# RADIUS上のMSCHAPv2を使用したFTDリモー トアクセスVPNの設定

## 内容

概要
 前提条件
 要件
 使用するコンポーネント
 背景説明
 設定
 ネットワーク図
 FMCによるAAA/RADIUS認証を使用したRA VPNの設定
 MS-CHAPv2を認証プロトコルとしてサポートするためのISEの設定
 確認
 トラブルシュート

### 概要

このドキュメントでは、リモート認証ダイヤルインユーザサービス(RADIUS)認証を使用するリモ ートアクセスVPNクライアントのFirepower Management Center(FMC)を介した認証方式として 、Microsoft Challenge Handshake Authentication Protocol(MS-CHAPv2)を有効にする方法につい て説明します。

## 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。

- Firepower Threat Defense(FTD)
- Firepower Management Center (FMC)
- Identity Services Engine ( ISE )
- Cisco AnyConnect セキュア モビリティ クライアント
- RADIUS プロトコル

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCv 7.0.0 (ビルド94)
- FTDv 7.0.0 (ビルド94)
- ISE:2.7.0.356

- AnyConnect 4.10.02086
- Windows 10 Pro

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

デフォルトでは、FTDはAnyConnect VPN接続用のRADIUSサーバの認証方式としてパスワード認証プロトコル(PAP)を使用します。

PAPは、ユーザが双方向ハンドシェイクでIDを確立するための簡単な方法を提供します。PAPパ スワードは共有秘密で暗号化され、最も高度ではない認証プロトコルです。PAPは、繰り返し発 生する試行錯誤からの保護をほとんど提供しないため、強力な認証方式ではありません。

MS-CHAPv2認証では、ピア間の相互認証とパスワード変更機能が導入されます。

VPN接続用にASAとRADIUSサーバ間で使用されるプロトコルとしてMS-CHAPv2を有効にするに は、接続プロファイルでパスワード管理を有効にする必要があります。パスワード管理を有効に すると、FTDからRADIUSサーバへのMS-CHAPv2認証要求が生成されます。

#### 設定

#### ネットワーク図



#### FMCによるAAA/RADIUS認証を使用したRA VPNの設定

手順については、次のドキュメントとビデオを参照してください。

- FTD での AnyConnect Remote Access VPN の設定
- FMCによって管理されるFTDの初期AnyConnect設定

ステップ1:リモートアクセスVPNが設定されたら、[**Devices**] > [Remote Access]に移動し、新し く作成した接続プロファイルを編集して、[AAA]タブに移動します。

Hitebower Management Center CISCO Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects AMP	Intelligence	Deploy Q 🗳 🗘 🙆 admin 🔻
RA_VPN			Save Carcel
Enter Description Connection Profile Access Interfaces Advanced			Exter Assocratic (1) Local Realm: None Dynamic Access Policy: None
		Edit Connection Profile	+
Name	AAA	Connection Profile:* RA_VPN	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	Group Policy.* DttGrpPolicy + +	/1
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Client Address Assignment AAA Aliases	D
		Authentication Authentication Method: Authentication Method: Authentication Server:	

[詳細設定]セク**ションを展開**し、[パスワード管理の有**効]チェックボックス**をオンにします。 [Save] をクリックします。

Firepower Management Center     Overview Analysis	Policies Devices Objects AMP	Intelligence	Deploy Q. 🧬 🗘 😝 admin •
RA_VPN			Save Cancel
Enter Description			
			Policy Assignments.(1)
Connection Profile Access Interfaces Advanced			Local Healm: None Dynamic Access Policy: None
		Edit Connection Profile	+
Name	AAA		
	Authentication: None	Connection Profile." RA_VPN	6
DefaultWEBVPNDroup	Authorization: None Accounting: None	Group Policy.* DttGrpPolicy + +	/1
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Client Address Assignment AAA Aliases	∕≆
		Use secondary authentication	
		Authorization	
		Authorization Server: Use same authentication server *	
		Allow connection only if user exists in authorization database	
		Accounting Server:	
		Advanced Settings	
		Strip Realm from usemame	
		Strip Group from username	
		Enable Password Management	
		Notify User     14     days prior to password expiration	
		Notify user on the day of password expiration	
		×	
		Cancel	

保存して展開。

Policies Devices Objects AMP Intelligence		Deploy 🔍 🧬 🗘 😝 admin •
	You have	e unsaved changes Save Cancel
		Parlies: Assistent and (1)
	Local Realm: None	Dynamic Access Policy: None
		+
AAA	Group Policy	
Authentication: None Authorization: None Accounting: None	B DROrpPolicy	/1
Authentication: ISE_Server (IRADIUS) Authorization: ISE_Server (IRADIUS) Accounting: None	Ph DhtGrpPolicy	/1
	Adda Adda Adda Adda Addrestication: Nove Addrestication: Nove	Addie     Original Mathematication: Nove       Advantantication: Nove

