ISE Posture를 사용하여 Duo SAML SSO를 Anyconnect Secure Remote Access와 통합

목차
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>구성</u>
<u>네트워크 다이어그램</u>
<u>트래픽 흐름</u>
<u>설정</u>
<u>- Duo 관리 포털 컨피그레이션</u>
<u>- DAG(Duo Access Gateway) 컨피그레이션</u>
<u>- ASA 컨피그레이션</u>
<u>-ISE 구성</u>
<u>다음을 확인합니다.</u>
<u>사용자 환경</u>
<u>문제 해결</u>
관련 정보

소개

이 문서에서는 자세한 상태 평가를 위해 Cisco ISE를 활용하는 Adaptive Security Appliance(ASA) Cisco AnyConnect Secure Mobility Client 액세스와 Duo SAML SSO를 통합하는 컨피그레이션 예 를 설명합니다. Duo SAML SSO는 초기 사용자 인증을 위해 Active Directory와 통신한 다음 다단계 인증을 위해 Duo Security(클라우드)와 통신하는 Duo DAG(Access Gateway)를 사용하여 구현됩니 다. Cisco ISE는 상태 평가를 사 항목으로 엔드 포인트 확인을 제공 하는 인증 서버로 사용 됩니다.

기고자: Dinesh Moudgil 및 Pulkit Saxena, Cisco HTTS 엔지니어

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동하며 Cisco ASDM(Adaptive Security Device Manager) 또는 CLI(Command Line Interface)에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Duo 액세스 게이트웨이 및 Duo 보안의 기초
- ASA의 원격 액세스 VPN 구성에 대한 기본 지식
- ISE 및 상태 서비스에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance 소프트웨어 버전 9.12(3)12
- Duo 액세스 게이트웨이
- Duo Security
- Cisco Identity Services Engine 버전 2.6 이상
- Microsoft Windows 10(AnyConnect 버전 4.8.03052)

✤ 참고: 이 구현에서 사용되는 Anyconnect Embedded Browser에는 각 릴리스의 9.7(1)24, 9.8(2)28, 9.9(2)1 이상 버전 및 AnyConnect 버전 4.6 이상에서 ASA가 필요합니다.

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.

구성

네트워크 다이어그램



트래픽 흐름

- 1. Anyconnect 클라이언트가 Cisco ASA에 대한 SSL VPN 연결을 시작합니다.
- 2. DAG(Duo Access Gateway)를 사용하는 기본 인증용으로 구성된 Cisco ASA는 SAML 인증을 위해 Anyconnect 클라이언트에 포함된 브라우저를 DAG로 리디렉션합니다
- 3. Anyconnect 클라이언트가 Duo 액세스 게이트웨이로 리디렉션됨
- 4. AnyConnect 클라이언트가 자격 증명을 입력하면 SAML 인증 요청이 생성되고 Cisco ASA에 서 Duo Access Gateway로 발급됩니다
- 5. Duo Access Gateway는 온사이트 active directory와의 통합을 활용하여 Anyconnect 클라이 언트에 대한 기본 인증을 수행합니다
- 6. 1차 인증에 성공하면 Duo Access Gateway가 TCP 포트 443을 통해 Duo Security에 요청을 보내 2단계 인증을 시작합니다
- 7. AnyConnect 클라이언트는 "Duo Interactive Prompt"를 제공했으며 사용자는 선호하는 방법 (푸시 또는 패스코드)을 사용하여 Duo 2단계 인증을 완료합니다
- 8. Duo Security가 인증 응답을 수신하고 이 정보를 Duo Access Gateway에 반환합니다.
- 9. Duo Access Gateway는 인증 응답을 기반으로 SAML 어설션을 포함하고 Anyconnect 클라이 언트에 응답하는 SAML 인증 응답을 작성합니다
- 10. Anyconnect 클라이언트가 Cisco ASA와의 SSL VPN 연결을 성공적으로 인증함
- 11. 인증에 성공하면 Cisco ASA는 Cisco ISE에 권한 부여 요청을 보냅니다

참고: Cisco ISE는 Duo Access Gateway에서 필요한 인증을 제공하므로 권한 부여용으로만 구성됩니다

- 12. Cisco ISE는 권한 부여 요청을 처리하며 클라이언트 상태 상태가 알 수 없음이므로 Cisco ASA를 통해 Anyconnect 클라이언트에 대한 제한된 액세스로 상태 리디렉션을 반환합니다
- 13. Anyconnect 클라이언트에 규정 준수 모듈이 없는 경우 상태 평가를 더 진행하려면 해당 모듈 을 다운로드하라는 메시지가 표시됩니다
- 14. Anyconnect 클라이언트에 규정 준수 모듈이 있는 경우, Cisco ASA와의 TLS 연결을 설정하고 포스처 플로우를 시작합니다
- 15. ISE에 구성된 포스처 조건에 따라 포스처 확인이 수행되고 Anyconnect 클라이언트에서 Cisco ISE로 세부 정보가 전송됩니다
- 16. 클라이언트 포스처 상태가 알 수 없음에서 규정준수로 변경되면 CoA(change of

authorization) 요청이 Cisco ISE에서 Cisco ASA로 전송되어 클라이언트에 대한 전체 액세스 권한을 부여하고 VPN이 완전히 설정됩니다

설정

- Duo 관리 포털 컨피그레이션

이 섹션에서는 Duo 관리 포털에서 ASA 애플리케이션을 구성합니다.

1. "Duo Admin Portal(Duo 관리 포털)"에 로그인하고 "Applications(애플리케이션) > Protect an Application(애플리케이션 보호)"으로 이동하여 보호 유형이 "2FA with Duo Access Gateway, self-hosted"인 "ASA"를 검색합니다. Cisco ASA를 구성하려면 맨 오른쪽에 있는 "보호"를 클릭합니다.

Ĥ	admin-77d04ebc.duosecurity.com/a	applications/protect/types				☆	
vlisc	🗎 Cisco Study 🗎 Cisco Tools 🗎	Mix 🖹 SourceFire 🗎 VPN 🗎 AAA 🗎 ASA 🗎] IFT 6.7				
	DUO	${\bf Q}_{\rm c}$ Search for users, groups, applications, or devices		Ø	Cisco ID: 2010-1403-48	ciscoduoblr	~
	Dashboard	Dashboard > Applications > Protect an Application					
	Device Insight	Protect an Application					
	Policies	Protect an Application					٦
	Applications	ASA					J
	Protect an Application	Application	2FA	Single Sign-On (if available)	Documentation	Action	
	Single Sign-On						
	Users	asana Asana	2FA	Duo Access Gateway (self-hosted)	Documentation 🗗	Protect	
	Groups						
	Endpoints	Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation C	Protect	ר
	2FA Devices	cisco)		
	Administrators						
	Reports	CISCO Cisco ASA	2FA	Single Sign-On (hosted by Duo)	Documentation 🗗	Configure	9

2. 보호된 응용 프로그램, ASA의 "서비스 공급자"에서 다음 특성을 구성합니다

기본 URL	firebird.cisco.com
터널 그룹	TG_SAML
메일 특성	AMAccountName,메일

페이지 하단의 "Save(저장)"를 클릭합니다.

Device Insight Policies	Cisco ASA - Duo Access Gateway				
Applications Protect an Application	Configure Cisco ASA To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions C' Next step: Download your configuration file				
Single Sign-On Users					
Groups Endpoints	Service Provider				
2FA Devices Administrators Reports	Base URL	firebird.cisco.com			
Settings Billing	Tunnel Group	TG_SAML Enter the Tunnel Group you are protecting with SSO.			
Need Help? Chat with Tech Support C Email Support Call us at 1-855-386-2884	Custom attributes	Vse this setting if your Duo Access Gateway authentication source uses non-standard attribute names.			
Account ID 2010-1403-48 Deployment ID	Mail attribute	sAMAccountName,mail The attribute containing the email address of the user.			
DU057 C Helpful Links Documentation C		Save Configuration			

이 문서의 나머지 구성에서는 기본 매개변수를 사용하지만 고객의 요구 사항에 따라 설정할 수 있 습니다.

애플리케이션 이름을 기본값에서 변경하거나 셀프 서비스를 활성화하거나 그룹 정책을 할당하는 등 현재 새 SAML 애플리케이션에 대해 추가 설정을 조정할 수 있습니다.

