Configuration du VPN d'accès distant FTD avec MSCHAPv2 sur RADIUS

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Diagramme du réseau Configuration du VPN RA avec authentification AAA/RADIUS via FMC Configurer ISE pour prendre en charge MS-CHAPv2 en tant que protocole d'authentification Vérification Dépannage

Introduction

Ce document décrit comment activer Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) en tant que méthode d'authentification via Firepower Management Center (FMC) pour les clients VPN d'accès distant avec authentification RADIUS (Remote Authentication Dial-In User Service).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Identity Services Engine (ISE)
- Client de mobilité sécurisée Cisco AnyConnect
- protocole RADIUS

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- FMCv 7.0.0 (build 94)
- FTDv 7.0.0 (build 94)
- ISE 2.7.0.356

- AnyConnect 4.10.02086
- Windows 10 Pro

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Par défaut, FTD utilise le protocole PAP (Password Authentication Protocol) comme méthode d'authentification avec les serveurs RADIUS pour les connexions VPN AnyConnect.

Le protocole PAP fournit une méthode simple permettant aux utilisateurs d'établir leur identité à l'aide d'un échange en deux étapes. Le mot de passe PAP est chiffré avec un secret partagé et est le protocole d'authentification le moins sophistiqué. Le protocole PAP n'est pas une méthode d'authentification puissante car il offre peu de protection contre les attaques répétées par essais et erreurs.

L'authentification MS-CHAPv2 introduit l'authentification mutuelle entre homologues et une fonction de modification du mot de passe.

Afin d'activer MS-CHAPv2 comme protocole utilisé entre l'ASA et le serveur RADIUS pour une connexion VPN, la gestion des mots de passe doit être activée dans le profil de connexion. L'activation de la gestion des mots de passe génère une demande d'authentification MS-CHAPv2 du FTD au serveur RADIUS.

Configuration

Diagramme du réseau



Configuration du VPN RA avec authentification AAA/RADIUS via FMC

Pour une procédure pas à pas, reportez-vous à ce document et à cette vidéo :

- <u>Configuration VPN d'accès à distance AnyConnect sur FTD</u>
- <u>Configuration AnyConnect initiale pour FTD géré par FMC</u>

Étape 1. Une fois le VPN d'accès à distance configuré, accédez à **Périphériques > Accès à distance**, modifiez le profil de connexion nouvellement créé, puis accédez à l'onglet **AAA**.

Hindly Firepower Management Center Overview Analysis Devices / VPN / Edit Connection Profile	Policies Devices Objects AMP	Intelligence	Deploy Q, 🧬 🗘 😝 admin •
RA_VPN			Sive Cancel
Enter Description			
			Post Association
Connection Profile Access Interfaces Advanced			Local Heart, None Ughamic Access Policy, None
		Edit Connection Profile	+
Name	AAA		
	Authentication: None	Connection Profile:* RA_VPN	
DefaultWEBVPNGroup	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: AAA Only *	
		Authentication Server: ISE_Server (RADIUS) +	
		Fallback to LOCAL Authentication	
		Use secondary authentication	
		Authorization	
		Authorization Server: Use same authentication server *	
		Allow connection only if user exists in authorization database	
		Accounting Server:	
		Advanced Settings	
		Cancel	

Développez la section **Paramètres avancés** et activez la case à cocher **Activer la gestion des mots de passe**. Click **Save**.

Gisco Devices / VPN / Edit Connection Profile Overview Analysis P	olicies Devices Objects AMP	Intelligence	Deploy Q 💕 🗘 😝 admin •
RA_VPN			Save Cancel
Enter Description Connection Profile Access Interfaces Advanced		Local	Policy Assignments (1) Realm: None Dynamic Access Policy: None
		Edit Connection Profile	+
Name	АЛА	Connection Profile.* RA_VPN	
DefaultWEBVPNOroup	Authentication: None Authorization: None Accounting: None	Group Policy.* DthOrpPolicy + +	/i
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Eff Grup Puky Client Address Assignment AAA Aliases	/i
		Curce Plasmed sufferitions	

Enregistrer et déployer.

CISCO Devices / VPN / Edit Connection Profile Overview Analysis Pr	olicies Devices Objects AMP Intelligence		Deploy 🔍 🧬 🌣 😝 admin •
RA_VPN		You have	e unsaved changes Save Cancel
Enter Description			Balley Barlander (B)
Connection Profile Access Interfaces Advanced		Local Realm: None	Dynamic Access Policy: None
			+
Name	AAA	Group Policy	
DefaultWEBVPHOroup	Authentication: None Authentication: None Accounting: None	Pa DR0rpPolicy	/1
RA_VPN	Authentication: (EE_Server (RADRUS) Authonization: ISE_Server (RADRUS) Accounting: Norm	Pa DR0rpPolicy	/1

La configuration VPN d'accès à distance sur l'interface de ligne de commande FTD est la suivante :

```
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
```

group-alias RA_VPN enable

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

Configurer ISE pour prendre en charge MS-CHAPv2 en tant que protocole d'authentification

On suppose que :

- 1. Le FTD est déjà ajouté en tant que périphérique réseau sur ISE afin de pouvoir traiter les demandes d'accès RADIUS à partir du FTD.
- 2. Au moins un utilisateur est disponible pour ISE pour authentifier le client AnyConnect.

