ISE를 사용하는 ASA 버전 9.2.1 VPN 상태 컨피 그레이션 예

목차

<u>소개</u> 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 구성 네트워크 다이어그램 및 트래픽 흐름 설정 ASA ISE 정기 재평가 다음을 확인합니다. 문제 해결 ISE에서 디버깅 ASA에서 디버깅 에이전트에 대한 디버그 NAC Agent 상태 실패 과련 정보

소개

이 문서에서는 IPN(Inline Posture Node)이 필요 없이 Cisco ISE(Identity Services Engine)에 대해 VPN 사용자를 보호하도록 Cisco ASA(Adaptive Security Appliance) 버전 9.2.1을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA CLI 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션에 대한 기본 지식
- 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 ASA 소프트웨어 버전 9.2.1 이상
- Microsoft Windows 버전 7(Cisco AnyConnect Secure Mobility Client 버전 3.1 포함)
- Cisco ISE 버전 1.2(패치 5 이상)

배경 정보

Cisco ASA 버전 9.2.1은 RADIUS CoA(Change of Authorization)를 지원합니다(RFC 5176). 이렇게 하면 IPN을 사용하지 않고도 Cisco ISE에 대해 VPN 사용자의 상태를 파악할 수 있습니다. VPN 사 용자가 로그인하면 ASA는 웹 트래픽을 ISE로 리디렉션합니다. 여기서 사용자는 NAC(Network Admission Control) 에이전트 또는 웹 에이전트로 프로비저닝됩니다. 에이전트는 OS(운영 체제), 패치, 안티바이러스, 서비스, 애플리케이션 또는 레지스트리 규칙과 같은 구성된 포스처 규칙 집합 에 대한 규정 준수를 확인하기 위해 사용자 컴퓨터에 대해 특정 검사를 수행합니다.

그런 다음 상태 검증 결과가 ISE로 전송됩니다. 시스템이 불만이라고 간주되면 ISE는 RADIUS CoA를 새 권한 부여 정책 집합과 함께 ASA에 전송할 수 있습니다. 상태 검증 및 CoA에 성공한 후 사용자는 내부 리소스에 액세스할 수 있습니다.

구성



네트워크 다이어그램 및 트래픽 흐름

다음은 네트워크 다이어그램에 나와 있는 트래픽 흐름입니다.

- 1. 원격 사용자는 ASA에 대한 VPN 액세스에 Cisco Anyconnect를 사용합니다.
- 2. ASA는 해당 사용자에 대한 RADIUS 액세스 요청을 ISE에 전송합니다.
- 3. 이 요청은 ISE에서 이름이 ASA92-posture인 정책에 도달합니다. 결과적으로 ASA92-posture 권한 부여 프로파일이 반환됩니다. ISE는 두 개의 Cisco 특성-값 쌍으로 RADIUS Access-Accept를 전송합니다.

url-redirect-acl=redirect - ASA에 로컬로 정의된 ACL(Access Control List) 이름으로, 리디렉션 해야 할 트래픽을 결정합니다.

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp - 원격 사용자를 리디렉션해야 하는 URL입니다.팁: VPN 클라이언트에 할당된 DNS(Domain Name System) 서버는 리디렉션 URL에 반환되는 FQDN(Fully Qualified Domain Name)을 확 인할 수 있어야 합니다. 터널 그룹 수준에서 액세스를 제한하기 위해 VPN 필터가 구성된 경우 클라이언트 풀이 구성된 포트(이 예에서는 TCP 8443)에서 ISE 서버에 액세스할 수 있는지 확 인합니다.

- 4. ASA는 RADIUS Accounting-Request 시작 패킷을 전송하고 응답을 수신합니다. 이는 세션에 대한 모든 세부 정보를 ISE에 보내기 위해 필요합니다. 이러한 세부 정보에는 session_id, VPN 클라이언트의 외부 IP 주소 및 ASA의 IP 주소가 포함됩니다. ISE는 해당 세션을 식별하기 위 해 session_id를 사용합니다. ASA는 또한 주기적인 중간 계정 정보를 전송합니다. 여기서 가 장 중요한 특성은 ASA에서 클라이언트에 할당한 IP가 포함된 Framed-IP-Address입니다(이 예에서는 10.10.10.10).
- 5. VPN 사용자의 트래픽이 로컬 정의 ACL(리디렉션)과 일치하면 https://ise2.testcisco.com:8443으로 리디렉션됩니다. 컨피그레이션에 따라 ISE는 NAC Agent 또는 웹 에이전 트를 프로비저닝합니다.
- 6. 에이전트는 클라이언트 시스템에 설치된 후 자동으로 특정 검사를 수행합니다. 이 예에서는 c:\test.txt 파일을 검색합니다. 또한 ISE에 상태 보고서를 보냅니다. ISE에 액세스하기 위해 스 위스 프로토콜 및 포트 TCP/UDP 8905를 사용하는 다중 교환을 포함할 수 있습니다.
- 7. ISE는 에이전트로부터 포스처 보고서를 받으면 권한 부여 규칙을 다시 한 번 처리합니다. 이번 에는 포스처 결과를 알고 또 다른 규칙이 맞는다. RADIUS CoA 패킷을 전송합니다.

사용자가 규정을 준수하는 경우 전체 액세스를 허용하는 DACL(Downloadable ACL) 이름이 전송됩니다(AuthZ 규칙 ASA92 준수).