3. "구성 파일 다운로드" 링크를 클릭하여 Cisco ASA 애플리케이션 설정(JSON 파일)을 확인합니다 . 이 파일은 이후 단계에서 Duo Access Gateway에 업로드됩니다

Device Insight Policies	Cisco ASA - Duo Access Gateway Authentication Log Bernove Application			
Applications Protect an Application	Configure Cisco ASA			
Single Sign-On Users	To set up this application, ins Next step: <mark>Download your co</mark>	tall the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions 답 nfiguration file		
Groups Endpoints	Service Provider			
2FA Devices Administrators	Base URL	firebird.cisco.com		
Reports Settings Billing	Tunnel Group	TG_SAML		
Need Help? Chat with Tech Support 더 Email Support	Custom attributes	Enter the Tunnel Group you are protecting with SSO.		
Call us at 1-855-386-2884 Account ID 2010-1403-48	Mail attribute	SAMAccountName,mail		
Deployment ID DU057 C Helpful Links Documentation C		Save Configuration		

4. "Dashboard(대시보드) > Applications(애플리케이션)"에서 새로 생성된 ASA 애플리케이션은 아 래 이미지와 같습니다.

admin-77d04ebc.duosecurity.com/applications 🚖 📅					
🗎 Cisco Study 📋 Cisco Tools	Mix SourceFire VPN AAA	🗎 ASA 📋 IFT 6.7			
DUO	A Search for users, groups, applications,	or devices		Cisco ID: 2010-1403-48 ciscoduobir ~	
Dashboard	Dashboard > Applications				
Device Insight	Annlingtions				
Policies	Applications			SSO Setup Guide Protect an Application	
Applications					
Protect an Application				Export V Search	
Single Sign-On					
Users	Name 🔺	Туре	Application Policy	Group Policies	
Groups	Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway			
Endpoints					
2FA Devices	1 total				

5. 이미지에 표시된 대로 "사용자 > 사용자 추가"로 이동합니다.

Anyconnect Remote Access 인증에 사용할 "duouser"라는 사용자를 생성하고 최종 사용자 디바이 스에서 Duo Mobile을 활성화합니다.



이미지에 표시된 대로 전화 번호를 추가하려면 "Add Phone(전화 추가)" 옵션을 선택합니다.



특정 사용자를 위해 "Duo Mobile" 활성화

Device Info

Learn more about Activating Duo Mobile 2.



Not using Duo Mobile Activate Duo Mobile



Model Unknown



OS Generic Smartphone

✤ 참고: 최종 사용자 장치에 "Duo Mobile"이 설치되어 있어야 합니다. IOS 디바이스용 Duo 애플리케이션 수동 설치 Android 디바이스용 Duo 애플리케이션의 수동 설치

이미지에 표시된 대로 "Generate Duo Mobile Activation Code(듀오 모바일 활성화 코드 생성)"를 선 택합니다.

	Q. Search for users, groups, applications, or devices Cisco ID: 2010-1403-48 ciscoduoblr ~
Deshboard	
Dasiboard	Dashboard > Phone: Activate Duo Mobile
Device Insight	Activate Duo Mobile
Policies	
Applications	This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their making during or authenticate via Duo Pueh
Users	mobile device or authenticate via Duo Push.
Groups	Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.
Endpoints	Phone Contraction Contraction
2FA Devices	
Phones	Expiration 24 bours v after generation
Hardware Tokens	
WebAuthn & U2F	
Administrators	Generate Duo Mobile Activation Code
Reports	
Settings	

이미지에 표시된 대로 "Send Instructions by SMS(SMS로 지침 보내기)"를 선택합니다.

Dashboard	Dashboard > Phone: +91	> Activate Duo Mobile
Device Insight	Activate Du	a Mabila
Policies	Activate Du	
Applications	A new Duo Mobile activatio	n code has been generated, and any old credentials have been invalidated.
Users	activation instructions to th	e user by SMS.
Groups	Phone	
Endpoints		
2FA Devices	Installation instructions	Send installation instructions via SMS
Phones		Welcome to Duo! Please install Duo Mobile from your app
Hardware Tokens		store.
WebAuthn & U2F		
Administrators		h.
Reports	Activation instructions	Sand activation instructions via SMS
Settings	Activation instructions	
Billing		To activate the app, tap and open this link with Duo Mobile: https://m-
		77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT
Need Help? Chat with Tech Support 다		h
Email Support		
Call us at 1-855-386-2884		Send Instructions by SMS pr skip this step

SMS에서 링크를 클릭하면 Duo 앱이 그림과 같이 Device Info(디바이스 정보) 섹션의 사용자 계정 에 연결됩니다.



- DAG(Duo Access Gateway) 컨피그레이션

1. 네트워크의 서버에 DAG(Duo Access Gateway) 구축

참고: 배포에 대해서는 아래 문서를 따르십시오.

Linux용 Duo 액세스 게이트웨이 https://duo.com/docs/dag-linux

Duo Access Gateway for Windows https://duo.com/docs/dag-windows

- 2. Duo Access Gateway 홈 페이지에서 "Authentication Source"로 이동합니다.
- 3. "소스 구성"에서 Active Directory에 대한 다음 특성을 입력하고 "설정 저장"을 클릭합니다.

Configure Sources

nfigure authentication	source settings below. Changes made to non-active authentication sources will take effect when made active.
Source type	Active Directory Specify the authentication source to configure.
Status:	 ✓ LDAP Bind Succeeded ✓ idap://10.197.243.110
Server	10.197. 389 Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separate d for failover functionality. For example: ad1.server.com, ad2.server.com, 10.1.10.150
Transport type	CLEAR LDAPS STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	SAMAccountName,mail Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	CN=Users,DC=dmoudgil,DC=local
Search attributes	SAMAccountName Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	iseadmin The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only acc
Search password	••••• The password corresponding to the search username specified above.
	Save Settings

4. "Set Active Source"에서 소스 유형을 "Active Directory"로 선택하고 "Set Active Source"를 클 릭합니다.

Set Ac	tive Source	
Speci	fy the source that	t end-users will use for primary authentication.
S	ource type	Active Directory
		Set Active Source

5. "Add Application(애플리케이션 추가)" 하위 메뉴 아래의 "Configuration file(컨피그레이션 파 일)" 섹션 내에서 Duo Admin Console에서 다운로드한 .json 파일을 업로드하여 "Applications(애플리케이션)"로 이동합니다. 해당 .json 파일은 3단계에서 Duo Admin Portal Configuration(듀오 관리 포털 컨피그레이션) 아래에 다운로드되었습니다

Applications

A	dd Application	
	Create a SAML application	n in the Duo Admin Panel. Then, download the provided configuration file and upload it here.
Configuration file		Browse Cisco ASA - Duo Access Gateway.json
		Upload

6. 애플리케이션이 성공적으로 추가되면 "Applications" 하위 메뉴에 표시됩니다

Applications							
Name	Туре	Logo					
Cisco ASA - Duo Access Gateway	Cisco ASA	cisco	Delete				

- 7. "Metadata(메타데이터)" 하위 메뉴에서 XML 메타데이터 및 IdP 인증서를 다운로드하고 나중 에 ASA에 구성된 다음 URL을 기록해 둡니다
 - 1. SSO URL
 - 2. 로그아웃 URL
 - 3. 엔티티 ID
 - 4. 오류 URL

Metadata		Recreate Certificate
Information for configuring	applications with Duo Access Gateway. Download XML metadata	
Certificate Expiration SHA-1 Eingerprint	/C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. Download certificate 2030-04-30 18:57:14	
SHA-256 Fingerprint		
SSO URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php	
Logout URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer	
Entity ID	https://explorer.cisco.com/dag/saml2/idp/metadata.php	
Error URL	https://explorer.cisco.com/dag/module.php/duosecurity/du	

- ASA 컨피그레이션

이 섹션에서는 SAML IDP 인증 및 기본 AnyConnect 컨피그레이션에 대해 ASA를 구성하는 방법을 설명합니다. 이 문서에서는 개요에 대한 ASDM 컨피그레이션 단계 및 CLI 실행 컨피그레이션을 제 공합니다.

