Configurar a autenticação ativa do FDM (Portal cativo)

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Diagrama de Rede Configurar Verificar Troubleshoot

Introduction

Este documento descreve um exemplo de configuração para o Firepower Device Manager (FDM) com integração Ative Authentication (Captive-Portal). Esta configuração usa o Ative Diretory (AD) como a origem e os certificados autoassinados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Certificados autoassinados.
- Secure Socket Layer (SSL)

Componentes Utilizados

As informações neste documento são baseadas na seguinte versão de software:

- Firepower Threat Defense 6.6.4
- Ative Diretory
- teste PC

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estabelecer a identidade do usuário por meio da autenticação ativa

A autenticação é o ato de confirmar a identidade de um usuário. Com a autenticação ativa, quando um fluxo de tráfego HTTP vem de um endereço IP para o qual o sistema não tem mapeamento de identidade de usuário, você pode decidir se deve autenticar o usuário que iniciou o fluxo de tráfego em relação ao diretório configurado para o sistema. Se o usuário autenticar com êxito, considera-se que o endereço IP tem a identidade do usuário autenticado.

A falha na autenticação não impede o acesso à rede para o usuário. Suas regras de acesso decidem, em última análise, qual acesso fornecer a esses usuários.

Diagrama de Rede



Configurar

Implementar a política de identidade

Para ativar a aquisição de identidade do usuário, de modo que o usuário associado a um endereço IP seja conhecido, você precisa configurar vários itens

Etapa 1. Configurar o território de identidade do AD

Quer você colete a identidade do usuário ativamente (por prompt para autenticação do usuário) ou passivamente, você precisa configurar o servidor do Ative Diretory (AD) que tem as informações de identidade do usuário.

Navegue até **Objetos > Serviços de identidade** e selecione a opção **AD** para adicionar o Ative Diretory.

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	TIPE	VALUE	RADIUS Server
Security Zones	1 LocalidentitySource	LOCAL		RADIUS Server Group
Application Filters				AD
C ⁹ URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client Pro				
State Identity Sources				
L Users				

Adicione a configuração do Ative Diretory:

Identity Realm is used for Identity Policies and Remote 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

Etapa 2. Criar certificados autoassinados

Para criar uma configuração do Portal cativo, você precisa de dois certificados, um para o portal cativo e um para a descriptografia de SSL.

Você pode criar um certificado autoassinado como neste exemplo.

Navegue até Objetos > Certificados

cisco. Firepower Devi	ce Manager Monitoring Policies Objects Device: firepower	S. 🖄 🗐 ? : admin Administrator
Object Types ←	Certificates	
C Networks	120 objects	Q Search + V
S Ports		Preset filters: System.defined - User.defined Add Internal CA
Security Zones	B NAME TYPE	Add Internal Certificate
Application Filters	1 NGFW-Default-InternalCA Internal CA	Add Trusted CA Certificate
n0 1101 n	2 ssl_captive_portal Internal CA	
OF URLS	3 DefaultInternalCertificate Internal Certificate	
Geolocations	4 DefaultWebserverCertificate Internal Certificate	

Certificado autoassinado do portal cativo:

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	rtificate with remote access VPN.
	CANCEL SAVE

Certificado com assinatura automática SSL:

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 certi	ificate with remote access VPN.
		CANCEL SAVE

Etapa 3. Criar regra de identidade

Navegue para **Políticas > Identidade >** selecione **[+]** o botão para adicionar uma nova regra de Identidade.

Você precisa criar a política de identidade para configurar a autenticação ativa, a política deve ter os seguintes elementos:

- Fonte de identidade do AD: O mesmo que você adiciona na etapa número 1
- Ação: AUTH ATIVO
- Server Certificate: O mesmo certificado autoassinado que você criou antes de [Neste cenário, portal cativo]
- Digite: HTTP Basic (neste cenário de exemplo)

Order Title	AD Identity Source	Action ACTIVE AL	ITHENTICATION
1 × ad_captive	Active_Directory ~	Active Auth	a against the specified identity source to obtain the user the source IP address.
Source / Destination Active authentication		PASSIVE AUTH Identity Sources are needed th Server	Certificate 👷 captive_portal:885
SOURCE		ACTIVE AUTH Captive Portal is needed	
Zones + Networks	+ Ports	No AUTH	vorks + Ports/Protocols +
ANY ANY	ANY	ANY AN	Y ANY

Uma vez que a política de Identidade é criada como autenticação ativa, cria automaticamente uma regra SSL, por padrão, esta regra é configurada como qualquer uma com **Decrypt-Resign**, o que significa que não há modificações SSL nesta regra.

