Configure Cisco Firepower and Cisco ISE for AnyConnect VPN Authentication and Dynamic Group Policy Mapping

Device Versions in this document:

- 1. Cisco ISE Version 2.4 Patch 11
- 2. Cisco FMC Version 6.5.0.4
- 3. Cisco FTD Version 6.5.0.4

In this article we will see how to configure Cisco Firepower using Firepower Management Centre (FMC) and Cisco ISE for AnyConnect VPN authentication and authorisation using dynamic Group Policy mapping from ISE. For example, you have different rules and ACL for Employees, Vendors, etc, you can create different Group Policy with all these rules and based on used connecting via AnyConnect, you can dynamically assign Group Policy from ISE. If vendor user connects, he will be allocated Vendor VPN Group Policy, hence restricting with Vendor ACL and other rules.

Cisco ISE is a AAA server supporting RADIUS (as default) and TACACS+ protocol for Authentication Authorization and Accounting. We can use ISE with Firepower to authenticate VPN clients and apply specific VPN group policy based on centralised directory like MS Active Directory (AD).

Steps Overview:

- 1. Connect Cisco ISE with Cisco FTD and FMC and configure Cisco FTD VPN Policy via FMC to authenticate and authorise thru Cisco ISE
- 2. Configure Cisco ISE parameters for VPN Authentication
- 3. Configure Cisco ISE parameters for Dynamic Authorisation Authorisation Policy
- 4. Configure different Cisco ISE policy for each VPN user category (e.g. Vendor, Employee, etc)
- 5. Testing and verification of the policy

Step 1 – Connect Cisco ISE with Cisco FTD and FMC and configure Cisco FTD VPN Policy via FMC to authenticate and authorise thru Cisco ISE

In this phase, we will configure Cisco ISE to allow AAA requests from Cisco FTD and FMC. When a VPN user connects, FTD will be sending request to ISE. Adding FMC is optional, but can be used for FMC GUI/CLI login authentication via ISE using centralised directory. You can skip this step, if FTD and FMC is already added to ISE. Also, we will configure VPN Policy to user ISE for Authentication, Authorisation and Accounting via FMC.

- 1. Login to Cisco ISE
- 2. Navigate to Administration → Network Resources → Network Devices
- 3. Click **Add**, and configure the below parameters:
 - a. Name and Description As you like
 - b. IP address Configure FTD inside, and outside interface (VPN Interface) IPs. If VPN connects to a different interface, please include that interface IP as well. Because FTD will send request to ISE from interface where VPN is connected.
 - c. Configure Device type, recommended to add new, so that it doesn't disturb any of your existing settings.
 - d. Configure Shared Key, this key will be later used with FTD/FMC configuration of Cisco ISE in FMC
- 4. Follow the same above steps to add FMC.
- 5. Login to Cisco Firepower Management Centre (FMC)
- 6. Navigate to **Objects** → **RADIUS Server Group** → **Add New**
- 7. Configure the name, description and add all you PSN ISE IP addresses
- 8. Save the configuration
- 9. Navigate to **Device** → VPN → Remote Access
- 10. Open your remote access policy
- 11. Edit your VPN policy
- 12. Navigate to AAA tab
- 13. Select ISE-AAA (RADIUS) under your Authentication, Authorisation and Accounting Server
- 14. Save the setting and Deploy the Change

Identity Services Engine Home Context Visibility Operations Policy - Administration Summary Endpoints Guests Vulnerability Threat + System METRICS Total Endpoints Active Endpoints • Active Endpoints • Maintenant	tion → Work Centers Network Resources pxGrid Services nt Network Device Groups s Network Device Profiles External RADIUS Servers ce RADIUS Servers
•!!!!. Identity Services Engine Home Context Visibility • System • Identity Management • Network Resources • Device • Network Devices Network Device Groups Network Device Profile Image: Network Devices Network Devices Network Devices Default Device Default Device Network Devices	
Device Security Settings <pre> Edit</pre> Cisco-FTD Network Devices * Name Cisco-FTD Description ETD Errowall	te 🕼 Import 🕼 Export 👻 🕜 Generate PAC 🗙 Delete
IP Address * IP : INTERNAL INTERFACE IP IP Address * IP : EXTERNAL VPN INTERFACE IP IP Address * IP : III = 1000000000000000000000000000000000	/ 32 / 32 / 32 / 32
* Device Profile Group	
Location All Locations Set To Default IPSEC No Set To Default Device Type Firewall Set To Default CREATE NEW IF RADIUS Authentication Settings	YOU DO NOT HAVE FOR FIREWALL
RADIUS UDP Settings Protocol RADIUS * Shared Secret Use Second Shared Secret ()	() Show