사용자가 규정을 준수하지 않으면 제한된 액세스를 허용하는 DACL 이름이 전송됩니다(AuthZ 규칙 ASA92-noncompliant).**참고**: RADIUS CoA는 항상 확인됩니다. 즉, ASA가 확인을 위해 ISE에 응답을 보냅니다.

- 8. ASA에서 리디렉션을 제거합니다. 캐시된 DACL이 없는 경우 ISE에서 다운로드하려면 Access-Request를 보내야 합니다. 특정 DACL은 VPN 세션에 연결됩니다.
- 9. 다음에 VPN 사용자가 웹 페이지에 액세스하려고 하면 ASA에 설치된 DACL에서 허용하는 모

든 리소스에 액세스할 수 있습니다.

사용자가 규정을 준수하지 않을 경우 제한된 액세스만 허용됩니다.

참고: 이 흐름 모델은 RADIUS CoA를 사용하는 대부분의 시나리오와 다릅니다. 유/무선 802.1x 인증의 경우 RADIUS CoA는 어떤 특성도 포함하지 않습니다. DACL과 같은 모든 특성 이 연결되는 두 번째 인증만 트리거됩니다. ASA VPN 상태의 경우 두 번째 인증은 없습니다. 모든 특성은 RADIUS CoA에서 반환됩니다. VPN 세션이 활성 상태이며 대부분의 VPN 사용자 설정을 변경할 수 없습니다.

설정

ASA 및 ISE를 구성하려면 이 섹션을 사용합니다.

ASA

다음은 Cisco AnyConnect 액세스를 위한 기본 ASA 컨피그레이션입니다.

```
ip local pool POOL 10.10.10.10.10.10.100 mask 255.255.255.0
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address xxxx 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.111.10 255.255.255.0
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
key cisco
webvpn
 enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable
```

ASA와 ISE Posture를 통합하려면 다음을 확인합니다.

• CoA를 수락 하기 위해 동적 권한 부여에 대한 AAA (인증, 권한 부여 및 계정 관리) 서버를 구성 합니다.

- ISE에 대한 VPN 세션 세부사항을 보내기 위해 터널 그룹으로 어카운팅을 구성합니다.
- 사용자에게 할당된 IP 주소를 전송하고 ISE에서 세션 상태를 주기적으로 업데이트하는 중간 어 카운팅을 구성합니다
- DNS 및 ISE 트래픽이 허용되는지 여부를 결정하는 리디렉션 ACL을 구성합니다. 다른 모든 HTTP 트래픽은 상태를 위해 ISE로 리디렉션됩니다. 구성 예는 다음과 같습니다.

access-list redirect extended deny udp any any eq domain access-list redirect extended deny ip any host 10.48.66.74 access-list redirect extended deny icmp any any access-list redirect extended permit tcp any any eq www aaa-server ISE protocol radius authorize-only interim-accounting-update periodic 1 dynamic-authorization aaa-server ISE (inside) host 10.48.66.74 key cisco tunnel-group RA general-attributes address-pool POOL authentication-server-group ISE accounting-server-group ISE default-group-policy GP-SSL

ISE

ISE를 구성하려면 다음 단계를 완료하십시오.

1. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고 ASA를 네트워크 디바이스로 추가합니다.

alialis at the state of the	
cisco Identity Services Engine	Home Operations ▼ Policy ▼ Administration ▼
🔆 System 🦉 Identity Management 📷 N	letwork Resources 🛃 Web Portal Management 👩 Feed Service
Network Devices Network Device Groups Ext	ernal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices	Network Devices List > New Network Device Network Devices * Name ASA Description * IP Address: 192.168.111.10 / 32 Model Name * Software Version * * Network Device Group Location All Locations Set To Default Device Type All Device Types Set To Default
	✓ Authentication Settings
	Enable Authentication Settings Protocol RADIUS * Shared Secret OCCON Show

2. Policy(정책) > Results(결과) > Authorization(권한 부여) > Downloadable ACL(다운로드 가능 한 ACL)로 이동하고 DACL이 전체 액세스를 허용하도록 DACL을 구성합니다. 기본 ACL 컨피 그레이션은 ISE의 모든 IP 트래픽을 허용합니다.

cisco Identity Services Engine	Administration ▼
🛃 Authentication 💿 Authorization 🔀	Profiling 👩 Posture 👩 Client Provisioning 📑 Security Group Access
Dictionaries Conditions Results	
Results	Downloadable ACL List > PERMIT_ALL_TRAFFIC Downloadable ACL * Name PERMIT_ALL_TRAFFIC Description Allow all Traffic * DACL Content 1 permit ip any any 3 4 5 6 7 8 9 10

- 3. (규정을 준수하지 않는 사용자에 대해) 제한된 액세스를 제공하는 유사한 ACL을 구성합니다.
- 4. Policy(정책) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프 로파일)로 이동하고 ASA92-posture라는 권한 부여 프로파일을 구성합니다. 그러면 포스처를 위해 사용자를 리디렉션합니다. Web Redirection(웹 리디렉션) 확인란을 선택하고 드롭다운 목록에서 Client Provisioning(클라이언트 프로비저닝)을 선택한 다음 ACL 필드에 리디렉션이

나타나는지 확인합니다(ACL은 ASA에서 로컬로 정의됨).

diada cisco Identity Services Engine	Administration ▼
Authentication S Authorization Results	Profiling 👩 Posture 👸 Client Provisioning 📑 Security Group Access
Results	Authorization Profiles > ASA92-posture Authorization Profile *Name ASA92:posture Description *Access Type ACCESS_ACCEPT • Service Template = Voice Domain Permission Voice Domain Permission Veb Redirection (CWA, DRW, MDM, NSP, CPP) Client Provisioning (Posture) • ACL redirect

