使用MSCHAPv2 over RADIUS設定FTD遠端存取 VPN

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> 設定 <u>網路圖表</u> 通過FMC配置具有AAA/RADIUS身份驗證的RA VPN</u> 配置ISE以支援MS-CHAPv2作為身份驗證協定 <u>驗證</u> <u>疑難排解</u>

簡介

本文檔介紹如何通過Firepower管理中心(FMC),為具有遠端身份驗證撥入使用者服務(RADIUS)身 份驗證的遠端訪問VPN客戶端啟用Microsoft質詢握手身份驗證協定版本2(MS-CHAPv2)作為身份驗 證方法。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- 身分識別服務引擎 (ISE)
- Cisco AnyConnect Security Mobility Solution 遠端存取
- RADIUS通訊協定

採用元件

本檔案中的資訊是根據以下軟體版本:

- •FMCv-7.0.0(內部版本94)
- •FTDv-7.0.0(內部版本94)
- ISE 2.7.0.356
- AnyConnect 4.10.02086

• Windows 10 Pro

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

預設情況下,FTD使用密碼驗證通訊協定(PAP)作為AnyConnect VPN連線的RADIUS伺服器的驗證 方法。

PAP為使用者提供了一種通過雙向握手建立其身份的簡單方法。PAP密碼使用共用金鑰加密,並且 是最簡單的身份驗證協定。PAP不是一種強大的身份驗證方法,因為它幾乎無法防止反複的試錯攻 擊。

MS-CHAPv2身份驗證引入了對等體之間的相互身份驗證和更改密碼功能。

要啟用MS-CHAPv2作為ASA和RADIUS伺服器之間用於VPN連線的協定,必須在連線配置檔案中啟 用密碼管理。啟用密碼管理會生成從FTD到RADIUS伺服器的MS-CHAPv2身份驗證請求。

設定

網路圖表



通過FMC配置具有AAA/RADIUS身份驗證的RA VPN

如需逐步程式,請參閱本檔案及以下影片:

- FTD上的AnyConnect遠端存取VPN組態
- FMC管理的FTD的初始AnyConnect配置

步驟1.配置遠端訪問VPN後,導航到**Devices > Remote Access**,編輯新建立的連線配置檔案,然後 導航到AAA頁籤。

International Content Center Overview Analysis International Content Overview Analysis	Policies Devices Objects AMP	Intelligence	Deploy 🔍 💕 🌣 📵 admin •
RA_VPN			Save Cancel
Enter Description Connection Profile Access Interfaces Advanced			Editor Assistants (1) Local Realm: None Dynamic Access Policy: None
		Edit Connection Profile	+
Name	AAA	Connection Profile:* RA_VPN	
DefaultWEBVPtvOroup	Authentication: None Authorization: None Accounting: None	Group Policy.* DthDpPolicy + +	/1
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Client Address Assignment AAA Aliases	D
		Authentication Authentication Method: MAA.Ony Authentication Server: Estimate (BALDUS) - Patback to LOCAL Authentication - Urbe secondary authentication - Urbe secondary authentication server: - Authorization - Authorization Server: - Authorization Server: - Authorization Server: - Accounting - Accounting Server: - Advanced Settings	

展開Advanced Settings部分,然後按一下Enable Password Management覈取方塊。按一下「Save」。

Sisco Devices / VPN / Edit Connection Profile Overview Analysis P	Policies Devices Objects AMP	Intelligence		Deploy Q 🔮 🌣 🔕 admin •
RA_VPN				Save Cancel
Enter Description Connection Profile Access Interfaces Advanced			Local Realm: None	Policy Assignments (1) Dynamic Access Policy: None
		Edit Connection Profile		+
Name	AAA	Connection Profile:* RA_VPN		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	Group Policy.* DthGrpPolicy + +		/¥
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Client Address Assignment AAA Aliases		20 C
		I use secodary sufferitionsion Authorization Authorization Authorization Authorization Authorization Berrier Cocurring Autorization Output user Strug Request in sufferitation distance Strug Request in sufferitation Strug Request in sufferitation Otodry User I dot y user on the day of password expiration		