1. 듀오 액세스 게이트웨이 인증서 업로드

A. "Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > CA Certificates(CA 인증서)"로 이동하여 "Add(추가)"를 클릭합니다.

B. "Install Certificate(인증서 설치) 페이지"에서 신뢰 지점 이름 Duo_Access_Gateway를 구성합니 다

C. "Browse(찾아보기)"를 클릭하여 DAG 인증서와 연결된 경로를 선택하고 "Install Certificate(인증 서 설치)"를 클릭합니다.

	Cisco ASDM 7.12	2(2) for ASA - 10.197.164.3		
Home 🦓 Configuration 🧾 Monitoring	🔚 Save 🔇 Refresh 🔇 Back	C Sorward 💡 Help Type topic	Go	cisco
O O O Device Management	0 0 0 Configuration > Devi	ce Management > Certificate Mana	agement > CA Certificates	
 Device Management Management Access Licensing System Image/Configuration High Availability and Scalability Logging Smart Call-Home Cloud Web Security Smart Call-Home Cloud Web Security Users/AAA Certificate Management Identity Certificates A Certificates Charles DHCP DNS REST API Agent Advanced 	Configuration > Devi Trustpoint Name: Install from a file: Paste certificate in PEM	<pre>ce Management > Certificate Mana Install Certificate o_Access_Gateway sers/pusaxena/Desktop/dag.crt format:</pre>	Browse	ıils RL
	Specify source Interface SCEP URL: http:// Retry Period: Retry Count:	: None 1 0	 minutes (Use 0 to indicate unlimited retries) 	l
Bevice Setup			More Options	
🟥 Firewall				
Remote Access VPN	Hel	p Cancel	Install Certificate	
Site-to-Site VPN				
Device Management		Reset App	ylc	

2. AnyConnect 사용자를 위한 IP 로컬 풀 생성

"Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워 크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀)"로 이동하여 "Add(추가)"를 클릭합니다.

			Cisco ASDM 7.12(2) for ASA - 10.197.164.3	
	Home	Configuration 📴 Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help Type topic Go	cisco
Bookmarks Device List		Remote Access VPN Introduction Network (Client) Access) AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies Forup Policies IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles IPsec(IKEv2) Connection Profiles IPsec(IKEv2) Connection Profiles IPsec(IKEv2) Connection Profiles Assianment Policy Address Assignment Address Pools Advanced Clientless SSL VPN Access AAA/Local Users Secure Desktop Manager Certificate Management Language Localization Load Balancing DHCP Server DNS	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Add Pools Configure named IP Address Pools. The IP Address Pools can be used in either a VPN [Psec(IKEv1) Conner Profiles, AnyConnect Connection Profiles, Group Policies configuration Add C Edit Delete Add IPv4 Pool net Mask/Prefix Length 5.255.255.0 Starting IP Address: 10.197.164.6 Ending IP Address: 10.197.164.7 Subnet Mask: 255.255.0 Help Cancel OK	ction
	3	Device <u>M</u> anagement	Reset Apply	

3. AAA 서버 그룹 구성

A. 이 섹션에서는 AAA 서버 그룹을 구성하고 권한 부여를 수행하는 특정 AAA 서버의 세부 정보를 제공합니다

B. "Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > AAA/Local Users(AAA/로컬 사용자) > AAA Server Groups(AAA 서버 그룹)"로 이동하여 "Add(추가)"를 클릭합니다.

	Home 🖓 Configuration 🧭 Monitorin	g 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help Type topic Go	cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups	
e Lis	? Introduction	AAA Server Groups	
evic	Retwork (Client) Access	Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts	Add
	AAA/Local Users	Add AAA Server Group	
cmarks	AAA Server Groups	AAA Server Group: ISE	Edit Delete
Bool	A Secure Desktop Manager		
	Certificate Management	Accounting Mode: Osimultaneous Osingle	
	B Load Balancing	Reactivation Mode: O Depletion Timed	
	P DHCP Server	Dead Time: 10 minutes	
	DNS DNS	May Folled Attempts 2	
	Advanced	Max Failed Attempts: 3	
		Enable interim accounting update	
		Update Interval: 24 Hours	Add
		Enable Active Directory Agent mode	Edit
		ISE Policy Enforcement	Delete
		Enable dynamic authorization	
		Dynamic Authorization Port: 1700	Move Up
		Use authorization only made (no common persuard configuration required)	Move Down
		Se authorization only mode (no common password configuration required)	Test
		VPN3K Compatibility Ontion	Test
	Device Setup	Help Cancel OK	
	Firewall		
	Remote Access VPN		
	Site-to-Site VPN	Find:	
	Device Management	LDAP Attribute Map	*
	»	Reset Apply	

C 같은 페이지에서 "Servers in the Selected group(선택한 그룹의 서버)" 섹션에서 "Add(추가)"를 클릭하고 AAA 서버의 IP 주소 세부 정보를 제공합니다

Remote Access VPN Configuration >: Remote Access VPN > AAA/Local Users > AAA Server Groups Advanced AnyConnect Customization/Localiz AnyConnect Customization/Localiz AnyConnect Customization/Localiz Address Assignment Server Group: Address Pools Server Authentication Port: Address Solution Server Authentication Port: Address Assignment Server Authentication Port: Address Solution Server Authentication Port: Matalization Server Authentication Port: Matalization Server Authentication Port: Matalization Server Key: Matalization Server Secret Key: More Dow		Cisco ASDM 7.12	2(2) for ASA - 10.197.164	4.3			a la
Introduction AAA Server Groups AAA Server Groups Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts Add AAA Server Groups Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts Add Age Connect Client Profiles BipSec(IKEV1) Connection Profiles Server Group: SE BipSec(IKEV1) Connection Profiles Server Group: SE Server Group: SE BipSec(IKEV1) Connection Profiles Server Group: SE Server Group: SE BipSec(IKEV1) Connection Profiles Server Group: SE Server Group: SE BipSec(IKEV1) Connection Profiles Server Group: SE Server Name or IP Address: 10.106.44.77 BipSec(IKEV1) Connect Group: SE Server Accounting Port: 1645 Server Accounting Port: 1646 Clintines SSL VPN Access MAddress Server Server Accounting Port: 1646 Server Mode Seconds Server Secret Key: Move Up Server Secret Key: Server Secret Key: Server Secret Key: Move Up Move Up Sol Messages Sol Messages Sol Messages Sol Messages Sol Messages Sol Messages <th>Remote Access VPN</th> <th></th> <th></th> <th>A /Local Lisers</th> <th>> A A A Som</th> <th>ver Groups</th> <th>cisc</th>	Remote Access VPN			A /Local Lisers	> A A A Som	ver Groups	cisc
 Metwork (Linef) Access MayConnect Customization/Localize AnyConnect Client Profile AnyConnect Client Software AnyConnect Client Software AnyConnect Client Software AnyConnect Client Software May Connect Software May Connect Software May Connect Software May Connect Software May Client Software May Client Software May Client Sof	? Introduction	AAA Server Groups	emote Access VFN 2 A/	MA/LOCALOSELS	> AAA Sell	ver Groups	
Image: Solution of the second sec	Network (Client) Access AnyConnect Connection Profiles	Server Group Protoc	col Accounting Mode	Reactivation Mode Depletion	Dead Time 10	Max Failed Attempts	Add
Image: Server Client Software Image: Server Solicies Image: Server Name or IP Address: Image: Server Name or IP Address: Image: Server Authentication Port: Image: Server Authentication Port: Image: Server Authentication Port: Image: Server Secret Key: Image: Server Secret	Horal AnyConnect Customization/Localizati	LOCAL LOCAL	L				Edit
Group Policies Bi Psec(IKEV2) Connection Profiles Bi Psec(IKEV2) Connection Profiles Secure Mobility Solution Address Assignment Address Assignment Address Assignment Address Pools Advanced Advanced Clentless SSL VPN Access Advanced Cortificate Management Secure Desktop Manager Cortificate Management Secure Desktop Manager Cortificate Management Secure Oselatization Common Password: Move Up Common Password: Microsoft CHAPv2 Capable: © SDI Messages Message Table Kensage Table Kensage Table	AnyConnect Client Software						Delete
IPsec(Kkv2) Connection Profiles IPsec(Kkv2) Connection Profiles Secure Mobility Solution Address Assignment Address Assignment Policy Address Pools Address SSL VPN Access Clientless SSL VPN Access AAA Server Groups ISE Clientless SSL VPN Access AAA Server Groups Image Local Users Image Localization Image Locali	Group Policies		Add AAA Serve	r			
Secure Mobility Solution Interface Name: Outside Address Assignment Address Pools Server Name or IP Address: 10.106.44.77 Timeout: 10 seconds RADIUS Parameters Add Edit Server Authentication Port: 1645 Server Authentication Port: 1646 Banguage Localization Common Password: Load Balancing Discort CHAPv2 Capable: Discort CHAPv2 Capable: Sol Messages Message Table Kenote Access VPN Help Cancel OK	IPsec(IKEv2) Connection Profiles IPsec(IKEv2) Connection Profiles	Server Group:	ISE				
Server Name or IP Address: 10.106.44.77 Server Name or IP Address: Seconds Server Address: Seconds RADIUS Parameters Server Authentication Port: Server Authentication Port: Server Accounting Port: Server Accounting Port: Seconds Server Accounting Port: Seconds Server Accounting Port: Server Accounting Port: Server Secret Key: Move Dow ACL Netmask Convert: Standard Ste-to-Site VPN LDAP Attribute Map Help Cancel OK	 Secure Mobility Solution Address Assignment 	Interface Name:	outside ᅌ				
Image: Solution of Solution Image: Solution of Solution of Solution Image: Solution of Solution of Solution Image: Solution of Solution of Solution of Solution Image: Solution of	Assignment Policy	Server Name or IP Addr	ress: 10.106.44.77				
Clientless SSL VPN Access AAAJ local Users AAAA Server Groups Coal Users Server Authentication Port: 1645 Server Accounting Port: 1646 Contribute Management Cortificate Management Server Secret Key: Move Up Server Secret Key: Server Secret Key: Move Up <td>Advanced</td> <td>Timeout:</td> <td>10 seconds</td> <td></td> <td></td> <td></td> <td></td>	Advanced	Timeout:	10 seconds				
Server Authentication Port: 1645 1045 1045 105 1046 105 105 106 105 107	Glientless SSL VPN Access AAA/Local Users	RADIUS Parameters				— — (Add
Server Accounting Port: 1646 Server Accounting Port: 1646 Retry Interval: 10 seconds © Server Secret Key: Common Password: ACL Netmask Convert: Standard © Move Up Move Up Move Up Move Up Move Dow ACL Netmask Convert: Standard © SDI Messages Message Table © SDI Messages Message Table © LDAP Attribute Map	AAA Server Groups	Server Authentication	n Port: 1645				Edit
A Secure Desktop Manager A Secure Desktop Manager A Secure Secure Manager Server Secret Key: Common Password: Common Password: Common Password: ACL Netmask Convert: Standard Move Up Move Dow Move Dow Move Dow Move Dow ACL Netmask Convert: Standard Test More Device Setup Specice Setup Specice Setup Messages Message Table Help Cancel OK	Local Users	Server Accounting Po	ort: 1646				Delete
Image: Second Secon	Certificate Management	Server Secret Key:					Move Up
Image: DhCP Server Image:	🔯 Language Localization 😤 Load Balancing	Common Password:					Move Down
Microsoft CHAPv2 Capable: Device Setup SDI Messages Message Table Message Table	PHCP Server	ACL Netmask Conve	rt: Standard		0		Test
Bevice Setup SDI Messages Image: Spice-to-Site VPN Message Table Image: Spice-to-Site VPN LDAP Attribute Map		Microsoft CHAPv2 Ca	apable: 🔽				
Firewall Message Table * Image: Site-to-Site VPN Help Cancel OK	Bevice Setup	SDI Messages				_	
Site-to-Site VPN Help Cancel OK	Firewall	Message Table				*	
Site-to-Site VPN	Remote Access VPN		Help Cancel	ОК			
	Site-to-Site VPN	LDAP Attribute Map					*
Device Management	Device <u>M</u> anagement		Des	Aralı			