5. ASA92-compliant라는 권한 부여 프로파일을 구성합니다. 이는 규정 준수 사용자에게 전체 액 세스를 제공하는 PERMIT_ALL_TRAFFIC이라는 DACL만 반환해야 합니다.

dhhh	
cisco Identity Services Engine	Home Operations ▼ Policy ▼ Administration ▼
🛃 Authentication 👩 Authorization 🔀	, Profiling 🛛 👩 Posture 🔊 Client Provisioning 📄 Security Group Access
Dictionaries Conditions Results	
Results	Authorization Profiles > ASA92-compliant Authorization Profile * Name ASA92-compliant Description * Access Type ACCESS_ACCEPT * Service Template * Common Tasks DACL Name PERMIT_ALL_TRAFFIC *

6. ASA**92**-noncompliant라는 유사한 권한 부여 **프로파일을 구성하며**, 이는 제한된 액세스(비규격 사용자의 경우)를 통해 DACL을 반환해야 합니다.

7. Policy(정책) > Authorization(권한 부여)으로 이동하고 권한 부여 규칙을 구성합니다.

포스처 결과가 규정을 준수하는 경우 전체 액세스를 허용하는 규칙을 생성합니다. 그 결과 권 한 부여 정책 ASA92 준수가 됩니다.

포스처 결과가 규정을 준수하지 않을 경우 제한된 액세스를 허용하는 규칙을 생성합니다. 그 결과 권한 부여 정책 ASA92-noncompliant가 됩니다.

앞의 두 규칙 중 어느 규칙에도 해당되지 않는 경우 기본 규칙은 **ASA92-posture를 반환하며**, 이는 ASA에서 리디렉션을 강제합니다.

1	~	ASA92 complaint	if	Session:PostureStatus EQUALS Compliant	then	ASA92-compliant
	2	ASA92 non complaint	if	Session:PostureStatus EQUALS NonCompliant	then	ASA92-noncompliant
	×	ASA92 redirect	if	Radius:NAS-IP-Address EQUALS 192.168.111.10	then	ASA92-posture

8. 기본 인증 규칙은 내부 ID 저장소의 사용자 이름을 확인 합니다. 이를 변경해야 하는 경우(예: AD(Active Directory)에서 선택) **Policy(정책) > Authentication(인증)**으로 이동하여 다음을 변 경합니다.

aliali cisco	Identity Services Engine	▲ Home Operations ▼	Policy V Administration V
📘 Au	thentication 🧕 Authorization 🔀	Profiling 💽 Posture 🔂 Clien	t Provisioning 🚊 Security Group Access 🦺 Pol
Auther	ntication Policy		
Define the Policy Typ	e Authentication Policy by selecting the proto be O Simple	cols that ISE should use to communicate	with the network devices, and the identity sources that it sh
	MAB : If Wire Wire Wire Vire Vire	id_MAB OR Iless_MAB e Internal Endpoints	Allow Protocols : Default Network Access
	Dot1X : If Wire Wire	:d_802.1X OR !less_802.1X	Allow Protocols : Default Network Access
	Default : use Default Rule (If no match) : Allow Pro	Internal Users otocols : Default Network Access	and use : Internal Users

9. Policy(정책) > Client Provisioning(클라이언트 프로비저닝)으로 이동하고 프로비저닝 규칙을 구성합니다. 프로비저닝해야 하는 에이전트의 유형을 결정하는 규칙입니다. 이 예에서는 간단 한 규칙이 하나만 있으며, ISE는 모든 Microsoft Windows 시스템에 대해 NAC Agent를 선택합 니다.



에이전트가 ISE에 없는 경우 다음 파일을 다운로드할 수 있습니다.

CAgent 4.9 🗢		Done
Agent Configuration		
Agent:	NACAgent 4.9.0.1013	📀 🗹 Is Upgrade Mandatory
Profile:	Choose a Profile	Agents
Compliance Module:	Choose a Compliance Module	
Agent Customization Package:	Choose a Customization Package	⇔ • ≡ •
Native Supplicant Co Config Wizard: Choose a Wizard Profile: Choose a	nfiguration Config Wizard © Wizard Profile ©	 Clear Control Download Resource NACAgent 4.9.0.52 NACAgent 4.9.0.1009 NACAgent 4.9.0.1013 WebAgent 4.9.0.24 WebAgent 4.9.0.28 WebAgent 4.9.0.31 WebAgent 4.9.0.1005
		WebAgent 4.9.0.1007

- 10. 필요한 경우 Administration(관리) > System(시스템) > Settings(설정) > Proxy(프록시)로 이 동하여 ISE에 대한 프록시를 구성할 수 있습니다(인터넷에 액세스할 수 있도록).
- 11. 클라이언트 컨피그레이션을 확인하는 포스처 규칙을 구성합니다. 다음을 확인하는 규칙을 구성할 수 있습니다.