Étape 2. Accédez à **Policy > Policy Sets** et recherchez la stratégie **Allowed Protocols** associée au Policy Set où vos utilisateurs AnyConnect sont authentifiés. Dans cet exemple, un seul ensemble de stratégies est présent, de sorte que la stratégie en question est *Accès réseau par défaut*.

ence identity Services Engine Home Context Visibility Operations	Policy Administration	* Work Centers			License Warning 🔺	4 0 o 0 <u>^</u>
Summary Endpoints Quests Vulnerability Threat	Pulicy Sets	Profiling				Ø -
METRICS	Policy Elements	Client Provisioning				- ø
Total Endpoints Active Endpoint	Conditional Conditional	Anomalous Behavior @	Authenticated Guests ()	BYOD Endpoints Cor	mpliance 0	
⊆ 1 ² 1 ,			0	0 0%	0	
AUTHENTICATIONS 0	Φσ×	NETWORK DEVICES Device Name Type Location	6 0 X	ENDPOINTS O		₽ ¤ ×
interusers: [100%]		drivea5506: [50%]	drived_7.0; [50%]	workstations: [100%]		
II BYOD ENDPOINTS €	ΒQX	II ALARMS 0	a o x	II SYSTEM SUMMARY 0		e o x
Tge Prote		Severity Name Occu Last Occurr	ed	1 node(s)		AI - 24HR -
No data available.		w Name		💿 📑 driverap-ISE-2-7		
		Feeching data from server		No da	a available	
https://10.31.124.31:6012/admin/#policy/policy_grouping_new						
-devils. Identity Senices Engine ноле + Contact Visibility + Operations Policy Sets Profiling Posure Client Provisioning + Policy Elements	Policy Administration	* Work Centers			License Warning	<u> </u>
Policy Sets					Reset Policyset Hitcour	ts Reset Save
Status Policy Set Name Description	Conditions			Allowed Proto	cols / Server Sequence Hits	Actions View
Search						
		+				
Default Default policy set				Default Netwo	R Access # * + 24	• >

Étape 3. Accédez à Stratégie > Eléments de stratégie > Résultats. Sous Authentication > Allowed Protocols, sélectionnez et modifiez Default Network Access.

Identity Services Engine	Home + Context Visibility + Operations	Policy Administration Work	Centers	License Warring 🔺	Q 0 0 0	o -
Policy Sets Profiling Posture	Client Provisioning + Policy Elements	Policy Sets Profi	ling			
		Posture Clier	t Provisioning			
Policy Sets		Policy Elements		Reset Policyset Hitcounts		
+ Otabus Dation Date	lama Description	Conditions		Alternal Destantia / Desser Destantia / Miles 4	view View	
o status Policy Set P	vame Description	Results		Allowed Protocols / Server Sequence Price A	coons view	
Search						
				+		
(P) Default	Default policy set			Default Network Access # * + + 24	• •	
•						
cisco Identity Services Engine	Home Context Visibility Operations	Policy Administration Work	Centers	Lisense Warning 🛕	A 🔍 o 🤤	o.
Policy Sets Profiling Posture	Client Provisioning Policy Elements					
Dictionaries + Conditions + Resu	-15 C					
* Authentication	Allowed Protocols Services For Policy Export go to Administration > System >	Backup & Restore > Policy Export Page				
Allowed Protocols	_				Gelected 1 Total 1 🧐	£
+ Authorization	✓ Edit - Add ≥ Duplicate X Delete			Show AI	V	ő
	Service Name Description	54				
+ Profiling	Certault Network Access Default A	Klowed Protocol Service				

Assurez-vous que la case **Allow MS-CHAPv2** est cochée. Faites défiler jusqu'en bas et **enregistrez**-le.



Vérification

Accédez à la machine cliente sur laquelle le client Cisco AnyConnect Secure Mobility est installé. Connectez-vous à la tête de réseau FTD (un ordinateur Windows est utilisé dans cet exemple) et saisissez les informations d'identification de l'utilisateur.



Les journaux en direct RADIUS sur ISE montrent :