Network Devices List > Cisco-Firepower-Management Network Devices										
* Name Cisco-Firepower-Madia										
Description FMC										
IP Address V *IP: FMC MANAGEMENT IP / 32										
IP Address V *IP: FMC INSIDE INTERFACE IP / 32										
* Device Profile 🗱 Cisco 👻 🕀										
Model Name										
Software Version										
* Network Device Group										
Location All Locations 📀 Set To Default										
IPSEC No 📀 Set To Default										
Device Type Firewall-Manage Set To Default CREATE SEPERATE DEVICE TYPE FOR FMC										
✓ RADIUS Authentication Settings										
DADIUS UDD Settings										
Protocol RADIUS										
* Shared Secret Show										
Use Second Shared Secret 🗌 (i)										
Show										
CoA Port 1700 Set To Default										
RADIUS DTLS Settings ()										
DTLS Required [] ()										
CoA Port 2083 Set To Default										
Issuer CA of ISE Certificates for CoA Select if required (optional)										
DNS Name										
General Settings										
* Key Encryption Key										
* Message Authenticator Code Key Show										
Key Input Format ASCII HEXADECIMAL										



Edit RADIUS Server Group				?	×		
Name:*	ISE-AAA						
Description:	AAA ISE						
Group Accounting Mode:	Single]					
Retry Interval:*	10	(1-10) Seconds					
Realms:	~	•]					
Enable authorize only							
Enable interim account update							
Interval:*	24	(1-120) hours					
Enable dynamic authorization							
Port:*	1700	(1024-65535)					
RADIUS Servers (Maximum 16 ser	vers)			0	-1		
IP Address/Hostname							
ADD ISE	ADD ISE IP ADDRESS						
10.04.07			P	ij	Н		
					Н		
		Save	Car	ncel	þ		



			O Add
Name	Status	Last Modified	
Ingland Realistican IN	Targeting 1 devices Up-to-date on all targeted devices	2020-08-12 08:45:37	

Connection Profile Access Interfaces Advanced			
			0
Name	ААА	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	05
And areast Associations (M)	Authentication: ISE-AAA (RADIUS) Authorization: ISE-AAA (RADIUS) Accounting: ISE-AAA (RADIUS)	🕒 DftGrpPolicy	

Edit Connection Profile		? ×					
Connection Profile:* Group Policy:* DfltGrpPolicy Edit Group Policy							
Client Address Assignment A	AA Aliases						
Authentication							
Authentication Method:	AAA Only						
Authentication Server:	ISE-AAA (RADIUS)						
Use secondary authentication							
Authorization Server:	ISE-AAA (RADIUS)						
Accounting		-					
Accounting Server:	ISE-AAA (RADIUS)						
 Advanced Settings 	•						

In this phase we will configure parameters used for VPN authentication in Cisco ISE policy, like AD group membership, etc. In my configuration I will use three AD Groups for Employee, Vendor and ITSupport.

- 1. Login to Cisco ISE
- 2. Navigate to **Policy** → **Policy Elements** → **Conditions**
- 3. We will create **Condition Element** for those three AD groups by selecting below:
 - a. In Attribute, select Identity → Your AD Group → Equals → <Select your AD Group>

Note - If you do not see AD group, you first have to add that AD group to ISE from

Administration \rightarrow External Identity Source \rightarrow Active Directory \rightarrow <Your Directory> \rightarrow Groups

 \rightarrow Add

b. Similarly create Condition Element for other two Groups – Vendor and ITSupport

Editor														
0	Click to add an a	lick to add an attribute												
t;	Equals	Select a	attribute for condition										×	
		Ø	F2 C 👛	<u>.</u>	F	5			©	1	ø	٤	((:-	
			Dictionary		Attribute	e				ID		Info		
			All Dictionaries	~	Attribute					ID.				
		*										<i>(i)</i>	~	
			IdentityGroup		Descripti	on						<i>(i)</i>		
		串	IdentityGroup		Name							<i>(i)</i>		
		-48-	InternalUser		IdentityG	roup						<i>(i)</i>		
		-	PassiveID		Passivel	D_Grou	ips		_			<i>(i)</i>	_	
		28			External	Groups						()	~	
						_	_	_	_	_	_	_	_	

