# FCM(Secure Firewall Chassis Manager)에 대한 ISE Radius 인증 구성

## 목차

소개

이 문서에서는 ISE를 사용하는 Secure Firewall Chassis Manager에 대한 RADIUS 권한 부여/인증 액세스를 구성하는 방법에 대해 설명합니다.

# 사전 요구 사항

#### 요구 사항

Cisco에서는 다음 항목에 대해 숙지할 것을 권장합니다.

- FCM(보안 방화벽 섀시 관리자)
- Cisco ISE(Identity Services Engine)
- Radius 인증

사용되는 구성 요소

- Cisco Firepower 4110 Security Appliance FXOS v2.12
- Cisco ISE(Identity Services Engine) v3.2 패치 4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

설정

보안 방화벽 섀시 관리자

1단계. firepower Chassis Manager GUI에 로그인합니다. 2단계. 플랫폼 설정으로 이동합니다.

verview Interfaces	s Logical Dev	vices Security Engli	ne Platform S	Settings				Sys	tem Tools Help adn
FPR4K-1-029A78 Model: Cisco Fi	B 172.16. repower 4110	0.130 Security Appliance	Version:	2.12(0.8) Op	erational State: <b>O</b>	perable	Chassis	Uptime 00:0	5:02:19 <b>じ</b> の①
DNSOLE MGMT USB		Power 2 - Removed		Network Module 1	7 7 8	Module 2 : Empty	Netv	vork Module 3 : l	Empty
FAULTS 3(3) © CRITICAL	<b>0(0)</b>	INTERFACES 3 ODWN	5 10 10	INSTANCES O O DOWN	1 100 UP	LICENSE Smart Agent UNREGISTERED	INVENTORY 1(1) Security Engine	<b>6(6)</b> ☆ Fans	1(2) ⇒ Power Supplies
Select All Faults Cancel	Selected Faults A	cknowledge							
Severity	Description				Cause	Occurrence	т	ïme	Acknowledged
CRITICAL	FPGA version l	ower than 2.00 is detected	A critical upgrade	e from the firmwar	fpga-upgrade-requ	uired 1	2022-02-20	T22:32:45.641	no
	Network Modul	le 3 removed when in onlir	e state. It is recon	nmended to set m	module-suprise-ren	noval 1	2022-11-07	T09:03:02.022	no
uccessful Login in last 24 hr	rs - <u>View Details</u>   Th	u Feb 01 2024 at 17:00:55 f	rom - 172.16.0.35						نداند cisc

3단계. 왼쪽 메뉴에서 AAA 위를 클릭합니다. Radius를 선택하고 새 RADIUS 제공자를 추가합니다.

Overview Interfaces Logic	al Devices Security Engine	Platform Settings		System	Tools Help admin
NTP	LDAP RADIUS TACACS				
SSH					
SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
AAA					
Syslog	Retries:* 1				
DNS	RADIUS Providers				
FIPS and Common Criteria					Add
Access List					
MAC Pool	Hostname	Order	Service	Auth Port	
Resource Profiles					
Network Control Policy					
Chassis URL					
	Save Cancel				
8 Successful Login in last 24 hrs - View (	Details   Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35			.1 1.1 1. cisco

4단계. 프롬프트 메뉴에 Radius 제공자의 요청 된 정보를 채웁니다. OK(확인)를 클릭합니다.

Overview Interfaces Logi	cal Devices Security Engin	e Platform Settings			System Tools	Help admin	
Overview         Interfaces         Logic           NTP         SSH         SNMP           HTTPS         AA         Syslog           DNS         FIPS and Common Criteria         Access List           MAC Pool         Resource Profiles         Network Control Policy           Chassis URL         Chassis URL         Control Policy	LDAP     RADIUS     TACAC       Properties     Timeout.*     5     Sec       Retries.*     1     RADIUS Providers	Platform Settings   Add RADIUS Provider  Hostname/FQDN/IP Address:*  Order:*  Key:  Confirm Key:  Authorization Port:*  Timeout:*  Retries:*	172.16.0.12 lowest-available •••••••• 1812 5 1	Image: Set: No   Set: No   Secs   Cancel	System Tools	Help admin	
8 Successful Login in last 24 hrs - <u>View</u>	Save Cancel	rom - 172.16.0.35				ahaha cisco	

5단계. System(시스템) > User Management(사용자 관리)로 이동합니다.

