FDMアクティブ認証の構成(キャプティブポー タル)

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ネットワーク図</u>
<u>設定</u>
確認
トラブルシュート

概要

このドキュメントでは、アクティブ認証(キャプティブポータル)統合を使用したFirepower Device Manager(FDM)の設定例について説明します。この設定では、ソースおよび自己署名証明 書としてActive Directory(AD)を使用します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- 自己署名証明書:
- Secure Socket Layer (SSL)

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Threat Defense 6.6.4
- Active Directory
- PCテスト

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

アクティブ認証によるユーザIDの確立

認証は、ユーザのアイデンティティを確認する行為です。アクティブ認証では、システムにユー ザIDマッピングがないIPアドレスからHTTPトラフィックフローが着信した場合、システムに設定 されたディレクトリに対してトラフィックフローを開始したユーザを認証するかどうかを決定で きます。ユーザが正常に認証されると、そのIPアドレスは認証されたユーザのアイデンティティ を持つと見なされます。

認証に失敗しても、ユーザのネットワークアクセスは妨げられません。アクセスルールは、最終 的に、これらのユーザに提供するアクセスを決定します。

ネットワーク図



設定

アイデンティティポリシーの実装

IPアドレスに関連付けられたユーザが認識されるようにユーザIDを取得できるようにするには、 いくつかの項目を設定する必要があります

ステップ1:ADアイデンティティレルムの設定

ユーザIDをアクティブに(ユーザ認証のプロンプトで)収集するか、パッシブに収集するかにか かわらず、ユーザID情報を持つActive Directory(AD)サーバを設定する必要があります。 [**Objects**] > [**Identity Services**]の順に移動し、[**AD**]オプションを選択してActive Directoryを追加します。

CISCO. Firepower Device	ce Manager Monitoring Policies	Objects Device: firepower	S 🖨 Ø	? * admin Administrator
Object Types ←	Identity Sources			
C Networks	2 objects		Q Search	+ ~
\$ Ports	# NAME	TYPE	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				
Identity Sources				
1 Users				

Active Directory設定を追加します。

Identity Realm is used for Identity Policies and Remote this realm.	te Access VPN. Any changes impact all features that use
Name	Туре
Active_Directory	Active Directory (AD)
Directory Username	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

手順2:自己署名証明書の作成

キャプティブポータル設定を作成するには、キャプティブポータル用とSSL復号化用の2つの証明 書が必要です。

この例のように、自己署名証明書を作成できます。

```
[Objects] > [Certificates]に移動します。
```

CISCO. Firepower Devi	ice Ma	anager 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		B 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		
		3 DefaultInternalCertificate	Internal Certificate		
Geolocations		4 DefaultWebserverCertificate	Internal Certificate		

キャプティブポータル自己署名証明書:

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

SSL自己署名証明書:

Add Internal CA

Name	
ssl_captive_portal	
Country	State or Province
Maying (MAY)	Mavies
Mexico (MX)	 Miexico
Locality or City	
Mexico	
Organization	Organizational Unit (Department)
MexSecTAC	MexSecTAC
Common Name	
ss_fdmcaptive	
You must specify a Common Name to use t	the certificate with remote access VPN.
	CANCEL SAVE

ステップ3:IDルールの作成

[Policies] > [Identity] > [select [+]ボタンに移動し、新しいアイデンティティルールを追加します。

アクティブ認証を設定するには、アイデンティティポリシーを作成する必要があります。ポリシ ーには次の要素が含まれている必要があります。

- AD IDソース:手順1で追加したものと同じ
- Action:アクティブ認証
- ・サーバ証明書:前に作成したのと同じ自己署名証明書[このシナリオではcaptive_portal]
- Type:HTTP Basic (この例では)

Order Title	AD Identity Source	Action ACTIVE AUTHENTICATION For HTTP connections only, prompt for us	sername and password and
ad_captive	Active_Directory •	Additional authenticate against the specified identity intentity for the source IP address.	y source to obtain the user
Source / Destination Active authentication		Identity Sources are needed th Server Certificate (captive_p	ortal:885
SOURCE		ACTIVE AUTH Captive Portal is needed	_
Zones + Networks	+ Ports	NO AUTH	Ports/Protocols +
ANY ANY	ANY	ANY ANY	ANY