Editor SMC_AD·ExternalGroups Equals Set to 'ls not'	AD.LOCAL\GROUP\EMPLOYEES	© ^
Save condition	×	
Save as existing Library C	ondition (replaces current version and impact all policies that use this condition)	
Select from list	•	
Save as a new Library Con	ndition	
MemberOf_Employee		
Description (optional)		
Condition Description		
	Close	

In this phase, we will create resultant authorisation policy/profile when authentication and authorisation is successful. In this phase we will mention the Group Policy Name to be applied to the user.

- 1. Login to Cisco ISE
- 2. Navigate to Policy → Policy Element → Results → Authorisation → Authorisation Profiles → Add
- 3. Configure as below:
 - a. Name and Description As per your choice or naming convention
 - **b.** Access Type **ACCESS_ACCEPT**
 - c. Common Tasks → ASA VPN → OU=<Group Policy Name>
 - d. Submit
- 4. Create for Employee, Vendor and ITSupport as per Step 3.

dentity Services Engine Ho	ome	
Policy Sets Policy Elements		Policy Sets Policy Elements
Dictionaries + Conditions - Results		Dictionaries
0		Results
Authentication	Standard Authorization Profiles For Policy Export go to Administration > System	n > Backup & Restore > Policy Export Page
- Authorization		
Authorization Profiles	/ Edit + Add Duplicate X Delete	
Downloadable ACLs	□ Name	Profile
Downloadable AGES		dtto Cisco ⊕
▶ Profiling		ditto Cisco 🕀
▶ Posture		🗰 Cisco 🕀
		🗱 Cisco 🕀
Client Provisioning		atto Cisco 🕀
		white Cinese (F)

Authorization Profil	
* Nan	e VPN_Employee
Descriptio	n Employee VPN Profile
* Access Typ	e ACCESS_ACCEPT V
Network Device Profile	della Cisco 👻 🕀
Service Templa	
Track Moveme	nt 🗌 🕡
Passive Identity Trackin	9 🗌 👔
▼ Common Tasks	
Web Authenticatio	n (Local Web Auth)
Airespace ACL Na	Me SYNTAX - OU= <group policy=""></group>
AVC Profile Name	
▼ Advanced Attrib	ites Settings
Select an item	
▼ Attributes Detail	5
Access Type = ACCES Class = OU=AnyConne	S_ACCEP T ct-Employee
Submit Cancel	

Step 4 - Configure different Cisco ISE policy for each VPN user category (e.g. Vendor, Employee, etc)

In this phase, we will create ISE policy for each VPN user.

- 1. Login to Cisco ISE
- 2. Navigate to **Policy** \rightarrow **Policy Set** \rightarrow *Select your main policy*
- 3. Add new authorisation policy at top as below:
 - a. Name VPN-Employee
 - b. Conditions:
 - i. DEVICE Device Type \rightarrow Equals \rightarrow Firewall
 - *ii.* Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Name → Equals → <*AnyConnect*

Remote Access Connection Profile Name>

- iii. MemberOf-Employee
- c. Result → VPN-Employee
- 4. Similarly, create authorisation rules for Vendor and ITSupport, just change the MemberOf and Resultant

Policy.



Policy	Sets					Reset Policyset Hitcount	s R	leset	Save
+	Status	Policy Set Name	Description	Condi	tions	Allowed Protocols / Server Sequence	Hits	Actions	View
Searc	h								
	۲	Default - Local user DENY	Local user DENY - Default Policy Set	AND		*		٥	>
	0			AND	8			0	>
	0	100 million (1997)	Annaly States (States)		81881-3873	100 Mar (0.000 - 0.000 - 1	-	¢	>
	Ø			OR	2 2 2 2 2 2 2 2	PAP_ONLY * * *		¢	Þ
	Ø	Default - MAB	MAB - Default Policy Set		Wired_MAB	Default Network Access × + +	0	٥	>
	Ø	Default - Dot1X	Dot1X - Default Policy Set		Wired_802.1X	Default Network Access × * +	0	٥	>
	\odot	Default	Default policy set			Default Network Access × * +	0	¢	>
							F	Reset	Save