Overview Interfaces Logic	al Devices Security Engi	Platform Settings				System <sup>1</sup> Too	ls Help admin
				Configuration	Licensing	Updates	Jser Management
SSH SNMP HTTPS ► AAA	Properties Timeout:* 5 Se	c5					1
Syslog DNS FIPS and Common Criteria	Retries:* 1 RADIUS Providers						Add Q
Access List	Hostname	Order	Ser	vice	Auth Port		
Resource Profiles Network Control Policy Chassis URL	172.16.0.12	1	aut	horization	1812		2
	Save						
avascript:void(0) last 24 hrs - View D	etails   Thu Feb 01 2024 at 17:00:55	from - 172.16.0.35					սիսիս

6단계. Settings(설정) 탭을 클릭하고 드롭다운 메뉴에서 Default Authentication(기본 인증)을 Radius로 설정한 다음 아래로 스크롤하여 컨피그레이션을 저장합니다.

Overview Interfaces Logica	al Device	es Security Engine Platform Settings			System	Tools Help admin
			Configuration	Licensing	Updates	User Management
Local Users Settings						
Default Authentication	Local Local	*Local is fallback authentication method				
Console Authentication	RADIUS LDAP	• -				
Remote User Settings	TACACS	;				
Remote User Role Policy	None	No-Login				
Local User Settings						
Password Strength Check	Enab	le				
History Count	5	(0-disabled,1-15)				
Change Interval	48	🕑 (1-730 hours)				
Change Count	2	(1-10)				
No Change Interval		(1-730 hours)				
Days until Password Expiration	0	(0-never,1-9999 days)				
Password Expiration Warning Period	0	(0-9999 days)				
Expiration Grace Period	0	(0-9999 days)				
Password Reuse Interval	0	(0-disabled,1-365 days)				
Session Timeout(web UI,ssh,telnet)	600	(0-never.3600 seconds)				
8 Successful Login in last 24 hrs - View De	<u>etails</u>   Thu	Feb 01 2024 at 17:00:55 from - 172.16.0.35				cisco



참고: 이 시점에서 FCM 컨피그레이션이 완료되었습니다.

ISE(Identity Service Engine)

1단계. 새 네트워크 디바이스를 추가합니다.

왼쪽 상단 모서리에 있는 버거 아이콘 ≡ > 관리 > 네트워크 리소스 > 네트워크 장치 > +Add로 이동 합니다.

≡ Cisco ISE			Administration · Net	work Resources			🔺 Evaluation Mode 18 Days Q 💿 👼
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More $\vee$
Network Devices		-					
Default Device	Network	Devices					
Device Security Settings		_					Selected 0 Total 0 🧭 🚳
	0 Edit + Ad	d Duplicate 🕁 Import	🗄 Export 🗸 🛛 🙆 Generate Pi	AC 🚦 Delete 🗸			$\sim 10^{-10}$
	Name	∧ IP/Mask	Profile Name	Location Type		Description	
				No data available			

2단계. 새 네트워크 디바이스 정보에 대해 요청한 매개변수를 채웁니다.

2.1 RADIUS 확인란을 선택합니다

2.2 FCM Radius 컨피그레이션과 동일한 공유 암호 키를 구성합니다.

2.1 아래로 스크롤하여 Submit(제출)을 클릭합니다.

🔳 Cisco ISE	Administration - Network Resources	▲ Evaluation Mode 18 Days Q. ③ 58 ④
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxGrid Direct Connectors Location Services	
Network Devices Default Device Device Security Settings	Network Devices List > New Network Device Network: Devices	
	Name IPR-4110 Description	
	E PAGNIN U *P1 122.16.6.130 / 32 O	
	Device Profile Crico v O	
	Model Name F96-410 V	
	Network Version 2.12	
	Location All Locations V Set To Default	
	IPSEC In IPSEC Device Set To Default	
	Device Types V Set To Default	
	RADIUS Authentication Settings	
	RADIUS UDP Settings Protocol RADIUS	
	Shared Secret Show	
	Use Second Shared Shared	
	Secret Show	