파일 - 존재, 버전, 날짜

레지스트리 - 키, 값, 존재

application - 프로세스 이름, 실행 중, 실행 중 아님

service - 서비스 이름, 실행 중, 실행 중이 아님

안티바이러스 - 100개 이상의 공급업체 지원, 버전, 정의 업데이트 시

안티스파이웨어 - 정의가 업데이트될 때 100개 이상의 공급업체 지원, 버전

복합 상태 - 모든 혼합

사용자 지정 사전 조건 - 대부분의 ISE 사전 사용

12. 이 예에서는 간단한 파일 존재 확인만 수행됩니다. c:\test.txt 파일이 클라이언트 시스템에 있는 경우 호환되며 전체 액세스가 허용됩니다. Policy(정책) > Conditions(조건) > File Conditions(파일 조건)로 이동하고 파일 조건을 구성합니다.

cisco Identity Services Engine	Home Operations Policy Administration	
Authentication Authorization	Profiling 👩 Posture 👦 Client Provisioning 📄 Security Group Access 🌉 Pol	icy Elements
Posture	File Conditions List > file_condition File Condition * Name file_condition Description * File Path ABSOLUTE_PATH * [::\test.txt * File Type FileExistence * * File Operator Exists * * Operating System Windows All \$ Save Reset	œ.

13. Policy(**정책) > Results(결과) > Posture(포스처) > Requirements(요건)**로 이동하고 요건을 생 성합니다. 이 요건은 이전 조건이 충족될 때 충족되어야 한다. 그렇지 않은 경우 교정 작업이 실행됩니다. 사용 가능한 여러 유형의 교정 작업이 있을 수 있지만, 이 예에서는 가장 간단하 게 특정 메시지가 표시됩니다.

cisco Identity Services Engine	Home Operations Policy	Administration •		
🛓 Authentication 🛛 🧔 Authorization 🖉	Profiling 🖉 Posture 🕞 Client Provisionin	ng 🔄 Security Group Acces	ss 🚯 Policy Elements	
Dictionaries Conditions Results				
Results	Requirements			
Q	Name	Operating Systems	Conditions	Remediation Actions
@ * E * 🛞,				
Authentication Authentication	file_requirement	for Windows All	metri file_condition	else Message Text Only
 Protiting 	Any_AV_Installation_Win	for Windows All	met if ANY_av_win_inst	else Message Text Only
 Postare Remediation Actions 	Any_Av_Definition_Win	for Windows All	metif ANY_av_win_def	else AnyAVDefRemediation/VII n
Requirements Client Provisioning	Any_AS_Installation_Win	for Windows All	metif ANY_as_win_inst	else Message Text Only
 Security Group Access 	Any_AS_Definition_Win	for Windows All	metif ANY_as_win_def	else AnyASDelRemediation/W
	Any_AV_Installation_Mac	for Mac OSX	met if _ANY_av_mac_inst	else Message Text Only
	Any_AV_Definition_Mac	for Mac OSX	metif ANY_av_mac_def	else AnyAVDefRemediationMa
	Any_AS_Installation_Mac	for Mac OSX	metif ANY_as_mac_inst	eise Message Text Only
	Any_AS_Definition_Mac	for Mac OSX	metif ANY_as_mac_def	else Message Text Only

참고: 일반적인 시나리오에서는 File Remediation 작업을 사용할 수 있습니다(ISE에서 다운 로드 가능한 파일을 제공함).

14. Policy(정책) > Posture(포스처)로 이동하고 포스처 규칙에서 이전 단계(file_requirement로

이름 지정됨)에서 생성한 요건을 사용합니다. 유일한 포스처 규칙은 모든 Microsoft Windows 시스템이 file_requirement를 충족해야 **합니다**. 이 요구 사항이 충족되면 스테이션은 규정을 준수하고, 충족되지 않으면 스테이션은 규정을 준수하지 않습니다.

cisco Identity Services Engine	🟠 Home Operatio	ns • Policy • Administrat	tion 🖛	
👗 Authentication 🧕 Authorization 🛛	Profiling 🖉 Posture	Client Provisioning 📑 💼 Sec	curity Group Access 💦 🐴 Policy E	lements
Posture Policy Define the Posture Policy by configuring rules base	d on operating system and/or other (conditions.		
Status Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
posture	if Any	and Windows All		then file_requirement

정기 재평가

기본적으로 Posture는 일회성 이벤트입니다. 그러나 주기적으로 사용자의 컴플라이언스를 점검하 고 그 결과에 따라 리소스에 대한 액세스를 조정해야 할 필요가 있는 경우가 있습니다. 이 정보는 SWISS 프로토콜(NAC Agent)을 통해 푸시되거나 애플리케이션(웹 에이전트)에서 인코딩됩니다.

사용자 규정 준수를 확인하려면 다음 단계를 완료하십시오.

1. Administration(관리) > Settings(설정) > Posture(포스처) > Reassessments(재평가)로 이동하 고 전역으로 재평가를 활성화합니다(ID 그룹 컨피그레이션별).



2. 모든 재평가와 일치하는 포스처 조건을 생성합니다.

cisco Identity Services Engine	▲ Home Operations ▼	Policy Administration	*
🛓 Authentication 🛛 🧔 Authorization 🔀	Profiling 👩 Posture 👸 Client	Provisioning 📃 Security	Group Access 🔒 Policy Elements
Dictionaries Conditions Results			
Posture	Dictionary Conditions List > New Dictionary Simple Conditi * Name reassesment Description * Attribute Session:Agent-Request-Type ③ Submit Cancel	* Operator Equals	*Value • Periodic Reassessment •
E AV Compound Condition			
AS Compound Condition			
E Dictionary Simple Condition			
Dictionary Compound Condition	- 1		

3. 초기 평가와 일치하는 유사한 조건을 생성합니다.