Policy S	Sets +	Second State							Reset Policyset Hitcounts	Reset	Save
	Status	Policy Set Name	Description	c	Conditio	IS			Allowed Protocols / Se	ver Sequer	nce Hits
Search											
	\odot	100011-000	Contraction of the		OR		And a second		PAP_ONLY	× - +	-
						₽	Frank				
							Connection Profile Access Interfaces Adv	anced			
							Cisco FMC - Device - V	PN - Remote Acce	ss - VPN Policy		
> Auth	entication	n Policy (1)					Name		AAA		_
> Auth	orization	Policy - Local Exceptions					DefaultWEBVPNGroup		Authentication: None Authorization: None Accounting: Mone		
> Auth	orization	Policy - Global Exceptions					Connection	Profile Name	Authentication: ISE-AAA (RADIUS) Authorization: ISE-AAA (RADIUS) Accounting: ISE-AAA (RADIUS)		_
◆ Auto	Ionzation	Policy (15)									
(+)								Results			
<u> </u>	Status	Rule Name	Conditions				. /	Profiles	Security Groups	Hits	Actions
Search	h										
				VICE Device Ty	pe EQUA	LS All Device Types#Firewall	K				
	Ø	(resident)	AND 🖁 Cis	co-VPN3000 C	VPN3000	/ASA/PIX7x-Tunnel-Group-Name EQUALS	Connection Profile Name	VPN_EMPLOYEE +	Select from list 🔹 🔹	•	۵
			Mer Mer	mberOf-VPN		MEMBEROF-EMPLOYEE					
			DE DE	VICE Device Typ	pe EQUA	LS All Device Types#Firewall					
	Ø	100.000	AND & Cis	co-VPN3000-C	VPN3000	ASA/PIX7x-Tunnel-Group-Name EQUAL	Sciences W	VPN_VENDOR +	Select from list	-	0
			Mer	mberOf-VPN	N	AemberOf-Vendor				_	
-					_					_	

Step 5 – Testing and Verification of the policy

In this phase, we will connect via VPN and test if we getting the right policy, ACL and IP address.

- 1. Connect using Employee username/password group via AnyConnect
- 2. Login to Cisco ISE
- 3. Navigate to **Operations** → Live Log
- 4. Search based on the **username** to see the log
- 5. Find the VPN policy log and click the Details column Magnifying Glass to view details
- 6. In details section you can see, **resultant policy**, which rule it is hitting, AD group and all other details.
- 7. Login to Cisco FMC to verify under FMC
- 8. Navigate to Analysis \rightarrow Users \rightarrow User Activity
- 9. Search based on username
- 10. You will see a record of your user with **Group Policy** details.

-Indentity Services Engine Home Context Visibility	Operations Policy Administration Work Centers
▼RADIUS Threat-Centric NAC Live Logs → TACACS → Troubles	RADIUS Threat-Centric NAC Live
Live Logs Live Sessions	Live Logs Logs
	Troubleshoot
Misconfigured Supplicants	TACACS Diagnostic Tools
misconingureu supplicants	Live Logs Download Logs
0	Reports



Overview Analysis Policies Devices Objects	AMP Intellig	igence				
Context Explorer Connections • Intrusions •	Files • Hosts •	Users Correlation Adv				
	Active Sessions					
Summary Dashboard	Users					
Provides a summary of activity on the appliance	User Activity					
Network × Threats × Intrusion Events × 5	ra Indications of Compromise					

U	Bookmark: This Page: Report Designer: Dashboard: View Bookmarks: Search • User Activity Table View of Events: > Users: Users: Search • Users: Search • Searc																
• :	Search Constraints (<u>Edit Search</u>)																
		▼ <u>Time</u> ×	Event ×	<u>Username</u> ×	Realm ×	Discovery × Application	Authentication ×	IP Address ×	Start × Port	End × Port	Description ×	VPN Session × Type	VPN Group × Policy	VPN Connection Profile ×	VPN Client Public IP	× <u>VPN Client</u> × <u>Country</u>	VPN Clie
4		2020-09-17 16:38:27	User Login	B	-	LDAP	International Andrewson Street	all an an an an					EMPLOYEE	5			_
4		2020-09-17 16:38:23	VPN User Login	E	Discovered Identities	LDAP	VPN Authentication	-				AnyConnect SSL	GROUP_POLICY	inclusion income of	-	AUS	win
ŀ	< < Page 1 of 1 >) Displaying rows 1-2 of 2 rows																
	View	Delete															
	View A	Delete All															_