실행하고 암호화 알고리즘 불일치로 인해 연결이 실패했음을 확인합니다.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.

Sisco Secure Client			×	Cisco Secure Client		
AnyConnect VPN: Ready to connect.	~	Connect		The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.		
				OK		

연결 실패

2단계. CLI에서 Syslog 확인

syslog에서 IKEv2 협상이 실패했음을 확인합니다.

<#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERI

Failed to find a matching policy

참조

AAA 및 인증서 인증을 사용하여 ASA에 AnyConnect Over IKEv2

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.