cisco Identity Services Engine	Home Operations ▼ Policy ▼ Administration ▼
🚨 Authentication 🛛 👩 Authorization	Profiling 👩 Posture 👸 Client Provisioning 🚊 Security Group Access 🚺 🥵 Policy Elements
Dictionaries Conditions Results	
Posture	Dictionary Conditions List > New Dictionary Condition
م ا	Dictionary Simple Condition
⇔ • ≡ • ⊗	Description
E File Condition	
Registry Condition	
Application Condition	* Attribute * Operator * Value
Service Condition	Session:Agent-Request-Type 📀 🛛 Equals 👻 Initial
E Compound Condition	Submit Cancel
E AV Compound Condition	
AS Compound Condition	
E Dictionary Simple Condition	
E Dictionary Compound Condition	

이 두 가지 조건 모두 상태 규칙에서 사용 할 수 있습니다. 첫 번째 규칙은 초기 평가에만 일치하고 두 번째 규칙은 모든 후속 평가와 일치합니다.

cisco Identity Services Engine	A Home Operation	ns • Policy • Administratio	on I 💌	
🚉 Authentication 🧕 Authorization	🛃 Profiling 💽 Posture 👸	Client Provisioning 🛛 🚊 Secu	irity Group Access 🛛 🐴 Policy I	Elements
Posture Policy Define the Posture Policy by configuring rules bas	sed on operating system and/or other	conditions.		
Status Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
🗹 posture_initial	lf Any	and Windows All	initial	then file_requirement
gosture_reassessment	If Any	and Windows All	reassessment	then file_requirement

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계에 설명된 대로 단계를 완료해야 합니다.

- 1. VPN 사용자는 ASA에 연결합니다.
- 2. ASA는 RADIUS 요청을 전송하고 url-redirect 및 url-redirect-acl 특성이 포함된 응답을 수신합 니다.

۵ 🛛 📕 👗 د	🗎 X 😅 🔍 🌳 🆗	د الم
Filter:		Expression Clear Apply Save
No. Source	Destination	Protocol Length Info
1 192.168.111.10	10.48.66.74	RADIUS 312 Access-Request(1) (id=46, l=270)
2 10.48.66.74	192.168.111.10	RADIUS 311 Access-Accept(2) (id=46, 1=269)
4		
Frame 2: 311 bytes o	n wire (2488 bits), 3	11 bytes captured (2488 bits)
Ethernet II, Src: Vm	ware_c0:00:03 (00:50:	56:c0:00:03), Dst: Ymware_e8:ef:25 (00:0c:29:e8:ef:25)
Internet Protocol Ve	rsion 4, Src: 10.48.6	6.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)
> User Datagram Protoc	ol, Src Port: sightli	ne (1645), Dst Port: 54459 (54459)
Radius Protocol		
Code: Access-Accep	t (2)	
Packet identifier:	0x2e (46)	
Length: 269		
Authenticator: bef	22fb479a10c1e2dea50937	7882e0d4
This is a response	e to a request in fra	<u>e 11</u>
[Time from request	: 0.059399000 seconds)	
* Attribute Value Pa	irs	
▷ AVP: l=7 t=User-	Name(1): cisco	
▷ AVP: l=40 t=Stat	e(24): 52656175746853	657373696f6e3a63306138373030613030
▷ AVP: l=50 t=Clas	s(25): 434143533a6330	6138373030613030303064303030353262
✓ AVP: l=33 t=Vend	lor-Specific(26) vmcis	coSystems(9)
▷ VSA: l=27 t=Cis	co-AVPair(1): url-red	irect-acl=redirect
✓ AVP: l=119 t=Ver	dor-Specific(26) v=ci	scoSystems(9)
a second di seconda della		

> VSA: l=113 t=Cisco-AVPair(1): url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a000000052b1b1bc&action=cpp

3. ISE 로그는 권한 부여가 포스처 프로파일과 일치함을 나타냅니다(첫 번째 로그 항목).

	x		#ACSACL#-IP-P		ASA9-2			Compliant	ise2
	×	à		192.168.10.67	ASA9-2	ASA92-compliant		Compliant	ise2
,	0	<u>a</u> () cisco	192.168.10.67				Compliant	ise2
	×	0	cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro	Pending	ise2

4. ASA는 VPN 세션에 리디렉션을 추가합니다.

aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10

5. ASA의 VPN 세션 상태는 상태가 필수임을 보여주고 HTTP 트래픽을 리디렉션합니다.

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username	:	CISCO	Inde	x	:	9		
Assigned IP	:	10.10.10.10	Publ	ic IP	:	10	.147.24.	.61
Protocol	:	AnyConnect-Parent SSL-	Tunne	l DTLS-Tu	un	nel	<u>_</u>	
License	:	AnyConnect Essentials						
Encryption	:	AnyConnect-Parent: (1)	none	SSL-Tuni	ne	1:	(1)RC4	DTLS-Tunnel: (1)AES128
Hashing	:	AnyConnect-Parent: (1)	none	SSL-Tuni	ne	1:	(1)SHA1	DTLS-Tunnel: (1)SHA1
Bytes Tx	:	16077	Byte	s Rx	:	19	9497	
Pkts Tx	:	43	Pkts	Rx	:	22	25	
Pkts Tx Drop	:	0	Pkts	Rx Drop	:	0		
Group Policy	:	GP-SSL	Tunn	el Group	:	RA	A	
Login Time	:	14:55:50 CET Mon Dec 2	3 201	3				
Duration	:	0h:01m:34s						
Inactivity	:	0h:00m:00s						
VLAN Mapping	:	N/A	VLAN		:	no	one	
Audt Sess ID	:	c0a8700a0000900052b840	еб					
Security Grp	:	0						
AnyConnect-Pa	are	ent Tunnels: 1						

SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 9.1 Public IP : 10.147.24.61 Encryption : none Hashing : none TCP Src Port : 50025 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 779 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 9.2 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Hashing : SHA1 Encryption : RC4 TCP Src Port : 50044 Encapsulation: TLSv1.0 TCP Dst Port : 443Auth Mode : userPasswordIdle Time Out: 30 MinutesIdle TO Left : 28 Minutes TCP Dst Port : 443 Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 172 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 9.3 Assigned IP : 10.10.10.10 Public IP : **10.147.24.61** Hashing : SHA1 Encryption : AES128 UDP Src Port : 63296 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode : userPassword 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 3.1.02040 Bytes Tx : 5669 Bytes Rx : 18546 : 35 Pkts Tx : 222 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 ISE Posture:

Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway? sessionId=c0a8700a0000900052b840e6&action=cpp Redirect ACL : redirect

6. 리디렉션 ACL과 일치하는 HTTP 트래픽을 시작하는 클라이언트는 ISE로 리디렉션됩니다.

aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for 10.10.10.10

7. 클라이언트는 다음 상태를 위해 ISE로 리디렉션됩니다.

۲	 https://ise2test-cisco.com/04/3/sut iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	h/CppSetup.action?session=c0e0700e000052b0066c8ces=Windows T (4) 🏫 🛡 🖱 📑 - AVG Secure Search 👂 🖡 🏫 💽 : ovisioning Portal
	Cisco Identity Se Engine Network Notice	Security Warning Security Warning Do you want to Continue? The connection to this website is untrusted. Website: https://ise2.test-tisco.com:8443 Note: The contribute is not valid and cannot be used to verify the identity of this website. This application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute. Please context the Publisher for more information. More information Continue: Continue

8. NAC Agent가 설치되어 있습니다. NAC Agent를 설치 한 후, 스위스 프로토콜을 통해 상태 규 칙을 다운로드 하고 규정 준수를 결정 하기 위해 확인을 수행 합니다. 그런 다음 상태 보고서가 ISE로 전송됩니다.

😕 Cisco NAC Agent	
cisco NAC Agent	About
Full Network Access	
Your device conforms with all the security policies for this protected network	

9. ISE는 상태 보고서를 받고, 권한 부여 규칙을 재평가하고, (필요한 경우) 권한 부여 상태를 변 경하고 CoA를 전송합니다. 이는 ise**-psc.log**에서 확인할 수 있습니다.

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a000900052b840e6

:::- Decrypting report

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a000900052b840e6

:::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity

Groups:Employee,NAC Group:NAC:IdentityGroups:An

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a000900052b840e6

:::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a000900052b840e6

:::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2

cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a000900052b840e6

:::- Posture coA is triggered for endpoint [null] with session

[c0a8700a000900052b840e6]

