Configure FDM Active Authentication (Captive Portal)

Contents

Introduction Prerequisites Requirements Components Used Background Information Network Diagram Configure Verify Troubleshoot

Introduction

This document describes a configuration example for Firepower Device Manager (FDM) with Active Authentication (Captive-Portal) integration. This configuration uses Active Directory (AD) as the source and self-signed certificates.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Self-signed Certificates.
- Secure Socket Layer (SSL)

Components Used

The information in this document is based on the following software version:

- Firepower Threat Defense 6.6.4
- Active Directory
- PC test

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Establish User Identity through Active Authentication

Authentication is the act of confirms the identity of a user. With active authentication, when an HTTP traffic flow comes from an IP address for which the system has no user-identity mapping, you can decide whether to authenticate the user who initiated the traffic flow against the directory configured for the system. If the user successfully authenticates, the IP address is considered to have the identity of the authenticated user.

Failure to authenticate does not prevent network access for the user. Your access rules ultimately decide what access to provide these users.

Network Diagram



Configure

Implement the Identity Policy

To enable user identity acquisition, so that the user associated with an IP address is known, you need to configure several items

Step 1. Configure the AD identity realm

Whether you collect user identity actively (by prompt for user authentication) or passively, you need to configure the Active Directory (AD) server that has the user identity information.

Navigate to **Objects** > **Identity Services** and select the option **AD** to add the Active Directory.

cisco. Firepower Devic	e Manager Monitoring Policies	Objects Device: firepower	> 🛎 🙆 🤅	admin Administrator
Object Types 🛛 🔶	Identity Sources			
C Networks	2 objects		Q Search	+ ~
S Ports	# NAME	TYPE	VALUE	RADIUS Server
Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
F Application Filters				AD
6 ⁹ URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
IPSec Proposals				
AnyConnect Client Pro				
S Identity Sources				
1 Users				

Add the Active Directory configuration:

Identity Realm is used for Identity Policies and Remot this realm.	e Access VPN. Any changes impact all features that use	
Name	Туре	
Active_Directory	Active Directory (AD)	~
Directory Username sfua	Directory Password	
e.g. user@example.com		
Base DN	AD Primary Domain	
CN=Users,DC=ren,DC=lab	ren.lab	
e.g. ou=user, dc=example, dc=com	e.g. example.com	
Directory Server Configuration		
172.17.4.32:389	<u>Test</u> 👻	
Add another configuration		
	CANCEL	

Step 2. Create Self-signed certificates

In order to create a Captive Portal configuration, you need two certificates one for the captive portal and one for SSL decryption.

You can create a self-signed certificate like in this example.

Navigate to Objects > Certificates

cisco. Firepower Devi	ce Manager Monitoring Policies Objects	Device: firepower		admin Administrator
Object Types ←	Certificates			
C Networks	120 objects		Q Search	+~
S Ports			Preset filters: System defined - User defined	Add Internal CA
Security Zones	H NAME	туре		Add Internal Certificate
🐨 Application Filters	1 NGFW-Default-InternalCA	Internal CA		Add Trusted CA Certificate
6 2 1101 o	2 ssl_captive_portal	Internal CA		
OF URLS	3 DefaultInternalCertificate	Internal Certificate		
Geolocations	4 DefaultWebserverCertificate	Internal Certificate		

Captive portal Self Signed Certificate:

Add Internal Certificate	8 ×
Name	
captive_portal	
Country	State or Province
Mexico (MX)	Mexico
Locality or City	
Mexico	
Organization	Organizational Unit (Department)
MexSecTAC	MexSecTAC
Common Name	
fdmcaptive	
You must specify a Common Name to use the ce	ertificate with remote access VPN.
	CANCEL SAVE

SSL Self Signed certificate:

Add Internal CA

Name		
ssl_captive_portal		
Country		State or Province
Mexico (MX)	~	Mexico
Locality or City		
Mexico		
Organization		Organizational Unit (Department)
MexSecTAC		MexSecTAC
Common Name		
ss_fdmcaptive		
You must specify a Common Name to use	e the cert	ificate with remote access VPN.
		CANCEL SAVE

Step 3. Create Identity rule

Navigate to **Policies** > **Identity** > select [+] button to add a new Identity rule.

You need to create the Identity policy in order to configure active authentication, the policy must have the below elements:

- AD Identity Source: The same you add in the step number 1
- Action: ACTIVE AUTH
- Server Certificate: The same Self-signed Certificate you created Before [In this scenario captive_portal]
- Type: HTTP Basic (in this example scenario)

Order Title 1 v ad_captive	AD Identity Source Active_Directory ~	Action	ACTIVE AUTHENTICATION For HTTP connections only, prompt for authenticate against the specified iden	r username and password and tity source to obtain the user
Source / Destination Active authentication		PASSIVE AUTH Identity Sources are needed	d h Server Certificate	_portal:885
SOURCE		ACTIVE AUTH Captive Portal is needed		
Zones + Networks	+ Ports	NO AUTH	Networks +	Ports/Protocols +
ANY ANY	ANY	ANY	ANY	ANY

Once the Identity policy is created as active authentication, automatically creates an SSL rule, by default this rule is set up as any any with **Decrypt-Resign**, which means that there are no SSL modifications into this rule.