#### 3단계. 새 디바이스가 Network Devices(네트워크 디바이스)에 표시되는지 확인합니다.

≡ Cisco ISE		Administration - Netv	vork Resources			A Evaluation Mode 18 Days Q (	D ,79	0
Network Devices	Network Device Groups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More $\vee$		
Network Devices	Network Devices							
Default Device	Network Devices							
Device Security Settings						Selected 0 Total 1	8 <b>0</b>	
	🖉 Edit 🕂 Add 📋 Duplicate 🅁 Import	🏝 Export 🖂 🔒 Generate PA	C 🗍 Delete 🗸			AI	~ 7	
	Name	lame Location	Туре	Description				
	FPR-4110 172.16.0 🗰 Cisco	All Locations	All Device Types					
				_				

4단계. 필요한 사용자 ID 그룹을 생성합니다. 왼쪽 상단 구석에 있는 버거 아이콘 ≡ > 관리 > 신원 관 리 > 그룹 > 사용자 ID 그룹 > + 추가

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💿 🗔 💿
Identities Groups External Identit	ty Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 12 Ø		Selected O Total 9 🧭 🚳
> 🛅 Endpoint Identity Groups	🖉 Edit 🕂 Add 🔵 Delete 🗸 🤠 Import 🖞 Export 🗸	All 🗸 🏹
> 🛅 User Identity Groups	Name   Description	
	ALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default) User Group	
	Employee Default Employee User Group	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default) User Group	
	GuestType_Contractor (default)     Identity group mirroring the guest type	
	Af GuestType_Daily (default)     Identity group mirroring the guest type	
	GuestType_SocialLogin (default)     Identity group mirroring the guest type	
	GuestType_Weekly (default)     Identity group mirroring the guest type	
	Ar OWN_ACCOUNTS (default)     Default OWN_ACCOUNTS (default) User Group	

5단계. 컨피그레이션을 저장하려면 Admin User Identity Group(관리자 사용자 ID 그룹)의 이름을 설 정하고 Submit(제출)을 클릭합니다.

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💮 👼 🗇
Identities Groups External Identities	entity Sources Identity Source Sequences Settings	
Identity Groups       Image: Constraint of the second	User Identity Group > New User Identity Group           * Name         FRR-4110-Admin           User Group for Administratos:         User Group for Administratos:	Cancel

5.1 ReadOnly 사용자에 대해 동일한 프로세스를 반복합니다.

≡ Cisco ISE		Administration - Identity Management		▲ Evaluation Mode 18 Days Q ⑦ 53 @
Identities Groups Ex	cternal Identity Sources Identity Sou	ce Sequences Settings		
Identity Groups	User Identity Groups > New User Identity Composition  Co	nthy Group Only Driv Users.	Submit	Cancel

6단계. User Identity Groups(사용자 ID 그룹) 아래에 새 사용자 그룹이 표시되는지 확인합니다.

E Cisco ISE	Adm	inistration - Identity Management	▲ Evaluation Mode 18 Days Q ③ 🖉
dentities Groups External Iden	tity Sources Identity Source Sequences	Settings	
Identity Groups	User Identity Groups		
< The second sec	🖉 Edit 🕂 Add 🔕 Delete 🗸 🕁 Import d	û Export ∨	Selected O Total 11 🤤 🏟
> 🛅 User Identity Groups	Name ^	Description	
	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group	
	Employee	Default Employee User Group	
	C 분 FPR-4110-Admin	User Group for Administrator.	
	FPR-4110-ReadOnly	User Group for Read Only Users.	
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group	
	C & GuestType_Contractor (default)	Identity group mirroring the guest type	
	GuestType_Daily (default)	Identity group mirroring the guest type	
	GuestType_SocialLogin (default)	Identity group mirroring the guest type	
	GuestType_Weekly (default)	Identity group mirroring the guest type	
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group	

7단계. 로컬 사용자를 생성하고 해당 Responder 그룹에 추가합니다. 버거 아이콘으로 이동 ≡ > 관 리 > 신원 관리 > ID > + 추가.

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 🗇 🖟 🕸
Identities Groups Ext	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 0 💋 🚳
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🖒 Export 🗸 📋 Delete 🗸 🚺 Duplicate	$_{ m All}$ $\sim$ $~$ $\nabla$
	Status Username  Description First Name Last Name Email Address User Identity Groups Admin	
	No data available	

7.1 관리자 권한이 있는 사용자를 추가합니다. 이름, 비밀번호를 설정하고 FPR-4110-Admin에 할당 한 후 아래로 스크롤하고 Submit(제출)을 클릭하여 변경 사항을 저장합니다.

