Configuratie van FDM Actieve Verificatie (Captive Portal)

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Netwerkdiagram Configureren Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft een configuratievoorbeeld voor Firepower Apparaat Manager (FDM) met actieve verificatie (Captive-Portal) integratie. Deze configuratie gebruikt Active Directory (AD) als de bron- en zelfgetekende certificaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversie:

- Firepower Threat Defense, 6.6.4
- Actieve map
- PC-test

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Gebruikersidentiteit instellen door actieve verificatie

Verificatie is het bewijs van de identiteit van een gebruiker. Met actieve authenticatie, wanneer een HTTP verkeersstroom van een IP adres komt waarvoor het systeem geen gebruiker-identiteit mapping heeft, kunt u beslissen of u de gebruiker die de verkeersstroom in werking stelde, authenticeert aan de folder die voor het systeem is ingesteld. Als de gebruiker echt verklaart, wordt het IP-adres geacht de identiteit van de geauthentiseerde gebruiker te hebben.

Niet-authentiek verklaren verhindert de netwerktoegang voor de gebruiker niet. Uw toegangsregels beslissen uiteindelijk welke toegang deze gebruikers verschaft.

Netwerkdiagram



Configureren

Het identiteitsbeleid uitvoeren

Om het verwerven van een gebruikersidentiteit mogelijk te maken, zodat de gebruiker die aan een IP-adres is gekoppeld, bekend is, moet u verschillende items configureren

Stap 1. Het AD-identiteitsveld configureren

Of u actief gebruikersidentiteit verzamelt (door prompt gebruikersverificatie) of passief, moet u de Active Directory (AD) server configureren die de gebruikersidentiteitsinformatie heeft.

Navigeren in op **Exemplaar > Identity Services** en selecteer de optie **AD** om de actieve map toe te voegen.

CISCO. Firepower Devi	ce Manager Monitoring Policies	Objects Device: firepower	S 🖨 Ø 🤅) * admin * Administrator
Object Types ←	Identity Sources			
C Networks	2 objects		Q Search	+ ~
S Ports	a NAME	туре	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
Application Filters				AD
69 URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client Pro				
Lidentity Sources				
1 Users				

Voeg de configuratie van de Actieve Map toe:

Identity Realm is used for Identity Policies and Remo this realm.	te 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	Test 👻
Add another configuration	
	CANCEL

Stap 2. Maak zelf ondertekende certificaten

Om een configuratie van het Captive Portal te maken, hebt u twee certificaten nodig één voor het gevangen portaal en één voor SSL decryptie.

U kunt een zelfondertekend certificaat maken zoals in dit voorbeeld.

Navigeren in op objecten > certificaten

CISCO. Firepower Devi	ice M	lanager Monitoring Policies	章王 Objects	Device: firepower	>> 📾 🐵 ?	* admin * Administrator
Object Types 🛛 🗧 🗧		Certificates				
C Networks		120 objects			Q Search	+ ~
S Ports					Preset filters: System stefined - User stefines	Add Internal CA
Security Zones		NAME		туре		Add Internal Certificate
🐬 Application Filters		1 NGFW-Default-InternalCA		Internal CA		Add Trusted CA Certificate
A2 1101 a		2 ssl_captive_portal		Internal CA		
0° URLS		3 DefaultInternalCertificate		Internal Certificate		
Geolocations		4 DefaultWebserverCertificate		Internal Certificate		

Zelfondertekend certificaat voor portal

Add Internal Certificate	?
Name captive_portal	
Country	State or Province
Mexico (MX)	Mexico
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 Zelfondertekend certificaat:

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	the certi	ficate with remote access VPN.
		CANCEL SAVE

Stap 3. Maak identiteitsregels

Navigeer naar **beleid > Identity >** selecteer [+] om een nieuwe identiteitsregel toe te voegen.

U moet het identiteitsbeleid creëren om actieve authenticatie te configureren hebt het beleid de volgende elementen:

- AD-identiteitsbron: Het zelfde dat u in stap nummer 1 toevoegt
- Actie: ACTIEVE AUTO
- servercertificaat: Hetzelfde certificaat dat u voor [In dit scenario in gevangenschap_portal] hebt gemaakt
- Type: HTTP Basic (in dit voorbeeldscenario)

Order Title	AD Identity Source	Action ACTIVE AUTHENTICATION	
1 v ad_captive	Active_Directory ~	Active Auth Active Auth Activ	tor username and password and dentity source to obtain the user
Source / Destination Active authentication		PASSIVE AUTH Identity Sources are needed th Server Certificate Q cap	tive_portal:885
SOURCE		ACTIVE AUTH Captive Portal is needed	
Zones + Networks	+ Ports	NO AUTH	+ Ports/Protocols +
ANY ANY	ANY	ANY ANY	ANY

Zodra het identiteitsbeleid als actieve authenticatie wordt gecreëerd, creëert automatisch een SSL regel, door standaard wordt deze regel ingesteld als elke andere met **Decrypt-Resign**, wat betekent dat er geen SSL aanpassingen in deze regel zijn.