4. AnyConnect 클라이언트 소프트웨어 매핑

A. WebVPN에 사용할 AnyConnect 클라이언트 소프트웨어 webdeploy 이미지 4.8.03052 for windows를 매핑합니다.

B. "Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트 워크(클라이언트) 액세스) > AnyConnect Client Software(AnyConnect 클라이언트 소프트웨어)"로 이동하여 "Add(추가)"를 클릭합니다.



5. ISE의 결과로 푸시되는 리디렉션 ACL을 구성합니다

A. "Configuration(컨피그레이션) > Firewall(방화벽) > Advanced(고급) > ACL Manager(ACL 관리자)"로 이동하여 Add(추가)를 클릭하여 리디렉션 ACL을 추가합니다. 항목이 구성되면 다음과 같이 표 시됩니다.

	••				Cisco ASDM 7.12(2) f	or ASA - 10.	197.164.3			
6	Home	🖧 Configuration 🧕 Monito	ring 🔚	Save 🔇 R	lefresh 🔇 Back 💽	Forward	? Help Type topic G	0		cisco
st	00	O Firewall		O Configu	ration > Firewall > A	dvanced >	ACL Manager			_
e Li	23	Access Rules	(💠 A	dd 🚽 🖬 Ed	it 📋 Delete 👌 🗲	3 m 🛍	 Sind 🔜 Export 	•		
Devid		NAT Rules	#	Enabled	Source	Se	Destination	Security Group	Destination Service	Action
n	Ĩ		🔻 re	direct						
٦		Filter Rules	1		🧼 any		🧼 any		💵 domain	🕴 Deny
arks		Ethertype Rules	2		🧼 any		🖳 10.197.243.116		≖> ip	🕴 Deny
ž		Public Servers	3		🧼 any		🧼 any		🥵 icmp	🕴 Deny
ĝ		URL Filtering Servers	4		🧼 any		🧼 any		≖> ip	🖌 Permit
	2	Threat Detection	5		🧼 any		🧼 any		😎 http	🖌 Permit
		Identity Options								
	2	Identity by TrustSec								
		VM Attribute Agent								
		Bothet Tramc Filter								
		Unified Communications								
	v (Advanced								
		Anti-Spoofing								
	►	🖻 Certificate Management								
		😼 Fragment								
	►	No. IP Audit								
		SUNRPC Server								
		TCP Options								
		S Global Timeouts								
		ACL Manager								
		Per-Session NAT Rules								
		Device Setup								
		- F <u>i</u> rewall								
	8	Remote Access VPN								
		Site-to-Site VPN		ollanse All	Expand All					
		Device <u>M</u> anagement		mapse rai	Expand All					
		» *					Reset Apply)		

6. 기존 그룹 정책 검증

A. 이 설정은 기본 그룹 정책을 사용하며 "Configuration(컨피그레이션) > Remote Access VPN(원 격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책)"에서 볼 수 있습니다.



7. 연결 프로파일 구성

A. AnyConnect 사용자가 연결할 새 연결 프로파일을 만듭니다

B. "Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트 워크(클라이언트) 액세스) > Anyconnect Connection Profiles(Anyconnect 연결 프로파일)"로 이동 하여 "Add(추가)"를 클릭합니다.

• •		Cisco ASDM 7.1	12(2) for ASA - 10.	197.164.3				
Home 🍓 Configuration 📴 Monitori	ing 🔚 Save 🔇	Refresh 🔇 Bao	ck 🔘 Forward	? Help Type topic	Go	cis		
O O Remote Access VPN	○ ○ ○ Configu	iration > Remot	e Access VPN > N	Network (Client) Ac	cess > <u>AnyConnect Conne</u>	ection Profiles		
 Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Local AnyConnect Client Profile AnyConnect Client Software 	The security a initial client d tunnel as well Access Interface V Enable Cit	appliance automa eployment requi as SSL tunnel wi es sco AnyConnect	tically deploys the res end-user adm ith Datagram Tran VPN Client access	e Cisco AnyConnect inistrative rights. Th sport Layer Security on the interfaces so	VPN Client to remote users the Cisco AnyConnect VPN Cl (DTLS) tunneling options.	upon connection. The ient supports IPsec (II		
Poince Access Policies	SSL access mi	SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .						
Group Policies	Interface	SSL Access		IPsec (IKEv2) Acces	s			
IPsec(IKEV1) Connection Profiles		Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate		
Secure Mobility Solution	outside					De la Catalia de		
Address Assignment						Port Settings		
Advanced								
 Language Localization Load Balancing DHCP Server DNS Advanced 	Allow use Shutdown Connection Prof	r to select conne portal login pag ïlles	ection profile on th Je.	ne login page. 🛛 🕤				
auvanceu	Connection profession from certification	rofile (tunnel gro te to connection	up) specifies how profile <u>here</u> .	user is authenticate	ed and other parameters. You	u can configure the m		
	Add A	dit 🔟 Delete	Find:	\bigcirc	Match Case			
	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy		
A Device Setup	DefaultRAGr		<u>~</u>		AAA(LOCAL)	DfltGrpPolicy		
	DefaultWEBV	. 🔽			AAA(LOCAL)	DfltGrpPolicy		
Firewall	TG_SAML			SAML_User:	s Saml	DfltGrpPolicy		
Image: Second state Image: Second state Image: Second state Second state Image: Second state Second state	Let group	URL take preced	ence if group URL atches the certifica	and certificate map ate map will be used) match different connection I.	profiles. Otherwise,		
Device <u>M</u> anagement				Reset App	ly			