儲存和部署。

cisco Devices / VPN / Edit Connection Profile Overview Analysis Pr	olicies Devices Objects AMP Intelligence		Deploy 🔍 🕼 🌣 🔕 admin 🔹
RA_VPN		You have un	nsaved changes Save Cancel
Enter Description Connection Profile Access Interfaces Advanced		Local Realm: None	Policy Assignments (1) Dynamic Access Policy: None
			+
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authentication: None Accounting: None	Ba DRorpPolicy	/1
RA_VPN	Authonitication: SE_Seneer (RADIUS) Authonitation: SE_Seneer (RADIUS) Accounting: Home	B DttorpPolicy	/1

FTD CLI上的遠端存取VPN組態如下:

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 group-alias RA_VPN enable

配置ISE以支援MS-CHAPv2作為身份驗證協定

假設:

- 1. FTD已作為ISE上的網路裝置新增,因此它可以處理來自FTD的RADIUS存取要求。
- 2. 至少有一個使用者可用於ISE對AnyConnect客戶端進行身份驗證。

步驟2.導覽至**Policy > Policy Sets**,並找到**Allowed Protocols**策略附加到您的AnyConnect使用者進 行身份驗證的策略集。在本示例中,僅存在一個策略集,因此所討論的策略是*預設網路訪問*。



步驟3.導覽至Policy > Policy Elements > Results。在Authentication > Allowed Protocols下,選擇 並編輯Default Network Access。

cisco	dentity Servi	ices Engine Hor	ve + Context Visibility + Operations	Policy Administration	Work Centers	License Warring 📥 🔍	0 0 0
Policy	Sets Profili	ng Posture Client P	hovisioning + Policy Elements	Policy Sets	Profiling		
				Posture	Client Provisioning		
Policy	Sets			Policy Elements Dictionaries		Reset Policyset Hiccounts R	
٠	Status	Policy Set Name	Description	Conditions	1	Allowed Protocots / Server Sequence Hits Action	s View
Search					•		
						+	
	0	Default	Default policy set			Default Network Access ** + 24 Q	>
obobs	dentity Servi	ces Engine un	a A Contract Machilles - A Constantions		a Mind Pantan	Lionne Warring 🛕 🔍	0 0 0
Policy 1	iets Profilir	ng Posture Client P	rovisioning Policy Elements	- Pointy	P man Genara		
Diction	ries + Con	ditions Results					
		0					
+ Authen	lication	Alk	wed Protocols Services Policy Export go to Administration > System	> Backup & Restore > Policy Export P	999		
Allow	d Protocols		the state is building White				Seechel Total 1
+ Authori	zation		Service Name . Descrip	tion		2008	. 0
+ Profile	9		Default Network Access Default	Allowed Protocol Service			
1 Pasket							
+ Client I	revisioning						

確保選中Allow MS-CHAPv2覈取方塊。一直向下滾動,然後儲存它。



驗證

導航到安裝Cisco AnyConnect安全移動客戶端的客戶端電腦。連線到FTD頭端(此範例中使用的是Windows電腦),並鍵入使用者憑證。

🚳 Cisco AnyC	onnect Secure Mobility Client			×
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:33			IPv4	4
\$ (i)			(1) (15	ilii co

ISE上的RADIUS即時日誌顯示:

Endpoint Profile

tity Group

Location

-

Event	5200 Authentication succeeded	
Jsemame	user1	
Endpoint Id	00.50.56.56.46.6F B	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Static IP Address User 1	
thentication Details	StatioPaddwaiUaer1	
Authorization Result	StatidRedRedDext/ter1	
thentication Result thentication Details Source Timestamp Received Timestamp	StatidPedewal/ker1 2021-09-29 00:06:02:94 2021-09-29 00:06:02:94	
Authorization Result thentication Details Source Timestamp Received Timestamp Policy Server	StatioPAdewarber1 2021-09-28 00 056 02 54 2021-09-28 00 055 294 detempol 556-27	
thentication Result thentication Details Source Timestamp Policy Server Event	StatioPedewscher1 2021-09-28 00 06 02 94 2022-09-28 00 06 02 94 diversp-156-0-7 5029 Authentiation successided	
thentication Result thentication Details Source Timestamp Policy Server Event Sservame	StatioPedeworkher1 2021-04-28 00 05 02 54 2022-04-28 00 05 02 54 driversyst8-0-7 5009 Authentioston succeeded user1	
thentication Result thentication Details Source Timestamp Received Timestamp Policy Server Event Jsername Jser Type	50410PA65exUver1 2021-05-28 00:00:02:94 2021-05-28 00:00:02:94 2021-05-28 00:00:02:94 2014emp-186-3-7 5020-4.04emficiation successed user1 User	