= Cisco	o ISE				Administration - Identity Management	Liveluation Mode 18 Days	0,0	53 4	0
Identities	Groups	External Identity Sources	Identity Source Sequences	Settings					
Users Latest Manual Net	work Scan Res	<ul> <li>Network Access</li> <li>Usename</li> <li>Status</li> <li>Account Name Atlas</li> <li>Email</li> <li>Passwords</li> </ul>	i User cisce_sdmin E Enabled ~						
		Password Type: in Password Lifetine With Expiration Never Expires (	innet Users V	Re-Enter Password					
		* Login Password Enable Password			Generate Password           Generate Password         Image: Construct Password				
		User Informatio     Account Option     Account Disable	n 15 e Policy						
		✓ User Groups	tmin 🗸 🕘 😁						

7.2 읽기 전용 권한이 있는 사용자를 추가합니다. 이름, 비밀번호를 설정하고 FPR-4110-ReadOnly에 할당한 후 아래로 스크롤하고 Submit(제출)을 클릭하여 변경 사항을 저장합니다.

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 🔘 🕫 🕸
Identities Groups I	xternal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Vetwork Access User Username Gescuredonly Status Account Name Allas Email		
	V Passwords Password Type: Internet Users: V Password Lifetime: V Password Lifetime: V Password in starts in 60 days Never Expiret ()		
	Password Re-Enter Password * Login Password Citable Password	Generate Password     O       Generate Password     O	
	Vuer Information     Account Options     Account Disable Policy		
	✓ User Groups E FPR-4110-ReadOny ✓ ③ ●		

7.3 사용자가 Network Access Users(네트워크 액세스 사용자)에 있는지 확인합니다.



8단계.관리자 사용자에 대한 권한 부여 프로파일을 생성합니다.

FXOS 섀시에는 다음과 같은 사용자 역할이 포함됩니다.

- 관리자 전체 시스템에 대한 완전한 읽기 및 쓰기 액세스. 기본 관리자 계정은 기본적으로 이 역할에 할당되며 변경할 수 없습니다.
- 읽기 전용 시스템 상태를 수정할 권한이 없는 시스템 컨피그레이션에 대한 읽기 전용 액세스
- 운영 NTP 컨피그레이션, Smart Licensing용 Smart Call Home 컨피그레이션, 시스템 로그 (syslog 서버 및 결함 포함)에 대한 읽기 및 쓰기 액세스 시스템의 나머지 부분에 대한 읽기 액 세스.
- AAA 사용자, 역할 및 AAA 구성에 대한 읽기 및 쓰기 액세스. 시스템의 나머지 부분에 대한 읽기 액세스

각 역할의 특성:

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operations"

```
cisco-av-pair=shell:roles="읽기 전용"
```



참고: 이 설명서는 admin 및 read-only 특성만 정의합니다.

버거 아이콘으로 이동 ≡ > 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일 > +추가.

권한 부여 프로파일의 이름을 정의하고, Access Type(액세스 유형)을 ACCESS\_ACCEPT로 남겨두 고 Advanced Attributes Settings(고급 특성 설정)에서 cisco-av-pair=shell:roles="admin"을 추가하 고 Submit(제출)을 클릭합니다.

≡ Cisco I	ISE	Policy - Policy Elements	7 Days (	20	6	٥
Dictionaries	Conditions	Results				_
Authentication	>	Authorization Profiles > FPR-4110-Admins				
Authorization	~	Authorization Profile				
Authorization Profi	lles	* Name FPR-4110-Admins				
Downloadable ACI	Li .	Description				
Profiling	>					
Posture	>	* Access Type ACCESS_ACCEPT V				
<b>Client Provisioning</b>	>	Network Device Profile 🗰 Disco 🗸 🕀				
		Service Template				
		Track Movement				
		Agenties Posture 0				
		Passive identity (racking U)				
		ALL IPv6 (Fitter=D)				
		Advanced Attributes Settings				
		Eiscocisco-av-pair     * shell:roles*admin*     > = +				
		✓ Attributes Details				
		Access Type - ACCESS ACCOPT Access Type - ACCESS ACCOPT	1			
		Sale Sale Sale Sale Sale Sale Sale Sale	mit	Ci	ncel	

8.1 이전 단계를 반복하여 읽기 전용 사용자에 대한 권한 부여 프로파일을 생성합니다. 이번에는 Administrator 대신 읽기 전용 값으로 Radius 클래스를 만듭니다.