C. 연결 프로파일과 관련된 아래 세부 정보를 구성합니다.

이름	TG_SAML
별칭	SAML_사용자
방법	SAML
AAA 서버 그룹	로컬
클라이언트 주소 풀	AC_풀
그룹 정책	DfltGrp정책

Basic Advanced	Name:	TG_SAML	
Auvanceu	Aliases:	SAML_Users	
	Authentication		_
	Method:	SAML	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	
	CAMI Identity Provider		
	SAML Identity Provider		
	SAML Server :	https://explorer.cisco.com/dag/saml2/idp/metadata.php	Manage
	Client Address Assignment		
	DHCP Servers:		
		• None OHCP Link OHCP Subnet	
	Client Address Pools:	AC_Pool	Select
	Client IPv6 Address Pools:		Select
	Default Croup Policy		
	Croup Policy	DfltCrpPolicy	Manage
	(Following fields are linked	to attribute of the group policy selected above)	Manage
	Enable SSL VPN clien	it protocol	
	Fnable IPsec(IKEv2) of		
	DNS Servers		
	WINE Conversi		
	wins servers:		
	Domain Name:		
Find:		Next Previous	

D. 같은 페이지에서 아래와 같이 SAML ID 제공자 세부 정보를 구성합니다.

IDP 엔티 티 ID	https://explorer.cisco.com/dag/saml2/idp/metadata.php
로그 인 URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
로그 아웃 URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco
기본 URL	https://firebird.cisco.com

E. "Manage > Add"를 클릭합니다.

	Add SSO Server
IDP Entity ID:	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Settings	
Sign In URL:	https 📀 :// explorer.cisco.com/dag/saml2/idp/SSOService.php
Sign Out URL:	https ᅌ :// explorer.cisco.com/dag/saml2/idp/SingleLogoutSe
Base URL	https ᅌ :// firebird.cisco.com
Identity Provider Certificate	Duo_Access_Gateway:o=Duo Security Inc., I=Ann Ar
Service Provider Certificate:	ID_CERT:cn=firebird.cisco.com:cn=SHERLOCK-CA, dc=c
Request Signature:	None 🗘
Request Timeout:	1200 seconds (1-7200)
Enable IdP only accessible on Internal Network	
Request IdP re-authentication at login	
Help	Cancel

F. 연결 프로파일의 Advanced(고급) 섹션에서 권한 부여를 위한 AAA 서버를 정의합니다

"Advanced(고급) > Authorization(권한 부여)"으로 이동하고 "Add(추가)"를 클릭합니다.

		Edit AnyConnect Connection Profile: TG_SAML
[Basic	Authorization Server Group
	 Advanced General 	Server Group: ISE Manage
	Client Addressing	Users must exist in the authorization database to connect
	Secondary Authentic	Interface-specific Authorization Server Groups
	Accounting Croup Alias (Croup L	Add Edit Delete Assign Authorization Server Group to Interface
	Group Allas/Group (Interface: Outside Interface: Ou
		Help Cancel OK

G. Group Alias(그룹 별칭)에서 연결 별칭을 정의합니다.

"Advanced(고급) > Group Alias/Group URL(그룹 별칭/그룹 URL)"로 이동하고 "Add(추가)"를 클릭 합니다. Edit AnyConnect Connection Profile: TG_SAML

Basic Advanced General	 Enable the display of Radius Reject-Messa Enable the display of Securld messages on 	ge on the login screen when authentication is rejected the login screen
Client Addressing Authentication Secondary Authentication Authorization Accounting	Connection Aliases This SSL VPN access method will present a list the Login Page Setting in the main panel to cor Add Delete (The table is in-line editable	of aliases configured for all connection profiles. You mus nplete the configuration.
Group Alias/Group URL	Add Connection Alias Alias: SAML_Users C Enabled	Enabled
	Help Cancel OK	the connection profile, without the need for user s

H. 이렇게 하면 ASA 컨피그레이션이 완료됩니다. CLI(Command-Line Interface)에서도 아래와 같 이 표시됩니다

```
1
hostname firebird
domain-name cisco.com
I
I
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
1
   -----Client pool configuration------Client pool configuration------
1 - -
1
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
I
   -----Redirect Access-list-----
1 -
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
1
1
    -----AAA server configuration------AAA server
!
aaa-server ISE protocol radius
authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
 key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
1
crypto ca trustpoint Duo_Access_Gateway
enrollment terminal
crl configure
ï
!-----Configure Trustpoint for ASA Identity Certificate------
T
crypto ca trustpoint ID_CERT
enrollment terminal
 fqdn firebird.cisco.com
```

```
subject-name CN=firebird.cisco.com
 ip-address 10.197.164.3
 keypair ID_RSA_KEYS
no ca-check
crl configure
1
   ----Enable AnyConnect and configuring SAML authentication-----
! -
I
webvpn
 enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
 anyconnect enable
 saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
 url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
 url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
 base-url https://firebird.cisco.com
 trustpoint idp Duo_Access_Gateway
 trustpoint sp ID_CERT
 no signature
 no force re-authentication
 timeout assertion 1200
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
I
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
1
!--
   -----Tunnel-Group (Connection Profile) Configuraiton-------
1
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
 address-pool AC_Pool
authorization-server-group ISE
 accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
 authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
I
```

```
-ISE 구성
```

```
1. 네트워크 디바이스로 Cisco ASA 추가
```

"Administration > Network Resources > Network Devices"에서 "Add"를 클릭합니다. 네트워크 디바이스의 이름, 연결된 IP 주소를 구성하고 "Radius Authentication Settings(RADIUS 인 증 설정)"에서 "Shared Secret(공유 암호)"를 구성하고 "Save(저장)"를 클릭합니다.

Notwor	A Devices	
Networ		
	IP Address • IP : 10.197.164.3	/ 32
	* Device Profile	
	Software Version	
	* Network Device Group	
	Location All Locations 📀 Set To Default	
	IPSEC No Set To Default	
	Device Type All Device Types 📀 Set To Default	
	RADIUS UDP Settings	
	Protocol	RADIUS
	* Shared Secret	••••• Show
	Use Second Shared Secret	
	Use Second Shared Secret	Show
	Use Second Shared Secret CoA Port	Image: Show Image: Show Image: Show Set To Default
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i)	Image: Show 1700 Set To Default
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret	Image: Show Image: Show <t< th=""></t<>
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (2) DTLS Required Shared Secret CoA Port	Image: Constraint of the second se
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings 7 DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name	Image: Show Image: Show Image: Image: Show Image: Image: Image: Show Image: Ima
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings	Image: Show Image: Show Image: Image: Show Image: Image: Show Image: Image: Show Image: Image: Image: Image: Image: Show Image: Im
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key	Image: Show 1700 Set To Default Image: Set To Default Image: Set To Default Select if required (optional)
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key	Image: Show Image: Image: Image: Show Image: Imag
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: I
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Constraint of the second s
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: I
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format • TACACS Authentication Settings • SNMP Settings	image: show 1700 Set To Default image: show Show Show ASCII HEXADECIMAL

2. 최신 상태 업데이트를 설치합니다.

"Administration > System > Settings > Posture > Updates"로 이동하고 "Update Now"를 클릭합니 다.