10. ISE는 전체 액세스를 허용하는 session_id 및 DACL 이름을 포함하는 RADIUS CoA를 전송
```

합니다.

No.	Source	Destination	Protocol	Length I	nfo		
7	10.48.66.74	192.168.111.10	RADIUS	231 C	oA-Request(43) (id=1	1, l=189)
8	192.168.111.10	10.48.66.74	RADIUS	62 C	oA-ACK(44)	(id=11, l:	=20)
4							***
▶ Fr	ame 7: 231 bytes on v	wire (1848 bits), 23	1 bytes	captured	(1848 bits)	
▶ Et	hernet II, Src: Vmwa	re_c0:00:03 (00:50:5	6:c0:00:	03), Dst	: Vmware_e8	:ef:25 (00	0:0c:29:e8:ef:25)
▶ In	ternet Protocol Vers	ion 4, Src: 10.48.66	.74 (10.	48.66.74), Dst: 192	.168.111.	10 (192.168.111.10)
▶ Us	er Datagram Protocol	, Src Port: 44354 (4	4354), D	st Port:	mps-raft (1700)	
▼ Ra	dius Protocol						
0	Code: CoA-Request (43	;)					
	Packet identifier: 0	:b (11)					
1	ength: 189						
	Authenticator: d20817	c6ca828ce7db4ee54f1	5177b8d				
	The response to this	<u>request is in fram</u>	<u>e 81</u>				
~ /	Attribute Value Pairs						
	AVP: l=6 t=NAS-IP-	Address(4): 10.147.2	4.61				
	AVP: l=15 t=Callin	g-Station-Id(31): 19	2.168.10	0.67			
	AVP: l=6 t=Event-T	imestamp(55): Dec 18	, 2013 1	15:32:10.	000000000 C	ET	
	AVP: l=18 t=Messag	e-Authenticator(80):	1ee29f1	ld83e5f3a	a4934d60aa6	17ebeb	
1	AVP: l=75 t=Vendor	-Specific(26) v=cisc	oSystems	;(9)			
	▹ VSA: l=69 t=Cisco	AVPair(1): ACS:Cisc	oSecure-I	Defined-	ACL=#ACSACL	#-IP-PERMI	<pre>[T_ALL_TRAFFIC.51ef7db1</pre>
	AVP: l=49 t=Vendor	-Specific(26) v=ciso	oSystems	5(9)			
	▶ VSA: l=43 t=Cisco	AVPair(1): audit-se	ssion-id:	=c0a8700a	a0000d00052	b1b1bc	

이는 ISE 로그에 반영됩니다.

첫 번째 로그 항목은 상태 프로필을 반환 (리 디렉션 포함) 초기 인증을 위한 것입니다.

두 번째 로그 항목은 규정 준수 스위스 보고서가 수신된 후 채워집니다.

세 번째 로그 항목은 CoA가 전송될 때 확인(Dynamic Authorization Succeeded)과 함께 채워 집니다.

최종 로그 항목은 ASA가 DACL을 다운로드할 때 생성됩니다.

. 🗹	ġ.	#ACSACL#-IP-P	ASA9-2		Compliant ise2
- 🛃	à	192.168.10.67	ASA9-2	ASA92-compliant	Compliant ise2
	à	0 cisco 192.168.10.67			Compliant ise2
- 🗹	ò	cisco 192.168.10.67	ASA9-2	ASA92-posture User Ide	ntity Gro Pending ise2

11. ASA에서 디버그를 수행하면 CoA가 수신되고 리디렉션이 제거됨을 알 수 있습니다. ASA는 필요한 경우 DACL을 다운로드합니다.

ASA# Received RAD_COA_REQUEST

RADIUS packet decode (CoA-Request)

 Radius: Value (String) =

 41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d
 | ACS:CiscoSecure

 44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53
 | Defined-ACL=#ACS

 41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41
 | ACL#-IP-PERMIT_A

 4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37
 | LL_TRAFFIC-51ef7

 64 62 31
 | db1

Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=

#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

aaa_url_redirect: **Deleted url redirect** for **10.10.10.10** 12. VPN 세션 후 Cisco는 사용자에 대해 DACL을 적용(전체 액세스)했습니다.

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Username
                                               : 9
           : cisco
                                    Index
Assigned IP : 10.10.10.10
                                   Public IP : 10.147.24.61
Protocol
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License
            : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
           : 94042
                                   Bytes Rx : 37079
Pkts Tx : 169
                                    Pkts Rx
                                               : 382
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
Group Policy : GP-SSL
                                    Tunnel Group : RA
Login Time : 14:55:50 CET Mon Dec 23 2013
           : 0h:05m:30s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                    VLAN
                                             : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
 Tunnel ID : 9.1
 Public IP : 10.147.24.61
 Encryption : none
TCP Src Port : 50025
                                    Hashing : none
                                     TCP Dst Port : 443
 Auth Mode : userPassword
                                    Idle TO Left : 24 Minutes
 Idle Time Out: 30 Minutes
 Client OS : win
 Client Type : AnyConnect
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx : 5204
                                    Bytes Rx : 779
 Pkts Tx
             : 4
                                     Pkts Rx
                                                 : 1
 Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
SSL-Tunnel:
 Tunnel ID : 9.2

      Assigned IP : 10.10.10.10
      Public IP : 10.147.24.61

      Encryption : RC4
      Hashing : SHA1

 Encapsulation: TLSv1.0
                                    TCP Src Port : 50044
 TCP Dst Port : 443
                                     Auth Mode : userPassword
 Idle Time Out: 30 Minutes
                                    Idle TO Left : 24 Minutes
 Client OS : Windows
 Client Type : SSL VPN Client
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx
            : 5204
                                    Bytes Rx : 172
                                                 : 2
 Pkts Tx
             : 4
                                     Pkts Rx
 Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
 Filter Name : #ACSACL#-IP-PERMIT ALL TRAFFIC-51ef7db1
                              Public IP : 10.147.24.61
Hashing : SHA1
UDP Src Port - Co
DTLS-Tunnel:
 Tunnel ID : 9.3
 Assigned IP : 10.10.10.10
 Encryption : AES128
 Encapsulation: DTLSv1.0
                                    Auth Mode : userPassword
 UDP Dst Port : 443
                               Idle TO Left : 29 Minutes
 Idle Time Out: 30 Minutes
 Client OS : Windows
```

Filter Name	:	#ACSACL#-IP-PERMIT	L_ALL	_TRAF	FIC-51ef7	dł	51
Pkts Tx Drop	:	0		Pkts	Rx Drop	:	0
Pkts Tx	:	161		Pkts	Rx	:	379
Bytes Tx	:	83634		Byte	s Rx	:	36128
Client Ver	:	Cisco AnyConnect V	VPN A	gent	for Windo	SWS	3.1.02040
Client Type	:	DTLS VPN Client					

참고: CoA에 연결된 DACL이 없는 경우에도 ASA는 항상 리디렉션 규칙을 제거합니다.

문제 해결

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

ISE에서 디버깅

디버그를 **활성화하려면 Administration > Logging > Debug Log** Configuration으로 이동합니다. Cisco에서는 다음에 대해 임시 디버그를 활성화하는 것을 권장합니다.

- 스위스인
- NSF(무중단 전달)
- NSF 세션
- 프로비전
- 상태

디버그를 보려면 CLI에서 다음 명령을 입력합니다.

ise2/admin# show logging application ise-psc.log tail count 100

상태 보고서를 보려면 Operations(운영) > Reports(보고서) > ISE Reports(ISE 보고서) > Endpoints and Users(엔드포인트 및 사용자) > Posture Details Assessment(상태 세부 평가)로 이동합니다.