🖳 → 🖌 S	SL Decryption	ightarrow Identity	\rightarrow \bigcirc Secur	ity Intelligence $ ightarrow$	\rightarrow () NAT \rightarrow	Access Co	ntrol $ ightarrow$ 🖓 In	itrusion				
SSL Decryption	1 rule						Q Search				¢	+
		SOURCE			DESTINATION	1						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	,	CTIONS
- 🗵 Identity Polic	y Active Authentica	tion Rules 🧻										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	۳.	
SSL Native Rules	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												
및 → 📀	SSL Decryption	ightarrow Identit	$y \rightarrow \bigcirc$ Secu	rity Intelligence	\rightarrow \bigcirc NAT \rightarrow	Access Co	introl $ ightarrow$ 🗣 Ir	trusion				

	Decryption		uty -> O Sect	inty intelligence		Access U	Jontrol -> 📲	IIIUSIOII				
SSL Decryption The rules in this section are automatically generated from rules in the identity policy		Q Search							ф	+		
	SSL decry	ption rules are r	ead-only. These		DESTINATION							
II NAME	native rule	is, ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	4	ACTIONS
a 🛃 Identity Policy Ad	ctive Authentica	ation Rules 🧃										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.	
SSL Native Rules 🚺												
				Sta	There are no SSL Ru	ules yet. st SSL rule.						
				CREATE SSL F	RULE	ADD PRE-DEFI	NED RULES					

Etapa 4. Criar regra de acesso à política de controle de acesso

Você precisa permitir a **porta 885/tcp** que redireciona o tráfego para a autenticação do portal cativo. Navegue para **Políticas > Controle de acesso** e adicione a regra de acesso.

Order Title				Action							
1 ~ ad_	captive			Allo	w ~						
Source/Destination Applications URLs Users Intrusion Policy File policy Logging											
SOURCE						DESTINATION					
Zones	+	Networks	+	Ports	+	Zones	+	Networks	+	Ports/Protocols	+
ANY		ANY		ANY		ANY		ANY		≤ 885	
											_

Se precisar verificar se os usuários foram baixados do AD, você pode editar a regra de acesso e navegar até a seção **Usuários** e, em **USUÁRIOS DISPONÍVEIS**, você pode verificar quantos usuários o FDM já possui.

Order Title				Action	
1 ∨ ad_cap	otive			Allow	~
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS	-				CONTRO
▼ Filter					lf you config address, yo membershig
Identity Sources	Groups Users		-		appropriate different ad
Active_Directory	/ luis		•		network acc from one gr
Active_Directory	∖ ngfwtac				-
Special-Identitie	es-Realm \ No Auth	entica			
Active_Directory	∧ ren				
Active_Directory	∖ sfua				
Active_Directory	\ testuser		•		
Create new Identity Reals	n CANCEL	ок			

Lembre-se de implantar as alterações de configuração.

Verificar

Verifique se o dispositivo do usuário recebe a caixa de seleção ao navegar para um site HTTPS.

S https://10.115.117.43:885/x.auth: × +	
← → C ① 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

Insira as credenciais do AD do usuário.

S https://10.115.117.43:885/x.auth? × +					
← → C ③ 10.115.117.43:885/x.auth?s=dC)F7LRChg4FKX2BCiK46wfd	IQKDJMAXeaLGcyYeiycu	c%3D&u=http%3A%2F%2F	www.cisco.com%2F	
			Sign in https://10.1 Username Password	15.117.43:885 ngfwtac	Sign in Cancel
Cisco - Networking, Cloud, and ⊂ x + → C a cisco.com Cisco Platform Sufle > 1 1 1 1 1 Products Support &	Learn Partners Events & Vic	deos			ର ୧୧ କ⊮
Kiva and Cisco: Creati retail opportun	Active exp ng inclusive ities	bloit of Kaseya VSA in supply-of	chain attack. Read the Talos b		time to take the lead
Design Guides	Find Training	ર્્સ્ટ્રે Learning & Certifications	Software Downloads	දිරිදි Cisco Community	Activate Windows

Troubleshoot

Você pode usar o script **user_map_query.pl** para validar se o FDM tem o mapeamento ip do usuário

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)] No modo de silêncio, você pode configurar:

o sistema oferece suporte à identificação-depuração para verificar se o redirecionamento foi bemsucedido.

```
> 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
Referência:
```

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

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