Posture Updates		
 Web 	O Offline	
* Update Feed URL	https://www.cisco.com/web	b/secure/spa/posture-update.xml Set to Default
Proxy Address	72.163.217.104	
Proxy Port	80	HH MM SS
Automatically che	ck for updates starting from i	initial delay 06 - 00 - 18 - every 2 hours
Save	date Now Reset	
 Update Information 	ation	
Last successful upda	ate on	2020/05/07 15:15:05
Last update status s	ince ISE was started	No update since ISE was started. (i)
Cisco conditions ver	rsion	224069.0.0.0
Cisco AV/AS suppor	rt chart version for windows	171.0.0.0
Cisco AV/AS suppor	rt chart version for Mac OSX	91.0.0.0
Cisco supported OS	version	41.0.0.0

3. ISE에 Compliance Module 및 AnyConnect Headend Deployment Package를 업로드합니다.

"정책 > 정책 구성 요소 > 결과 > 클라이언트 프로비저닝 > 리소스"로 이동합니다. 파일을 로컬 워크 스테이션 또는 Cisco 사이트에서 가져올 것인지 여부에 따라 "추가"를 클릭하고 "로컬 디스크의 상 담원 리소스" 또는 "Cisco 사이트의 상담원 리소스"를 선택합니다.

이 경우 Category(범주) 아래의 로컬 워크스테이션에서 파일을 업로드하려면 "Cisco Provided Packages(Cisco 제공 패키지)"를 선택하고 "Browse(찾아보기)"를 클릭한 후 필요한 패키지를 선택 하고 "Submit(제출)"을 클릭합니다.

이 문서에서는 "anyconnect-win-4.3.1012.6145-iseccompliance-webdeploy-k9.pkg"를 규정 준수 모 듈로, "anyconnect-win-4.8.03052-webdeploy-k9.pkg"를 AnyConnect Headend Deployment Package로 사용합니다.

Agent Resources From Local Disk > Agent Resources From Local Disl	¢
Agent Resources From Local Disk	

Category	Cisco Provided Packages	Ţ.		
	Browse anyconnect-win-4.8.03	3052-webdeploy-k9.pkg		
-	AnyConnect Unloaded Persures	.e		
	Name	Туре	Version	Description
	AnyConnectDesktopWindows 4.8.30	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie



4. AnyConnect Posture 프로파일 생성

A. "Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프 로비저닝) > Resources(리소스)"로 이동합니다. "Add(추가)"를 클릭하고 "AnyConnect Posture Profile(AnyConnect 상태 프로파일)"을 선택합니다.

B. Anyconnect Posture Profile의 이름을 입력하고 서버 이름 규칙 아래에서 서버 이름을 "*"로 구성 한 다음 "저장"을 클릭합니다.

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:	Anyconnect Posture Profile	
Description		
		11.

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "-,cisco.com"
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

5. Anyconnect 구성 만들기

A. "Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프 로비저닝) > Resources(리소스)"로 이동합니다. "Add(추가)"를 클릭하고 "AnyConnect Configuration(AnyConnect 구성)"을 선택합니다.

B. AnyConnect 패키지 선택, 구성 이름 입력, 필요한 규정 준수 모듈 선택

C. "AnyConnect Module Selection(AnyConnect 모듈 선택)"에서 'Diagnostic and Reporting Tool(진 단 및 보고 툴)'을 선택합니다.

D. "Profile Selection"에서 Posture Profile을 선택하고 "Save"를 클릭합니다.

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package	AnyConnectDesktopWindows 4.8.3052.0	
* Configuration Name	AnyConnect Configuration	
Description:		
Description	Value	Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1250.614	
AnyConnect Module Selection		
ISE Posture	\checkmark	
VPN	\checkmark	
Network Access Manager		
Web Security		
AMP Enabler		
ASA Posture		

ASA Posture Network Visibility Umbrella Roaming Security Start Before Logon Diagnostic and Reporting Tool

Profile Selection

		_
* ISE Posture	Anyconnect Posture Profile	Ð
VPN		~
Network Access Manager		-
Web Security		-
AMP Enabler		·
Network Visibility		,
Umbrella Roaming Security		,
Customer Feedback		,

6. 클라이언트 프로비저닝 정책 생성

A. "Policy(정책) > Client Provisioning(클라이언트 프로비저닝)"으로 이동합니다.

B. "Edit"를 클릭한 다음 "Insert Rule Above"를 선택합니다.

C. Rule Name(규칙 이름)을 입력하고 필요한 운영 체제를 선택한 다음 Results("Agent" > "Agent Configuration" 내)에서 5단계에서 생성한 "AnyConnect Configuration(AnyConnect 컨피그레이션)"을 선택하고 "Save(저장)"를 클릭합니다.

ale de								_								_
cisco Ide	ntity Services Engine	B Home	a → (Context Visibility	r 1	 Operations 	→ Policy	→ 1	Administration	 Work Centers 			License Warning 🔺	0,	00	•
Policy Sets	Profiling Posture	Client Pro	visioning	 Policy Ele 	ments											
Client Pro	visioning Policy															
Define the Cl For Agent Co	ient Provisioning Policy infiguration: version of a	to determine v gent, agent pr	what use rofile, age	rs will receive up ent compliance r	con log module	gin and user sest a, and/or agent c	ion initiation ustomization	: pack	age.							
For Native St	upplicant Configuration:	wizard profile	and/or w	vizard. Drag and	drop r	ules to change the	he order.									
*																
	Rule Name		Ide	entity Groups		Operating Syst	lems		Other Condition	\$		Results				
	IOS		If Ar	ny	and	Apple iOS All		and	Condition(s)		then	Cisco-ISE-NSP			Edit	Ŧ
	Android		If Ar	ny	and	Android		and	Condition(s)		then	Cisco-ISE-NSP			Edit	
1	Windows_10		lf Ar	ny	and	Windows 10 (A	All)	and	Condition(s)		then	AnyConnect Configuration			Edit	•
	Windows		If Ar	ny	and	Windows All		and	Condition(s)		then	CiscoTemporalAgentWi			Edit	×
												WinSPWizard 2.5.0.1				
												And Cisco-ISE-NSP				
	MAC OS		lf Ar	ny	and	Mac OSX		and	Condition(s)		then	CiscoTemporalAgentOS X 4.7.00135 And			Edit	
												MacOsXSPWizard				
												NSP				
	Chromebook		If Ar	ny	and	Chrome OS A		and	Condition(s)		then	Cisco-ISE-Chrome-NSP			Edit	Ŧ
Save R	leset															

7. 포스처 조건 생성

A. "Policy(정책) > Policy Elements(정책 요소) > Conditions(조건) > Posture(포스처) > File Condition(파일 조건)"으로 이동합니다.

B. "Add(추가)"를 클릭하고 조건 이름 "VPN_Posture_File_Check", 필수 운영 체제를 "Windows 10(All)"로 구성, 파일 유형을 "FileExistence"로 구성, 파일 경로를 "ABSOLUTE_PATH"로 구성, 전 체 경로와 파일 이름을 "C:\custom.txt"으로 구성, 파일 연산자를 "Exists"로 선택

C 이 예에서는 C: drive 아래에 "custom.txt"라는 파일이 있는 경우를 파일 조건으로 사용합니다

dentity Services Engine	Home	► Operations	 Administration 	Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Eleme	nts		
Dictionaries - Conditions + Result	ts			
C Library Conditions Smart Conditions Time and Date Profiling	File Conditions List > VPN_Post File Condition * Name VPI Description * Operating System With	ture_File_Check)	
	Compliance Module Any	version		
Anti-Malware Condition		-Evistence -	Ø	
Anti-Spyware Condition		existence		
Anti-Virus Condition	* File Path	SOLUTE_PATH	C:\custom.txt	()
Application Condition	* File Operator Exi	sts 🔹		
Compound Condition	Save			
Disk Encryption Condition				
File Condition				

8. 포스처 교정 작업 생성

"정책 > 정책 구성 요소 > 결과 > 상태 > 위험 요소 제거 활동"으로 이동하여 해당 파일 위험 요소 제 거 활동을 만듭니다. 이 문서에서는 다음 단계에서 구성하는 교정 작업으로 "메시지 텍스트만"을 사 용합니다.