Windows10-Worksta

c0a800840000

All Locations

Authentication Identity Store Internal Users Workstation

Session Id dba50054000000 entication Method MSCHAPV2 entication Protocol MSCHAPV2 work Device ORIVERAP_FTD_7.0 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 Destay, 2019 Selaviang Aurosator Poly 2020 Losing to English Internat English 2017 2021 Sourid pP Radia Late-frame 2019 Selaviang Automatation Poly 2021 Selaviang Automatation Poly 2021 Selaviang Automatation Poly 2021 Selaviang Automatation Poly 2021 Max estanton policy parad 2021 Rest Restards Automation Selavian 2021 Restard Restards Automation Policy 2021 Restard Restards Automation 2021 Restard Restard Restard Restard Restard Restard Restard 2021 Restard Re

Identity Services Engine	
NAS Port Type	Vitual
Authorization Profile	Static/Paddres/User1
Response Time	231 milliseconds
3	
Other Attributes	
ConfigVersionId	547
DestinationPort	1812
Protocol	Radius
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
MS-CHAP-Challenge	0f.4f.04.ft.45.bf.4f.5b.4d.b5.97.1b.b7.fe.e8.c8
MS-CHAP2-Response	00 00 65 de ab 20 e4 45 ff 12 f7 6c 20 dc af 19 45 a9 00 00 00 00 00 00 00 00 00 00 00 00 00
CVPN3000/ASA/PUC7x-Tunnel-	0.4 1/041
Group Name	NA_VEN
NetworkDeviceProfileId	b0099505-3150-4215-a80a-0753c45b/50c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PUC7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/25
SelectedAuthenticationIdentityStore	s Internal Users
SelectedAuthenticationIdentityStore	s All_AD_Join_Points
SelectedAuthenticationIdentityStore	s Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
15EPolicySetName	Default
Identity SelectionMatchedRule	Default
D7LSSupport	Uninown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco

Class cisco-av-pair MS-CHAP2-Success	CACS: dbaloo4000e00001122x48 diversp-ISE-274174H97825 profile-name*Vindost b-Vindetalion 00 53 45 33 05 35 34 54 53 36 73 38 34 42 43 46 32 33 46 41 31 39 37 37 32 44 45 55 35 35 44 41 35 37 31 38 44 34 41 43 48 42 41
Class cisco-av-pair	CACS:dba000540000e00001525648.dtiverap-ISE-2.7/417494978/25 profile-name=Windows10-Wioklatation
Class	CACS xba800540000400081525x49 driverap-ISE-2-7/417494978/25
Framed-IP-Address	10.0.50.101
esult	
Cisco#/Pair	mon tor-version units globan 1914 ERECORD S27372CCRE2431455748AA2AE2C003, unit-CCB447571765782751451246211844485496C717E370388C030F 9449CCB80744, audit-sealion-inf-scala80004600081525c48, (parameter and an on tor- computative
	mdm illumder-los plasticamento, mdm illumder-los do do Bola 40.61 mdm illumder-los do do Bola 40.61 mdm illumder-los plasticamento do do do do do do do do mdm illumder-los plasticamento do do do do do do do do mdm illumder-los plasticamento, Toxi Values VII.01 D0208, mdm illumder-los plasticamento, Toxi Values VII.01 D0208,
Called-Station-ID	192.108.0.100
CPMSessionID	c0a800640000a00061525o49
Device IP Address	192.108.0.100
RADIUS Username	user1
Fabisfias	Enabled
-	serve general serve gene
Device Type	Device Tune#All Device Tunes

註:test aaa-server authentication命令始終使用PAP向RADIUS伺服器傳送身份驗證請求,無

法通過此命令強制防火牆使用MS-CHAPv2。

firepower# **test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXX** 資訊:正在嘗試對IP地址(172.16.0.8)進行身份驗證測試(超時:12秒) 資訊:身份驗證成功

附註:請勿透過Flex-config修改**tunnel-group ppp-attributes**,因為這對透過RADIUS為 AnyConnect VPN(SSL和IPSec)連線交涉的驗證通訊協定沒有影響。

tunnel-group RA_VPN ppp-attributes no authentication pap 驗證chap

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在FTD:

• debug radius all 在ISE上:

• RADIUS即時日誌