= Cisco ISE	Policy - Policy Elements	🛕 Evaluation Mode 18 Days Q 🕥 🔗 🔅
Dictionaries Conditions	Results	
Authentication >	Authorization Profiles > New Authorization Profile Authorization Profile	
Authorization Profiles Downloadable ACLs	* Name FPR-4110-ReadOnly Description	
Profiling > Posture >	* Access Type ACCESS_ACCEPT V	
Client Provisioning >	Network Device Profile 🗰 Cisco 🗸 🕀	
	Service Template  Track Movement	

ACL IPv6 (Filter-ID)		
Advanced Attributes Settings       Image: Ciscocisco-av-pair     v     * shelt:roles=*read-only*     v		
Attributes Details Access type - ACCESS, ACCEPT		
Globa-výar = thetroises "read-only"	Submit	Cancel

9단계.FMC IP 주소와 일치하는 정책 집합을 생성합니다. 이는 다른 디바이스에서 사용자에게 액세 스 권한을 부여하는 것을 방지하기 위한 것입니다.

좌측 상단 모서리에 ≡ > Policy > Policy Sets > Add 아이콘 기호로 이동합니다.

= Cisco ISE		Policy	Policy Sets			A Evaluation Mode 1	7 Days	Q (1)	6 B
Policy Sets					Reset	Reset Policyset P	litcounts		Save
Status Policy Set Name	Description	Conditions			Allowed Protocol	s / Server Sequence	Hits	Actions	View
Q Search									
			+						
O Default	Default policy set				Default Network	Access 🥒 🕂	58	$\langle \hat{Q} \rangle$	>
							Reset		Save

9.1 정책 세트의 맨 위에 새 라인이 배치됩니다. 새 조건을 구성하려면 Add(추가) 아이콘을 클릭합 니다.

۲	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	e Hits	Actions	View
9	Search							
	۲	New Policy Set 1		+	Select from list 🥒 -		ŵ	>
	•	Default	Default policy set		Default Network Access 🥒 -	58	<b>\$</b>	>

9.2 FCM IP 주소와 일치하는 RADIUS NAS-IP-Addressattribute에 대한 상위 조건을 추가한 다음 Use(사용)를 클릭합니다.

Library	
Search by Name	
	0 t 🕈
:: 📑 5G	
: Catalyst_Switch_Local_Web_Authentication	
🗄 🖹 Radius	
# E Switch_Local_Web_Authentication	
: [] Switch_Web_Authentication	
H Wired_802.1X	
# 🖪 Wired_MAB	
E Wireless_802.1X	
# Wireless_Access	
# E Wireless_MAB	
: WLC_Web_Authentication	

Editor

0

als 👻 Attri	Select attribute for condit	ion		×		View
	O 0 1 8	° 🛛 🖉 🗏 O	1 0	£ 🕈	Wrong value	
to its not	Dictionary	Attribute	ID	Info	Duplicate	
	All Dictionaries	Attribute	ID			>
	Microsoft	MS-User-IPv4-Address	61	0		>
	Network Access	ISE Host Name		0		
	Radius	DNS-Server-IPv6-Address	169	0		
	Radius	Framed-IP-Address	8	0		iave
	Radius	Framed-IPv6-Address	168	0		
	• Radius	NAS-IP-Address	4	0		
	Radius	Stateful+IPv6+Address+Pool	172	0		



#### 9.3 완료되면 저장을 클릭합니다.

≡ Cisco	ISE		Policy - Policy Sets		A Evaluation Mode	7 Days	Q (0)	Ø 6
Policy Sets				Reset	Reset Policyset H	litcounts		Save
🕣 Statu	s Policy Set Name	Description	Conditions	Allowed Protocol:	/ Server Sequence	Hits	Actions	View
Q Sear	ch							
٥	New Policy Set 1		Radius-NA5-IP-Address EQUALS 172.16.0.130	Default Network	Access 🐼 🗸 +		@>	>
۰	Default	Default policy set		Default Network /	Access 🥒 +	58	礅	>
						Reset		Save



팁: 이 연습에서는 Default Network Access Protocols(기본 네트워크 액세스 프로토콜) 목록 을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

10단계. 행의 끝에 있는 > 아이콘을 눌러 새 정책 집합을 확인합니다.