9. 포스처 요구 사항 규칙 만들기

A. "Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Posture(포스처) > Requirements(요구 사항)"로 이동합니다.

B. "Edit(수정)"를 클릭한 다음 "Insert new Requirement(새 요구 사항 삽입)"를 선택합니다.

C. 조건 이름 "VPN_Posture_Requirement", 필수 운영 체제를 "Windows 10(All)"로 구성, 규정 준수 모듈을 "4.x 이상"으로 구성, 포스처 유형을 "Anyconnect"로 구성

D. "VPN_Posture_File_Check"(7단계에서 생성)로 조건을 지정하고 Remediations Actions(교정 작 업)에서 Action(작업)을 "Message Text Only(메시지 텍스트만)"로 선택하고 에이전트 사용자에 대 한 사용자 지정 메시지를 입력합니다

9					(w	
hentication	Requirements					
	Name Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
horization	Default_Hardware_Attributes_Re for Mac OSX guirement_Mac	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Cleck	then Select Remediations	Edit
filing	Default_Firewall_Requirement_W for Windows All in	using 4.x or later	using AnyConnect	met if Default_Firewall_Condit on Win	then Default_Firewall_Remedi ation Win	Edit
ture	Default_Firewall_Requirement_M for Mac OSX ac	using 4.x or later	using AnyConnect	met if Default_Firewall_Condit on Mac	then Default_Firewall_Remedi ation_Mac	Edit
mediation Actions	USB_Block_temporal for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only	Edit
quirements	Any_AM_Installation_Win_tempo for Windows All ral	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only	Edit
t Provisioning	Any_AM_Installation_Mac_tempo for Mac OSX ral	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only	Edi
	Default_AppVis_Requirement_Wi for Windows All n_temporal	using 4.x or later	using Temporal Agent	met if Default_AppVis_Conditi n_Win	o then Select Remediations	Edi
	Default_AppVis_Requirement_M for Mac OSX ac_temporal	using 4.x or later	using Temporal Agent	met if Default_AppVis_Conditi n_Mac	o then Select Remediations	Edi
	Default_Hardware_Attributes_Re for Windows All quirement_Win_temporal	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Cleck	then Select Remediations	Edi
	Default_Hardware_Attributes_Re for Mac OSX quirement_Mac_temporal	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Cleck	then Select Remediations	Edi
	Default_Firewall_Requirement_W for Windows All in_temporal	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condit on_Win	i then Default_Firewall_Remedi ation_Win	Edi
	Default_Firewall_Requirement_M for Mac OSX ac_temporal	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condit on_Mac	i then Default_Firewall_Remedi ation_Mac	Edit
	VPN_Posture_Requirement for Windows 10 (A	All) using 4.x or later	using AnyConnect	met if VPN_Posture_File_Che	c then Message Text Only	Edit

10. 포스처 정책 생성

A. "Policies(정책) > Posture(포스처)"로 이동합니다.

B. 규칙 이름을 "VPN_Posture_Policy_Win"으로, 필수 운영 체제를 "Windows 10(All)"으로, 규정 준 수 모듈을 "4.x 이상"으로, 포스처 유형을 "Anyconnect"로, 요구 사항을 9단계에서 구성한

Identity	Services Engine	B Home ► Context Vis	ibility • Operation:	Policy Administ	tration				License Warning 🔺	
y Sets	Profiling Posture	Client Provisioning Polic	y Elements							
Delle										
the Postur	y Policy by configu	ring rules based on operating syst	em and/or other condition	0.05					•	
ule r ostal	e rolicy by conligu	ing tures based on operating syst		010.						
Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	R	leguirements	
0	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then D	Default_AppVis_Requir ement_Win	
0	Policy Options	Default_AppVis_Policy_Win_te mporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then D	efault_AppVis_Requir ment_Win_temporal	
0	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then D	efault_Firewall_Requir ment_Mac	
0	Policy Options	Default_Firewall_Policy_Mac_t emporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then D	efault_Firewall_Requir ment_Mac_temporal	
0	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then D	efault_Firewall_Requir ment_Win	
0	Policy Options	Default_Firewall_Policy_Win_te mporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then D	efault_Firewall_Requir ment_Win_temporal	
0	Policy Options	Default_Hardware_Attributes_P olicy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then D b c	lefault_Hardware_Attri utes_Requirement_Ma	
0	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then D b	efault_Hardware_Attri utes_Requirement_Ma _temporal	
0	Policy Options	Default_Hardware_Attributes_P olicy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then D b	efault_Hardware_Attri utes_Requirement_Wi	
0	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then D b	lefault_Hardware_Attri utes_Requirement_Wi _temporal	
0	Policy Options	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then U	JSB_Block	
0	Policy Options	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then U	ISB_Block_temporal	
~	Policy Options	VPN_Posture_Policy_Win	If Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then V	PN_Posture_Require	

11. 동적 ACL(DACL) 생성

"Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Downlodable ACLS"로 이동하고 여러 포스처 상태에 대한 DACL을 생성합니다.

이 문서에서는 다음 DACL을 사용합니다.

A. Posture Unknown: 트래픽이 DNS, PSN, HTTP 및 HTTPS 트래픽에 도달할 수 있도록 허용합니 다.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	ient Provisioning Policy Elements
Dictionaries	S
Authentication Authorization	Downloadable ACL List > PostureUnknown Downloadable ACL * Name PostureUnknown
Authorization Profiles	Description
Downloadable ACLs	IP version • IPv4 IPv6 Agnostic ()
▶ Profiling	* DACL Content 1234567 permit udp any any eq domain
▶ Posture	8910111 permit ip any host 10.106.44.77 2131415 permit top any any eq 80 1617181 permit top any any eq 443
Client Provisioning	9202122 2324252 6272829 3031323 3343536
	Check DACL Syntax
	Save

B. Posture NonCompliant: 사설 서브넷에 대한 액세스를 거부하고 인터넷 트래픽만 허용합니다.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements
Dictionaries Conditions Result	3
Authentication Authorization	Downloadable ACL List > PostureNonCompliant Downloadable ACL * Name PostureNonCompliant
Authorization Profiles	Description
Downloadable ACLs	
▶ Profiling	* DACL Content 1234567 deny jp any 10.0.0.0 255.0.0.0
▶ Posture	2131415 deny ip any 192.168.0.0 255.255.0.0 1617181 permit ip any any
Client Provisioning	9202122 2324252 6272829 3031323 3343536 • Check DACL Syntax
	Save Reset

C. Posture Compliant: Posture Compliant 엔드 유저를 위한 모든 트래픽을 허용합니다.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	ient Provisioning Policy Elements
Dictionaries	S
Authentication	Downloadable ACL List > PostureCompliant Downloadable ACL
- Authorization	* Name PostureCompliant
Authorization Profiles	Description
Downloadable ACLs	IP version OIPv4 OPv6 Aanostic @
▶ Profiling	* DACL Content 124567 permit ip any any
▶ Posture	2131415 1617181
Client Provisioning	9202122 2324252 6272829 3031323 3343536
	Check DACL Syntax
	Save Reset

12. 권한 부여 프로파일 생성

"정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일"로 이동합니다.

A. 알 수 없는 상태의 인증 프로파일

DACL "PostureUnknown"을 선택하고, Web Redirection을 선택하고, Client

Provisioning(Posture)을 선택하고, Redirect ACL name(리디렉션 ACL 이름)을 구성합니다(ASA에 서 구성), 그리고 Client Provisioning portal(클라이언트 프로비저닝 포털)을 선택합니다(기본값)

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	୍ ଡ o ¢
Policy Sets Profiling Posture Cl	Ilent Provisioning Policy Elements		
Dictionaries + Conditions - Result	ls		
0			
Authentication	Authorization Profiles > Posture Redirect Authorization Profile		
- Authorization	* Name Posture Redirect		
Authorization Profiles	Description		
Downloadable ACLs	* Access Type Access ACCEPT *		
Profiling	Network Device Profile 🛛 🏦 Cisco 💌 🕀		
▶ Posture	Service Template		
Client Provisioning	Track Movement 🗌 🕖		
	Passive Identity Tracking 🗌 🕧		
	▼ Common Tasks		
	DACL Name PostureUnknown		
Client Provisioning			
	Client Provisioning (Posture)		
	✓ Advanced Attributes Settings		
	Select an item 🕜 = 🛇 — 🕂		
	✓ Attributes Details		
	Access Type = ACCESS_ACCEPT DACL = PostureUnknown Gsco-w-pair = urf-redirect. Gsco-w-pair = urf-redirect. Gsco-w-pair = urf-redirect=https://p:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp		4
	Save Reset		

B. Posture Non-Compliant에 대한 인증 프로파일

DACL "PostureNonCompliant"를 선택하여 네트워크에 대한 액세스를 제한합니다.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۹. ۲	• •
Policy Sets Profiling Posture C	ient Provisioning Policy Elements			
Dictionaries + Conditions • Result	is a second s			
0				
Authentication	Authorization Profiles > Posture Non Compliant Authorization Profile			
- Authorization	* Name Posture Non Compliant			
Authorization Profiles	Description			
Downloadable ACLs	* Access Type Access Accept •			
Profiling	Network Device Profile 🗮 🖄 Clisco 💌 🕀			
Posture	Service Template			
Client Provisioning	Track Movement 🔿 🕧			
-	Passive Identity Tracking 💿 🕧			
	Common Tasks Zonci Name PostureHonCompilant			
	▼ Attributes Details			
	Access Type = ACCESS_ACCEPT DACL = PostureNonCompliant	li.		
(Save Reset			

C. Posture Compliant에 대한 권한 부여 프로파일

DACL "PostureCompliant"를 선택하여 네트워크에 대한 전체 액세스를 허용합니다.

Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers License Warning #	<u>्</u> । २
Policy Sets Profiling Posture C	Client Provisioning Policy Elements	
Dictionaries Conditions Result	ults	
G	Authorization Profiles > Full Access	
Authentication	Authorization Profile	
- Authorization	* Name Full Access	
Authorization Profiles	Description	
Downloadable ACLs	* Access Type ACCESS ACCEPT T	
Profiling	Network Device Profile 📾 Cisco 💌 🕀	
Posture	Service Template	
Client Provisioning	Track Movement 🗇 🕖	
	Passive Identity Tracking D	
	* Common Tasks	
	DACL Name PostureCompliant	
	Attributes Details Arrest Arrest	
	DACL = PERMIT_ALL_IPV4_TRAFFIC	lh.
	Save Reset	

12. 권한 부여 정책 구성

이전 단계에서 구성한 권한 부여 프로파일을 사용하여 Posture Compliant, Posture Non-Compliant, Posture Unknown에 대한 3가지 권한 부여 정책을 구성합니다.

공통 조건 "세션: 상태 상태"는 각 정책에 대한 결과를 결정하는 데 사용됩니다

dialla Ide	entity Service	es Engine Home	ext Visibility	Policy Administration	Work Centers			License Warning 🔺	् 🌒	•
Policy Se	ets Profiling	Posture Client Provisioning	 Policy Elements 							
Policy S	<mark>Sets →</mark> De	efault					F	teset Policyset Hitcount	Rese	Save
	Status	Policy Set Name	Description	Conditions				Allowed Protocols / Serve	r Sequence	Hits
Search										
	\odot	Default	Default policy set					Default Network Access	× - +	49
> Auth	entication Po	blicy (3)								
> Auth	orization Pol	icy - Local Exceptions								
> Auth	orization Pol	icy - Global Exceptions								
❤ Auth	orization Pol	icy (15)								
+						Results	Consult. Consul			
	Status	Rule Name	Conditions			Profiles	Security Groups		Hits	Actions
Search										
	\odot	Anyconnect Posture Compliant	ំ Session PostureStatus	s EQUALS Compliant		Full Access	Select from list	· +	6	۵
	0	Anyconnect Posture Non Compliant	Ê ₀ Session-PostureStatus	s EQUALS NonCompliant		Posture Non Compliant	Select from list	× +	0	٥
	Ø	Anyconnect Posture Unknown	AND Network Acc	ess-Device IP Address EQUALS 10.	.197.164.3	× Posture Redirect	Select from list	· +	13	ø
	Ľ		E Session-Post	tureStatus EQUALS Unknown						

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

사용자가 성공적으로 인증되었는지 확인하려면 ASA에서 다음 명령을 실행합니다.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed Username : 585b5291f01484dfd16f394be7031d456d314e3e62 Tndex : 125 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing Bytes Tx : 16404 Bytes Rx : 381 Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 Duration : 0h:00m:16s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 Public IP : 10.197.243.143 Encryption : none Hashing : none TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Client Ver : 7973 Bvtes Tx Bytes Rx : 0 Pkts Tx Pkts Rx : 6 · 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 125.2

Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 57248 Auth Mode : SAML TCP Dst Port : 443 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx Pkts Rx : 0 : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05 DTLS-Tunnel: : 125.3 Tunnel ID Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 : SAML Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 458 Bytes Rx : 381 Pkts Tx : 4 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture: Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&po Redirect ACL : redirect

상태 평가가 완료되면 "필터 이름" 필드에 푸시된 DACL에서 관찰한 대로 사용자 액세스가 전체 액 세스로 변경됩니다.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62 Index : 125 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

: AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing : 16404 Bytes Tx Bytes Rx : 381 Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 Duration : 0h:00m:36s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 Public IP : 10.197.243.143 Encryption : none Hashing : none TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 : 0 Pkts Tx Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 125.2 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 : SHA384 Encryption : AES-GCM-256 Hashing Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 57248 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes : Windows Client OS Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx Pkts Rx : 6 : 0 Pkts Rx Drop : 0 Pkts Tx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3 DTLS-Tunnel: : 125.3 Tunnel ID Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 : SAML Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 458 Bytes Rx : 381 Pkts Tx Pkts Rx : 4 : 6

Pkts Tx Drop : 0 Filter Name :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

ISE에서 권한 부여가 성공적으로 수행되었는지 확인하려면 "Operations(운영) > RADIUS > Live Logs(라이브 로그)"로 이동합니다.

이 섹션에는 인증된 사용자와 관련된 정보, 즉 ID, 권한 부여 프로파일, 권한 부여 정책, 포스처 상태 가 표시됩니다.

									Refresh	Never	Show Latest 20	records • Within	Last	t 24 hours
C	C Refresh O Reset Repeat Counts 2 Export To → T Filter → T												Filter • 🗘 •	
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Pro	Posture St	IP Address	1	Network Device
×		•			Identity	Endpoint ID	Endpoint Profi	Authentication	Authorization	Authorization Profiles	Posture Statu:	IP Address	•	Network Device
	Jun 14, 2020 07:44:59.975 AM	0	0	0	_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Anyconnect	Full Access	Compliant	10.197.164.7		
	Jun 14, 2020 07:44:59.975 AM		0			10.197.243.143			Anyconnect	Full Access	Compliant		/	ASA
	Jun 14, 2020 07:44:59.975 AM		0		#ACSACL#-IP-PERMI								/	ASA
	Jun 14, 2020 07:44:34.963 AM		0		#ACSACL#-IP-Posture								/	ASA
	Jun 14, 2020 07:44:34.958 AM		0		_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Default >> A	Posture Redirect	Pending		/	ASA

▲ 참고: ISE에 대한 추가 상태 검증은 다음 설명서를 참조하십시오. <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7</u>

Duo Admin Portal(듀오 관리 포털)에서 인증 상태를 확인하려면 인증 로그가 표시된 Admin Panel(관리 패널) 왼쪽의 "Reports(보고서)"를 클릭합니다. 추가 세부 정보: <u>https://duo.com/docs/administration#reports</u>

Duo Access Gateway에 대한 디버그 로깅을 보려면 다음 링크를 사용합니다. <u>https://help.duo.com/s/article/1623?language=en_US</u>

사용자 환경



문제 해결

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

≫ 참고: debug 명령<u>을</u> 사용하기 <u>전에 Debug 명령</u>에 대한 중요 정보를 참조하십시오.

▲ 주의: ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

대부분의 SAML 트러블슈팅에는 SAML 컨피그레이션을 확인하거나 디버그를 실행하여 찾을 수 있 는 잘못된 컨피그레이션이 포함됩니다. "debug webvpn saml 255"를 사용하여 대부분의 문제를 해결할 수 있지만 이 디버그가 유용한 정보 를 제공하지 않는 시나리오에서 추가 디버그를 실행할 수 있습니다.

debug webvpn 255 debug webvpn anyconnect 255 debug webvpn session 255 debug webvpn request 255

ASA에서 인증 및 권한 부여 문제를 트러블슈팅하려면 다음 debug 명령을 사용합니다.

debug radius all debug aaa authentication debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to

posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)

 참고: AnyConnect 및 ISE에 대한 자세한 상태 흐름 및 문제 해결 정보는 다음 링크를 참조하 십시오.
 ISE Posture Style Comparison for Pre and Post 2.2

Duo Access Gateway 디버그 로그를 해석하고 문제를 해결하려면 https://help.duo.com/s/article/5016?language=en_US

관련 정보

https://www.youtube.com/watch?v=W6bE2GTU0Is& https://duo.com/docs/cisco#asa-ssl-vpn-using-saml https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-postureover-anyconnect-remote-acces.html#anc0 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.