🖳 🔿 🖌 🖉 S	SL Decryption	ightarrow 🕑 Ident	tity \rightarrow \bigcirc Sec	urity Intelligence	\rightarrow O NAT	→ 🕗 Access (Control $ ightarrow$	Intrusion				
SSL Decryption	1 rule						Q Search				ф	+
		SOURCE			DESTINATION							
II NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
🧧 🔝 Identity Policy	y Active Authentica	ation Rules 🧻										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	P.	
SSL Native Rules	0											
				Sta	There are no SSL int by creating the RULE or	Rules yet. first SSL rule. ADD PRE-DEFI	NED RULES					
	SSL Decryption	ightarrow Iden	ntity $ ightarrow$ \bigcirc Sec	curity Intelligence	\rightarrow () NAT	→ 🕑 Access (Control $ ightarrow$	Intrusion				
SSL Decryption	The rules	s in this section a d from rules in th	ire automatically he identity policy				Q Search				\$	+

SSL Decryption The rules in this section are automatically generated from rules in the identity policy					Q Search				\$	+	
	that implement active auth SSL decryption rules are re rules are always evaluated	entication. These ad-only. These before the SSL		DESTINATION							
I NAME	Inative rules. ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	AC	TIONS
1 ad_captive	ANY Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	e.	
SSL Native Rules ()											
			Sta	There are no SSL art by creating the	Rules yet. first SSL rule.						
			CREATE SSL	RULE	ADD PRE-DEFI	NED RULES					

Stap 4. Maak een toegangsregel in het toegangscontrolebeleid

U moet **post 885/tcp** toestaan die het verkeer omleidt naar de interne poortverificatie. Navigeren in op **beleid > Toegangsbeheer** en toevoegen de toegangsregel.

Order Tit	tle			Α	ction						
1 ~	ad_captive				Allow ∨						
Source/Destina	ition Ap	oplications URLs	U	sers Intru	sion Policy	File policy	Logging				
SOURCE						DESTINATION					
Zones	+	Networks	+	Ports	+	Zones	+	Networks	+	Ports/Protocols	+
ANY		ANY		ANY		ANY		ANY		≤ 885	

Als u moet controleren of de gebruikers zijn gedownload van AD, kunt u de toegangsregel bewerken en naar het gedeelte **Gebruikers** navigeren, en dan **op beschikbare USERS**, kunt u controleren hoeveel gebruikers de FDM al heeft.

Order Title				Action	
1 × ad_ca	ptive			Allow	×
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS	-			6	. 🤱 CONTRO
▼ Filter					lf you config address, yo membership
Identity Sources	Groups Users		-		appropriate different ad
Active_Director	y \ luis		•		network acc from one or
Active_Director	y \ ngfwtac				
Special-Identitie	es-Realm \ No Auth	entica			
Active_Director	y \ ren				
Active_Director	y ∖ sfua				
Active_Director	v \ testuser		-		
Create new Identity Real	CANCEL	ОК			

Denk eraan om de configuratie veranderingen in te voeren.

Verifiëren

Controleer dat het apparaat van de gebruiker het aankruisvakje ontvangt wanneer u naar een HTTPS-site navigeert.

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

Voer de AD-referenties van de gebruiker in.

S https://10.115.117.43:885/x.auth? ×	+					
← → C ① 10.115.117.43:88	85/x.auth?s=dOF7LR0	hg4FKX2BCiK46wfd	QKDJMAXeaLGcyYeiycu	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 +	ucts Support & Learn	Partners Events & Vid	deos			Q
Kiva and Cit reta	sco: Creating in il opportunities	Active exp	Not of Kaseya VSA in supply-of See the action	han attack Read the Talos be Read the Talos be r	og nov	e time to take the lead
	Design Guides	(A)+ Find Training	کی کے Learning & Certifications	(1) Software Downloads	දුරියි Cisco Community	Activate Windows

Problemen oplossen

U kunt het script **user_map_query.pl** gebruiken om FDM te valideren dat de ip mapping de gebruiker is

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)] In de modus Engels kunt u het volgende configureren:

het systeem ondersteunt identiteit-debug om te controleren of omleiding een succes is.

> 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 = 0x10010.115.117.46-55809 > 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 = 0x11410.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001, fwFlags = 0x10010.115.117.46-65489 > 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 = 0x10010.115.117.46-65489 > 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 = 0x10010.115.117.46-53417 > 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
Referentie:
```

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