FTD CLIでのリモートアクセスVPNの設定は次のとおりです。

ip local pool AC\_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0 interface GigabitEthernet0/0 nameif Outside\_Int security-level 0 ip address 192.168.0.100 255.255.255.0 aaa-server ISE\_Server protocol radius aaa-server ISE\_Server host 172.16.0.8 key \*\*\*\*\* authentication-port 1812 accounting-port 1813 crypto ca trustpoint RAVPN\_Self-Signed\_Cert enrollment self fqdn none subject-name CN=192.168.0.100 keypair <Default-RSA-Key> crl configure ssl trust-point RAVPN\_Self-Signed\_Cert webvpn enable Outside\_Int http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache no disable error-recovery disable group-policy DfltGrpPolicy attributes vpn-tunnel-protocol ikev2 ssl-client user-authentication-idle-timeout none webvpn anyconnect keep-installer none anyconnect modules value none anyconnect ask none default anyconnect http-comp none activex-relay disable file-entry disable file-browsing disable url-entry disable deny-message none tunnel-group RA\_VPN type remote-access tunnel-group RA\_VPN general-attributes address-pool AC\_Pool authentication-server-group ISE\_Server password-management tunnel-group RA\_VPN webvpn-attributes

#### MS-CHAPv2を認証プロトコルとしてサポートするためのISEの設定

次のことを前提としています。

- 1. FTDはISEのネットワークデバイスとしてすでに追加されているため、FTDからRADIUSア クセス要求を処理できます。
- 2. ISEがAnyConnectクライアントを認証するために使用できるユーザが少なくとも1人あります。

ステップ2:[**Policy**] > [Policy Sets]に移動し、AnyConnectユーザが認証されたポリシーセットに関 連付けられている[Allowed Protocols]ポリシーを見つけます。この例では、1つのポリシーセット のみが存在するため、対象のポリシーは*Default Network Accessです*。



ステップ3:[Policy] > [Policy Elements] > [Results]に移動します。[Authentication] > [Allowed Protocols]で、[Default Network Access]を選択して編集します。

-devide Identity Services Engine Home + Context Visibility + Operations	Policy      Administration      Work Centers	Lidensa Warning 🔺 🔍 🎯 🌞 O
Policy Sets Profiling Posture Client Provisioning + Policy Elements	Policy Sets Profiling	
	Posture Ctient Provisioning	
Policy Sets	Policy Elements	Reset Policyset Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search		
		+
Default Default policy set		Default NationAl Access ** + 24 O >

dently Services Engine	Home + Context Vability + Operations + Rolloy + Administration + Wok Centers	License Warning 📥	۹. (	0 c	0
Policy Sets Profiling Posture (	Slent Providening Policy Elements				
Dictionaries + Conditions + Resu					
Authentication	Allowed Protocols Services for Patig Equat gate Administration > Bytem > Bedup & Electors > Patig Equat Page			neted 1   7	turi 🚯
Allowed Protocols	/ for	Show Al	_		16
Authorization	Service Name   Description				
+ Profiling	Cafault Network Access Default Allowed Protocol Service				
+ Posture					
+ Client Provisioning					

[Allow MS-CHAPv2]チェ**ックボックスがオンになっている**ことを確認してください。下にスクロールして[保存]します。



## 確認

Cisco AnyConnectセキュアモビリティクライアントがインストールされているクライアントマシンに移動します。FTDヘッドエンド(この例ではWindowsマシンを使用)に接続し、ユーザクレデンシャルを入力します。

🔇 Cisco AnyC	onnect Secure Mobility Client			$\times$
	<b>VPN:</b> Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:33			I	Pv4
<b>\$</b> ()				dinihi cisco

ISEのRADIUSライブログには次のように表示されます。

Endpoint Profile

tity Group

Location

ntication Protocol

erview		
Event	5200 Authentication succeeded	
Usemame	user1	
Endpoint Id	00.50.56.96.46.6F 🕀	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Static IP Address User 1	
Authorization Result	Static/PaddressUser1	
thentication Details		
thentication Details	2021-09-28 60 00 02 94	
thentication Details Source Timestamp Received Timestamp	2021-09-28 00 06 02 94 2021-09-28 00 06 02 94	
thentication Details Source Timestamp Received Timestamp Policy Server	2021-09-28-00-06-02-94 2021-09-28-00-06-92-94 driversp-186-3-7	
thentication Details Source Timestamp Received Timestamp Policy Server Event	2021-09-28 00 06 02 94 2021-09-28 00 06 02 94 driverse-186-27 6200 Authentication successfed	
thentication Details Source Timestamp Received Timestamp Policy Server Event Username	2021-09-28 00 06 02 94 2021-09-28 00 06 02 94 entways-156-27 5000 Authentication succeeded user1	
thentication Details Source Timestamp Received Timestamp Policy Server Event Username User Type	2021-09-26 00:06:02:04 2021-09-28 00:06:02:04 enverys-150-27 8:00 Authentication succeeded user	
sthentication Details Source Timestamp Received Timestamp Policy Server Event Usersame User Type Endpoint Id	2021-09-28 00 06 02 94 2021-09-28 00 06 02 94 driverup-156-2.7 E 250 Authentitation succeeded user 1 User 00 00 05 05 06 45 0F	