Policy Sets			Reset	Reset Policyset Hitcor	unts	Save
Status Policy Set Name	Description 0	Conditions	Allowed Protocols	/ Server Sequence H	its Actions	s View
Q Search						
New Policy Set 1		Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🛛 🗸 +	¢	>

10.1 Authorization Policy(권한 부여 정책) 메뉴를 확장하고 (+)를 클릭하여 새 조건을 추가합니다.

$\lor$ A	uthorization	n Policy (1)						
					Results			
6	Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
	Q Search	h						
	۰	Authorization Rule 1		+	Select from list	/ + Select from list	0 +	{}

10.2 AttributeName Equals User Identity Groups(AttributeName Equals User Identity Groups: FPR-4110-Admins)(7단계에서 만든 그룹 이름)와 일치하는 조건을 설정하고 Use를 클릭합니다.

Cisco IC	Conditions Studio			a Carr	Policy Cote					A Bashadaa Ma	0	×
Statu	Library	Editor										_
0, 5	Search by Name		Identity0	roup Na	sme						_ `	
	H 🗄 56 📀	-	Set to 'Is	Sele	ect attribute for condition	n 8 8 8 8	0 1	0 t 9	Ď	Duplicate	Save	
Authen	E BYOD_is_Registered				Dictionary	Attribute	ID	Info				
Author	E Catalyst_Switch_Local_Web_Authentication				All Dictionaries	Attribute	ID	-				)
Authori	E Compliance_Unknown_Devices			+	GWA IdentityGroup	CWA_ExternalGroups		0				
	E Compliant_Devices				IdentityGroup	Name		0				
• s	EAP-MSCHAPv2				InternalUser	IdentityGroup		0				
Q :	EAP-TLS			*	PassiveID	PassiveID_Groups		0				
	E Guest_Flow			*	administrator	ExternalGroups		0				
	E MAC_In_SAN O											
	II Network_Access_Authentication_Passed											
	E Non_Cisco_Profiled_Phones											
	E Non_Compliant_Devices											
	🗄 💽 Radius 📀											
	Switch_Local_Web_Authentication											
										Close	Use	

brary	Edi	litor			
Search by Name			IdentityGroup Name		(
♥ □ 0 <b>*</b> ♥ 묘 Φ 8 □ 8 8 0	10 E 🕈		Equals VUser Identity Groups:FPR-4110-		
50			Admin V		
BYOD_is_Registered			Set to 'is not'	Duplicate	Save
Catalyst_Switch_Local_Web_Authentication			NEW AND OR		
Compliance_Unknown_Devices					
Compliant_Devices					
EAP-MSCHAPv2					
EAP-TLS					
Guest_Flow					
MAC_in_SAN					
Network_Access_Authentication_Passed					
Non_Cisco_Profiled_Phones					
Non_Compliant_Devices					
🖪 Radius					
. Switch Local Web Authentication					

10.3단계 Authorization(권한 부여) 정책에 새 조건이 구성되었는지 확인한 다음 Profiles(프로필) 아 래에 사용자 프로필을 추가합니다.

$\vee$ Authorizatio	n Policy (1)								
				Results					
💿 Statur	Rule Name	Conditions		Profiles		Security Groups		Hits	Actions
Q Searc	h.								
٥	Authorization Rule 1	A IdentityGroup Name EQUALS User Identity Groups:FPR-4110-Admin		FPR-4110-Admins ×	<u>~</u> +	Select from list	~+		٢
۰	Default			DenyAccess	/+	Select from list	1+	•	٨

Reset Save

11단계. 읽기 전용 사용자에 대해 9단계에서 동일한 프로세스를 반복하고 Save(저장)를 클릭합니 다.

다음을 확인합니다.

1. 새 Radius 자격 증명을 사용하여 FCM GUI에 로그인합니다.

2. 버거 아이콘 = > Operations(운영) > Radius > Live logs(라이브 로그)로 이동합니다.

3. 표시되는 정보는 사용자가 성공적으로 로그인했는지 보여줍니다.