$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \bigcirc$ NAT $\rightarrow \bigotimes$ Access Control \rightarrow \circledast Intrusion												
SSL Decryption	1 rule						Q Search				\$	+
		SOURCE			DESTINATION							
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
🕘 🔝 Identity Poli	cy Active Authentica	ntion Rules 🚺										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	۵,	
SSL Native Rule	• 0											
SSL Native Rules There are no SSL Rules yet. Start by creating the first SSL rule. CREATE SSL RULE Or ADD PRE-DEFINED RULES												
□ →	SSL Decryption	ightarrow Identit	$v \rightarrow \bigcirc Seci$	urity Intelligence -	\rightarrow \bigcirc NAT \rightarrow	Access Co	ontrol $ ightarrow$ 😵 Ir	trusion				

🕒 🔶 🖌 SSL (Decryption $ ightarrow$ of Identi	ty \rightarrow \bigcirc Secu	rity Intelligence –	\rightarrow \bigcirc NAT \rightarrow	Access C	iontrol $ ightarrow$ 😵 I	ntrusion			
SSL Decryption	The rules in this section are generated from rules in the	automatically identity policy				Q Search				¢ +
II NAME	that implement active authentication. These SSL decryption rules are read-only. These rules are always evaluated before the SSL		PORTS	DESTINATION	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
J Identity Policy Act	tive Authentication Rules							0.120		
1 ad_captive	Re-Sign ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	e.
SSL Native Rules 🚺										
	There are no SSL Rules yet. Start by creating the first SSL rule.									
	Start by creating the first SSL rule. CREATE SSL RULE or ADD PRE-DEFINED RULES									

Step 4. Create Access rule into Access Control Policy

You need to allow **pot 885/tcp** which redirects the traffic to the captive portal authentication. Navigate to **Policies** > **Access Control** and add the access rule.

+
—

If you need to check if the users were downloaded from AD, you can edit the access rule and navigate to the **Users** section, then on **AVAILABLE USERS**, you can verify how many users does the FDM already has.

Order Title				Action	
1 ∨ ad_capt	ive			Allow	×
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS				•	CONTRO
▼ Filter					lf you config address, yo membership
Identity Sources	Groups Users	-	-		appropriate different ad
Active_Directory	luis		*		network acc from one gr
Active_Directory	ngfwtac				
Special-Identities	-Realm \ No Authe	entica			
Active_Directory	ren				
Active_Directory	sfua				
Active_Directory	testuser		•		
Create new Identity Realm	CANCEL	ОК			

Remember to deploy the configuration changes.

Verify

Verify that the user's device receives the check box when navigates to a HTTPS site.

S https://10.115.117.43:885/xauthi × +									
← → C () 10.115.117.43:885/x.auth?s=dOF7LRChg4FKX2BCiK46wfdQKDJMAXeaLGcyYeiycuc%3D&u=http%3A%2F%2Fwww.cisco.com%2F									
	Sign in https://10.115.117.43:885 Username Password Sign in Cancel								

Enter the user AD credentials.

https://10.115.117.43:885/x.auth?	× +					
← → C (1) 10.115.117.4	3:885/x.auth?s=dOF7LRC	hg4FKX2BCiK46wfd	QKDJMAXeaLGcyYeiycu	%3D&u=http%3A%2F%2F	www.cisco.com%2F	
				Sign in https://10.1 Username Password	15.117.43:885	Sign in Cancel
Cisco - Networking, Cloud, and (x + → C	Products Support & Learn	Partners Events & Vid	leos			ଦ ଥି ⊕୪
Kiva and	Cisco: Creating in etail opportunities	Active exp	Noit of Kaseya VSA in supply-of See the action	hain attack. Read the Talos b		time to take the lead
	E Design Guides	(A)+ Find Training	දියි Learning & Certifications	() Software Downloads	දුරියි Cisco Community	Activate Windows

Troubleshoot

You can use the user_map_query.pl script to validate FDM has the user ip mapping

user_map_query.pl	-i	x.x.x.	x >	for	ip	addresses	
root@firepower:~#	user_map_query.pl -u			ngfwtac			

```
WARNING: This script was not tested on this major version (6.6.0)! The results may be
unexpected.
Current Time: 06/24/2021 20:45:54 UTC
Getting information on username(s)...
___
User #1: ngfwtac
_ _ _
TD:
          8
Last Seen: 06/24/2021 20:44:03 UTC
for_policy: 1
Realm ID:
           4
Database
                          ------
##) IP Address [Realm ID]
1) ::ffff:10.115.117.46 [4]
##) Group Name (ID) [realm: Realm Name (ID)]
1) Domain Users (12) [realm: Active_Directory (4)]
On clish mode you can configure:
```

system support identity-debug to verify if redirection is successful.

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 10.115.117.46
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 2
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Logging EOF for event from hardware with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 : Received EOF, deleting the snort
session.
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 deleting firewall session flags = 0x10003,
fwFlags = 0x114
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 63784 -> 53, geo 16671760 -> 16671778
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 looked for user_id with realm_id 4 auth_type
```

```
2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 found active binding for user_id 8 in realm
4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 2023803385 user_id =
8 \text{ realm_id} = 4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 1,
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 50619 -> 443, geo 16671760 -> 16671778
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 looked for user_id with realm_id 4
auth_type 2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 found active binding for user_id 8 in
realm 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 matched auth rule id = 2023803385 user_id
= 8 \text{ realm_id} = 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 new firewall session
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 HitCount data sent for rule id: 1,
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 allow action
```

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptdfdm-identity.html#id_71535

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity-sources.html#task_83008ECD0DBF4E388B28B6247CB2E64B