アイデンティティポリシーがアクティブ認証として作成されると、は自動的にSSLルールを作成 します。デフォルトでは、このルールはDecrypt-Resignを使用してanyとして設定されます。つま り、このルールに対するSSL変更はありません。

\Box \rightarrow SSL Decryption \rightarrow \bigotimes Identity \rightarrow \bigcirc Security Intelligence \rightarrow \bigcirc NAT \rightarrow \bigotimes Access Control \rightarrow Intrusion											
SSL Decryption	1 rule						Q Search				¢ +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
🕘 🔝 Identity Polic	y Active Authentica	tion Rules 🚺									
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.
SSL Native Rules	0										
SSL Native Rules SSL Native Rules There are no SSL Rules yet. Start by creating the first SSL rule. CREATE SSL RULE Or ADD PRE-DEFINED RULES											
	$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \bigcirc$ NAT $\rightarrow \oslash$ Access Control $\rightarrow $ \textcircled{s} Intrusion										

SSL Decryption	The rules i generated	in this section are from rules in the	e automatically e identity policy				Q Search				ф	+
N NAME	that implement active authentication. These SSL decryption rules are read-only. These rules are always evaluated before the SSL		popre	DESTINATION	NETWODKS	00075/89070	ADDI ICATIONS	1101 0	LICEBO		ACTIONS	
J Identity Policy Ac	tive Authentica	ation Rules 🚺	RETHORKS	PURIS	ZUNES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ľ	ACTIONS
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. CREATE SSL RULE or ADD PRE-DEFINED RULES												

ステップ4:アクセスコントロールポリシーへのアクセスルールの作成

ポート885/tcpを許可し**て、キャプティブポータル**認証にトラフィックをリダイレクトする必要が あります。[Policies] > [Access Control] に移動し、アクセスルールを追加します。

	Action			
ive	Allow 🗸			
Applications URLs ⁰ Use	ers Intrusion Policy Fi	ile policy Logging		
		DESTINATION		
+ Networks +	Ports +	Zones +	Networks +	Ports/Protocols +
ANY	ANY	ANY	ANY	\$ 885
;i	Applications URLs Us Networks + ANY	Action Action Action Action Anny Action Action Action Action Action Action Action Action Action Acti	Action Ve Action Applications URLs [®] Users Intrusion Policy File policy [®] Logging Networks + Ports + Zones + ANY ANY ANY ANY ANY	Action ve Image: Action Applications URLs URLs Users Intrusion Policy File policy Cones Metworks ANY ANY

ユーザーがADからダウンロードされたかどうか確認する必要がある場合、アクセス・ルールを編 集して「ユーザー」セクショ**ンに移動**し、「AVAILABLE USERS」で、FDMがすでに持っている ユーザー数を確認できます。

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

設定変更を必ず導入してください。

確認

HTTPSサイトに移動するときに、ユーザのデバイスがチェックボックスをオンになっていること を確認します。

S https://10.115.117.43:885/x.authi: × +								
← → 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							

ユーザADクレデンシャルを入力します。

C O 10.115.117.43.385/x.auth?s=d0F7LRChg4FXX28Cik46wfdQKDJMAXeaLGy/tejcuc43D8u=http%3A942P%2Fwrw.cisc.com%2F Sign in uses Sign in uses india: uses uses	https://10.115.117.43:88	35/x.auth? × +					
	- → C (10.1	15.117.43:885/x.auth?s=dOF7LR0	Chg4FKX2BCiK46wfdQKE	DJMAXeaLGcyYeiycu	c%3D&u=http%3A%2F%2Fw	ww.cisco.com%2F	
<complex-block></complex-block>					Sign in https://10.11 Username Password	5.117.43:885 ngfwtac	Sign in Cancel
<complex-block></complex-block>	Cisco - Networking, Cloud, and ⊂ X → C â cisco.com Cisco Fist ↓ ↓ ↓ CISCO	+ torm Subc) III Products Support & Learn	Partners Events & Videos				Q 옵 (#)
	Kiva	a and Cisco: Creating in retail opportunities	Active exploit of	of Kaseya VSA in supply-of	ehein attack. Read the Talos bio	g now	s time to take the lead
Cato System		Ē	A +		٩	888	Activate Windows

トラブルシュート

user_map_query.plスクリプトを使用して、FDMにユーザipマッピングがあることを検証できます

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)] clishモードでは、次のように設定できます。

system support identity-debug」を参照してください。

```
> 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
参考資料
```

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