E Cisco ISE			Operations · RAD	DIUS		🛦 Evaluation Mode 17 Days Q. (1) 58 (1)
Live Logs Live Sessions						
Misconfigured Supplicants		Misconfigured Network Devices 📀		RADIUS Drops	Client Stopped Responding ()	Repeat Counter 🕕
0		0		1	0	0
					Refrest Neve	Show Latest 20 records U Utilin Latest 3 hours U
🖉 🖆 Reset Repeat Counts 🖄 Export To 🛇						Fitter 🗸 🔘
Time Status	Details Repea	Identity Endpoint ID	Endpoint Authenti Autho	oriz Authoriz IP Address	Network De Device Port Identity Group Posture	Server Mdm Ser IMEISV Usecasi
×	~	Identity Endpoint ID	Endpoint Pr Authenticat Autho	rizatic <u>Authorizatic</u> <u>IP Address</u> ~	Network Device Port Identity Group Posture Sta	Server Mdm Serve IMEISV Usecase
Feb 03, 2024 01:51:51.0	à	cisco_readonly	New Polic New Po	olic FPR-4110	FPR-4110 User Identity Group	marpath/SE
Feb 03, 2024 01:50:48.9	0	cisco_admin	New Polic New P	olic FPR-4110	FPR-4110 User Identity Group:	marpatinISE

4. Secure Firewall 섀시 CLI에서 로깅된 사용자 역할을 확인합니다.

FPR4K-1-029A78B# security	scope se server	service-pr	ofile
FPR4K-1-029A78B# FPR4K-1-029A78B / Remote User cisco	scope security /security # show o_admin:	remote-user	detail
Description: User Roles: Name: adm Name: rea	nin ad-only		
FPR4K-1-029A78B /	/security #		

1. ISE GUI에서 버거 아이콘 = > Operations(운영) > Radius > Live logs(라이브 로그)로 이동합니다

1.1 로그 세션 요청이 ISE 노드에 도달하는지 확인합니다. 1.2 실패한 상태의 경우 세션의 세부 정보를 검토합니다.

= Cis	co ISE					c	Operations • R	ADIUS							🔺 Evalua	tion Mode 18 Day	n Q @	523	٥
Live Logs	Live Sessions																		
Misco	nfigured Supplicants 🕕			Mise	configured Network	Devices 🕕		RA	DIUS Drops 📀				Client Stoppe	d Responding			Repeat	Count	or ()
	0				1				1					0				3	
ø	Seset Repeat Counts	🖞 Export To 🗸												Refresh Never	V Lates	t 20 records 、	Within Last 3 P	iours	~ >
	Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address		Network De	Device Port	Identity Group	Posture	Server	Mdr	m Sei
$\times$				~	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~	Network Device	Device Port	Identity Group	Posture Sta	Server	Md	n Sen
	Feb 02, 2024 07:32:18.8	۰	à		cisco_admin			Default >>	Default				FPR-4110		User Identity Group	- E	marpatin/SE		
	Feb 02, 2024 07:23:20.1		à		cisco_readonly			Default >>	Default >>	PermitAcc			FPR-4110		User Identity Group	- E	marpatin/SE		
	Feb 02, 2024 07:15:32.2		à		cisco_admin			Default >>	Default >>	PermitAcc			FPR-4110		User Identity Group	- E	marpatin/SE		

2. Radius Live 로그에 표시되지 않는 요청의 경우 UDP 요청이 패킷 캡처를 통해 ISE 노드에 도달 하는지 검토합니다.

버거 아이콘 ≡ > Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > TCP dump(TCP 덤프)로 이동합니다. UDP 패킷이 ISE 노드에 도착하는지 검토하기 위해 새 캡처를 추가하고 파일을 로컬 시스템에 다운로드합니다.

2.1 요청한 정보를 입력하고 아래로 스크롤한 다음 Save(저장)를 클릭합니다.

E Cisco ISE	Operations - Troubleshoot	A Evaluation Mode 17 Days	Q (0)	58 O
Diagnostic Tools Downloa	Logs Debug Wizard			
General Tools 🗸	TCP Dump > New			
RADIUS Authentication Troubl	Add TCP Dump			
Evaluate Configuration Validat	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.			
Posture Troubleshooting Agentiess Posture Troublesho	Need Nama* marpatinSE v			
EndPoint Debug				
Session Trace Tests	Terranis Interface* GigabitEhemet 0 (Up, Running) v 🕐			
TrustSec Tools	Filter         ()           ()			

2.2 캡처를 선택하고 시작합니다.



2.3 ISE 캡처가 실행되는 동안 Secure Firewall Chassis에 로그인을 시도합니다

2.4 ISE에서 TCP 덤프를 중지하고 파일을 로컬 시스템에 다운로드합니다.

2.5 트래픽 출력을 검토합니다.

예상 출력:

패킷 No1. 포트 1812(RADIUS)를 통해 보안 방화벽에서 ISE 서버로 요청 패킷 No2. 초기 요청을 수락하는 ISE 서버 응답입니다.



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.