dentity Services Engine		
Verview		Steps
Event	\$300 Authentication successful	11001 Received RADIUS Access-Request
		11917 RADIUS created a new session
Usemame	user1	15049 Evaluating Policy Group
Endpoint Id	00.50 56.96.46.6F (B)	1000 Evaluating Service Selection Policy
Endpoint Profile	Windows10-Workstation	10041 (paralog) Dentity Printy 10042 - Overside PRO, Neurophical English Read Section 2010
		10VHP superior I'm - Hermanian Industria (Balance) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1
Authentication Policy	Default >> Default	15013 Saladad Salada Unana Unan
Authorization Policy	Default >> Static IP Address User 1	24219 Looking up User in Internal Users IDStore - user1
Authorization Result	StatidPaddressUser1	24212 Found User in Internal Users IOStore
		22037 Authentication Passed
		24/15 JEE has not onfineed locally previous successful machine 24/15 Automatication for water in Adverse Desetory
Authentication Details		10036 Evaluating Authorization Policy
		24209 Looking up Endpoint in Internal Endpoints (OStore - user1
Source Timestamp	2021-09-28 00:06:02:94	24211 Found Endpoint in Internal Endpoint IDStore
eceived Timestamp	2021-09-28 00.00.02.94	15041 Queried PIP - Radius User-Name
		16016 Selected Authorization Profile - StatictPaddessUser1
Policy Server	driverap-ISE-2-7	22081 Max sessions policy passed
Event	5200 Authentication succeeded	22080 New accounting session created in Session cache
Username	usert	11002 Returned RADUS Access-Accept
User Type	User	
Endpoint Id	00.50.50.90.40.0F	
Calling Station M	102 148 0 101	
carring exacts of		
Endpoint Protile	minuous re-monstation	
Authentication Identity Store	Internal Users	
Identity Group	Workstation	
Audit Session Id	d2a300840000e00081525o49	
Authentication Method	MSCHAPV2	
Authentication Protocol	MSCHAPV2	
Network Device	DRIVERAP_FTD_7.0	
Device Type	All Device Types	
Location	All Locations	

deale Identity Services Engine

NAS Port Type	litual
Authorization Profile	StatidPaddressUser1
Response Time	231 milliseconds
2	
Other Attributes	
ConfigVersionId	547
DestinationPort	10.12
Protocol	Radus
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
MS-CHAP-Challenge	014f04 tt 45 bf 4f 5b 4d b6 97.1b b7.5e e8 c8
MS-CHAP2-Response	00 00 65 da ab 20 e4 45 ft 12 f7 6c 20 dc at 19 45 a9 00 00 00 00 00 00 00 00 00 00 06 4f 29 52 90 5a 2c e1 d9 e7 50 3c to Ba 73 32 a9 5d b4 27 bb 5d 99
CVPN3000/ASA/PD/7x-Tunnel- Group-Name	RA_VPN
NetworkDeviceProfileId	b0099505-3150-4215-a80a-6753645b/58o
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PDC7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/25
SelectedAuthenticationIdentityStore	a Internal Users
SelectedAuthenticationIdentityStores	AILAD_Join_Points
SelectedAuthenticationIdentityStore	a Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
1SEPolicySettlame	Default
Identity Selection/MatchedRule	Default
DTLS Support	Uhingwn
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco

MS-CHAP2-Success	00 53.3d 33.30 30 33.46 33.30 37.38 34.42 43.46 32 33.46 41.31 39 37 3 32.44 45 39 30 39 44 41 35 37 31 36 44 35 41 43 45 43 41
cisco-av-pair	profile-name=Windows10-Workstation
Class	CACS (0x800540000x00081525x49 driverap-ISE-2-7/417494975/25
Framed-IP-Address	10.0.50.101
esult	
CiscoAVPair	Internetissing platforms recorded 41 st methods and spatial and spatial and spatial and spatial methods and spatial and spatial and spatial filterates. If 2028, methods and spatial and spatial filterates and spatial global State Spatial and spatial and spatial and spatial methods and spatial and spatial and spatial and spatial spatial and spatial and spatial and spatial and spatial and spatial spatial and spatial and spatial and spatial and spatial and spatial spatial and spatial and spatial and spatial and spatial and spatial and spatial spatial and spatial and spatial and spatial and spatial and spatial and spatial spatial and spatial and spatial and spatial and spatial and spatial and spatial and spatial spatial and spatial and spat
Called-Station-ID	192, 108.0. 100 mdm/dvvice-platformwein,
CPMSessionID	c0a800540000e00051525e49
Device IP Address	192.168.0.100
RADIUS Username	user1
EnableFlag	Enabled
IP SEC	IPSEC#s IPSEC Device#No
Device Type	Device Type#All Device Types

Remarque : la commande **test aaa-server authentication** utilise toujours PAP pour envoyer des requêtes d'authentification au serveur RADIUS, il n'y a aucun moyen de forcer le parefeu à utiliser MS-CHAPv2 avec cette commande.

firepower# test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX INFORMATIONS : Tentative de test d'authentification sur l'adresse IP (172.16.0.8) (déli

INFORMATIONS : Tentative de test d'authentification sur l'adresse IP (172.16.0.8) (délai d'attente : 12 secondes) INFORMATIONS : Authentification réussie

Note: Ne modifiez pas **les attributs ppp-group tunnel** via Flex-config, car cela n'a aucun effet sur les protocoles d'authentification négociés sur RADIUS pour les connexions VPN AnyConnect (SSL et IPSec).

tunnel-group RA_VPN ppp-attribute

no authentication pap authentication chap authentication ms-chap-v1 no authentication ms-chap-v2 no authentication eap-proxy

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Sur FTD :

• debug radius all

Sur ISE :

• Journaux en direct RADIUS