Windows10-Workstal

04800540000 MSCHAPV2 MSCHAPV2

All Locations

DRIVERAP\_FTD\_7.0

Authentication Identity Store Internal Users Workstation

ice Type All Device Types

NAS IPv4 Address 0.0.0.0

#### Steps

- Decision
   Description

   11001
   Reactived RADUS Access Request

   11001
   Reactived RADUS Access Request

   11001
   Revealed Revealed

- 2007 Automatation Parad 2016 Automatation Parad 2016 Standborn to use A data Dealby 2019 Evaluation to use A data Dealby 2020 Looing up English Antonia Edgelish Otto 2021 Looing up English Antonia Edgelish Otto 2021 Dealby Control In Hermal Edgelish Otto 2021 Bouries IPP Radia Laberkame 2021 Standborn John Standborn Science 2021 Max essence particip seed 2021 Rest Edgelish Standborn Science and 2021 Rest Edgelish Standborn Standborn 2021 Max essence particip seed 2021 Rest Rest Standborn Science and 2022 Restment RADUS Access-Accept

ruenally betwices crigine	
NAS Port Type	Vitual
Authorization Profile	Static/PaddressUser1
Response Time	231 milliseconds
Other Attributes	
ConfigVersionId	547
DestinationPort	1812
Protocol	Radius
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
MS-CHAP-Challenge	01.41:04:#145:b1.41:5b:4d:b6:97:1b:b7:fe:e8:c8
MS-CHAP2-Response	00 00 65 da ab 20 e4 45 ft 12 f7 6c 20 do af 19 45 a9 00 00 00 00 00 00 00 00 00 00 00 00 00
CVPH2000/ASA/PD/7x-Tunnel- Group Name	RA_VPN
NetworkDeviceProfileId	b0099505-3150-4215-a80a-6753645b#56o
Is ThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/25
SelectedAuthenticationIdentityStore	s Internal Users
SelectedAuthenticationIdentityStore	AILAD_Join_Points
SelectedAuthenticationIdentityStore	s Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
15EPolicySettame	Default
Identity SelectionMatchedRule	Default
DTLS Support	Uningwn
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco

	indim Skridevice. usk-c058/01718/201782/B156124621184408598C717837D388C030F skridesesson-id-ska50048000400001525x49, isosure-e192.188.0101, coe-publifixe
	mdm dv=device-
CiscoAVPair	mdm-6v=device-uid- global+158F88E0DDF52F3F2CDE2431456F48AA2AE2C083,
	mdm/divradevice-public-macr/00-85-86-86-46-46. mdm/divradevice-gentPAnyConnect Windows 4.10.02086, mdm/divrdevice-gentVMase, Inc, VMaser Virtual Platform,
	mdm/thvndevice-platform=win, mdm/thvndevice-platform=venicn=10.0.18362 , mdm-thvndevice-platform-venicn=10.0.18362 ,
Called-Station-ID	192,158.0.100
CPMSessionD	
Poulos IR Address	19971
EnableFlag	Enabled
IPSEC	IPSEC#Is IPSEC Device#No
Device Type	Device Type#All Device Types

**注:test aaa-server authenticationコマンド**は、常にPAPを使用して認証要求をRADIUSサー

バに送信します。このコマンドを使用してファイアウォールにMS-CHAPv2を使用させる方 法はありません。

firepower# **test aaa-server authentication ISE\_Server host 172.16.0.8 username user1 password XXXXXX** INFO:IPアドレス(172.16.0.8)への認証テストを試みています(タイムアウト:12 秒) INFO:Authentication Successful

注:Flex-configを使用してtunnel-group ppp-attributesを変更しないでください。これは、 AnyConnect VPN(SSLおよびIPSec)接続のRADIUSでネゴシエートされた認証プロトコ ルには影響を与えません。

tunnel-group RA\_VPN ppp-attributes no authentication pap 認証CHAP authentication ms-chap-v1 no authentication ms-chap-v2 no authentication eap-proxy

## トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

FTD:

• debug radius all

ISE:

• RADIUS ライブ ログ