-duala.									242 (abox	Logent Neebeck D
CIDED Identity Services Engine	强 Home Oper	ations 🔻	Policy	• Admini	stration v					Satup As
🙍 Authentications 📑 Reports 📷 Endp	coint Protection Genice	Tott	foor right							
Report Selector	Posture Detail Asses	sment								🔶 Favorite 🛛 🔉 Export 🔡
Favorites										Generated at 2013-12-2
ISE Reports	From 12/23/2013 12:08:00	DAM to 12	15255012	03:56:58 PM						Page << 1 >> Parents167
Auth Dervices Stelue	Logged At	Status	Detail	PRA.	Identity	Endpoint D	P Address	Endpoint DS	Agent	Hessage
a reports	2013-12-23 15:21:34.9	-	.0	continue	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RIAC A	Received a posture report from an endpoint
 Deprogramment Status 11 reports 	2013-12-23 15:08:58.3		.o	continue	cisco	08/08/27/CD/EB/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
+ Endpoints and Users	2013-12-23 14:59:34.3	-	.0	continue	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RIAC A	Received a posture report from an endpoint
Client Provisioning	2013-12-23 14:55:28.6	٠	.0	NA	cisco	08/05/27/CD/E8/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
Current Active Sessions	2013-12-23 14:44:45.0	٠	.0	NA	cisco	08:08:27:CD:E8:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RAC A	Received a posture report from an endpoint
Gaest Activity	2013-12-23 13:34:30.3	٠	.0	NA	cisco	08/08/27/76/56/6	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A	Received a posture report from an endpoint
Guest Accounting	2013-12-23 13:27:10.3	۰	.0	NA	cisco	08:00:27:77:57:5	10.147.24.92	Windows 7 Ultimate 64-bit	CIBIO RAE A	Received a posture report from an endpoint
Guest Sponsor Happing										
Quest Sponsor Summary										
Endpoint Protection Service Audit										
Mobile Davice Hanagement										
Posture Detail Assessment Posture Detail Assessment Posture Today Today Run Run										

Posture More Detail Assessment(포스처 추가 세부사항 평가) 페이지에는 요건 이름이 표시된 정책 이름이 결과와 함께 표시됩니다.

Posture More Detail Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM Generated At: 2013-12-23 15:57:31.248

Client Details								
Username:		cisco						
Mac Address:		08:00:2	7:CD:E8:A2					
IP address:		10.147.	24.92					
Session ID:		c0a870	0a0000b00052b8	346c0				
Client Operating System	m:	Window	s 7 Enterprise 64-	-bit				
Client NAC Agent:		Cisc o N/	AC Agent for Wind	lows 4.9.0	0.1013			
PRA Enforcement:		1						
CoA:		Receive	d a posture report	from an	endpoint			
PRA Grace Time:								
PRA Interval:		240						
PRA Action:		continu	e					
User Agreement Statu	s:	NotEnak	oled					
System Name:		MGARCA	RZ-WS01					
System Domain:		cisca.co	m					
System User:		mgarca	z					
User Domain:		CISCO						
AV Installed:		McAfee	VirusScan Enterpr	rise;8.8.0	.975;7227;10/	13/2013;McAfeeA	V,Cisco Security Agent;6.0.2.130;;;Cisco	AV
AS Installed:		Window	s Defender;6.1.76	600.1638	5;1.95.191.0;1	1/19/2010;Micro	softAS	
Posture Report								
Posture Status:		Complia	nt					
Logged At:		2013-12	2-23 15:21:34.90	2				
Posture Policy Details								
Policy	Name		Enforcement	Statu	Passed	Failed	Skipped Conditions	
nosture initial	file rec	uire	Mandatory		file condition	1		

ASA에서 디버깅

ASA에서 다음 디버그를 활성화할 수 있습니다.

- debug aaa url-redirect
- aaa 권한 부여 디버그
- radius 동적 권한 부여 디버그
- 디버그 radius 디코딩
- radius 사용자 cisco 디버그

에이전트에 대한 디버그

NAC Agent의 경우, GUI에서 또는 CLI(CCAAgentLogPackager.**app**)를 통해 시작되는 Cisco Log Packager로 디버그를 수집할 수 있습니다.

🕂 Cisco Log Pa	ackager v1.7.0.11						
cisco.	Cisco Log Packager						
	Cisco Log Packager collects information for product support requests. The information is stored in a ZIP archive that can be protected by a password.						
Protect dat	ta with following password:						
Collect Da	ata Show Log Locate Report File Cancel	Exit					

팁: TAC(Technical Assistance Center) 툴을 사용하여 결과를 디코딩할 수 있습니다.

웹 에이전트에 대한 로그를 검색하려면 다음 위치로 이동하십시오.

- C: > Document and Settings > *<user*> > Local Settings > Temp > webagent.log(TAC 툴로 디 코딩됨)
- C: > 문서 및 설정 > *<사용자*> > 로컬 설정 > 임시 > webagentsetup.log

참고: 로그가 이러한 위치에 없는 경우 TEMP 환경 변수를 확인합니다.

NAC Agent 상태 실패

포스처가 실패하면 사용자에게 다음과 같은 사유가 표시됩니다.



그러면 사용자는 다음과 같이 구성된 경우 교정 작업을 수행할 수 있습니다.

CISCO Client Provisioning Portal		
Information	Cisco NAC Agent	Cancel About
	There is at least one mandatory requirement failing. You are required before you can access the network. Repair Show Details Continue System Check Complete System Check Complete System Check Complete	to update your system

관련 정보

- 보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- <u>Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1</u>
- Cisco Identity Services Engine 사용 설명서, 릴리스 1.2
- <u>기술 지원 및 문서 Cisco Systems</u>

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.