Configurar VPN de acesso remoto FTD com MSCHAPv2 sobre RADIUS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Diagrama de Rede Configurar a VPN RA com autenticação AAA/RADIUS via FMC Configurar o ISE para suportar MS-CHAPv2 como protocolo de autenticação Verificar Troubleshoot

Introduction

Este documento descreve como habilitar o Microsoft Challenge Handshake Authentication Protocol versão 2 (MS-CHAPv2) como o método de autenticação via Firepower Management Center (FMC) para clientes VPN de acesso remoto com autenticação RADIUS (Remote Authentication Dial-In User Service).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Identity services engine (ISE)
- Cisco AnyConnect Secure Mobility Client
- protocolo RADIUS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Por padrão, o FTD usa o PAP (Password Authentication Protocol) como o método de autenticação com servidores RADIUS para conexões VPN do AnyConnect.

O PAP fornece um método simples para que os usuários estabeleçam sua identidade com um handshake duplo. A senha PAP é criptografada com um segredo compartilhado e é o protocolo de autenticação menos sofisticado. O PAP não é um método de autenticação forte porque oferece pouca proteção contra ataques repetidos de tentativa e erro.

A autenticação MS-CHAPv2 introduz a autenticação mútua entre pares e um recurso de alteração de senha.

Para habilitar o MS-CHAPv2 como o protocolo usado entre o ASA e o servidor RADIUS para uma conexão VPN, o gerenciamento de senha deve ser habilitado no Perfil de conexão. A habilitação do gerenciamento de senha gera uma solicitação de autenticação MS-CHAPv2 do FTD para o servidor RADIUS.

Configurar

Diagrama de Rede



Configurar a VPN RA com autenticação AAA/RADIUS via FMC

Para um procedimento passo a passo, consulte este documento e este vídeo:

<u>Configuração de VPN de acesso remoto do AnyConnect no FTD</u>

<u>Configuração inicial do AnyConnect para o FTD gerenciado pela FMC</u>

Etapa 1. Depois que a VPN de acesso remoto estiver configurada, navegue para **Dispositivos > Acesso remoto**, edite o perfil de conexão recém-criado e navegue até a guia **AAA**.

Firepower Management Center Overview Analysis P	Policies Devices Objects AMP	Intelligence	Deploy 🔍 💕 🖏 🔕 admin •
RA_VPN			Sive Cancel
Enter Description			
			Policy Assignments.(1)
Connection Profile Access Interfaces Advanced			Local Realm: None Dynamic Access Policy: None
		Edit Connection Profile 0	+
Name	АЛА	Connection Profile:* RA_VPN	
DefaultWEBVPNOroup	Authentication: None Authorization: None Accounting: None	Group Policy.* DthOrpPolicy + +	∕≆
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 Accounting Server:	
		Advanced Settings	
		Cancel Seve	

Expanda a seção **Configurações avançadas** e clique na caixa de seleção **Habilitar gerenciamento de senha**. Click **Save**.

Firepower Management Center Overview Analysis Devices / VPN / Edit Connection Profile	Policies Devices Objects AMP	Intelligence	Deploy Q. 🧬 🗘 😝 admin
RA_VPN			Save Cancel
Enter Description Connection Profile Access Interfaces Advanced			Policy Associated (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.* DthOrpPolicy + +	/1
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	Eff Grue Paley 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	
		Accounting Server:	
		Advanced Settings Stein Readministration	
		Strip Group from username	
		C Enable Password Management	
		Notify User 14 days prior to password expiration	
		Notify user on the day of password expiration	
		v	
		Cancel	

Salvar e implantar.

cisco Devices / VPN / Edit Connection Profile Overview Analysis Po	olicies Devices Objects AMP Intelligence		Deploy 🔍 🧬 🗘 😝 admin 🔹
RA_VPN		You have	e unsaved changes Save Cancel
Enter Description			Policy Assignments (1)
		Local Realm: None	Dynamic Access Policy: None
Connection Profile Access Interfaces Advanced			
			+
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authentication: None Accounting: None	B DROrpPolicy	/1
RA_VPN	Authoritation: ISE_Server (RADIUS) Authoritation: ISE_Server (RADIUS) Accounting: Income	B DROpPolicy	/1
TOTAL TOTAL	Accounting: None	Le number out	/•

A configuração de VPN de acesso remoto na CLI FTD é:

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

Configurar o ISE para suportar MS-CHAPv2 como protocolo de autenticação

Pressupõe-se que:

- 1. O FTD já foi adicionado como um dispositivo de rede no ISE para poder processar solicitações de acesso RADIUS do FTD.
- 2. Há pelo menos um usuário disponível para o ISE autenticar o cliente AnyConnect.

Etapa 2. Navegue até **Policy > Policy Sets** e encontre a política **Allowed Protocols** anexada ao conjunto de políticas onde seus usuários do AnyConnect são autenticados. Neste exemplo, apenas um Conjunto de políticas está presente, de modo que a política em questão é o *Acesso de rede padrão*.



Etapa 3. Navegue até **Política > Elementos de política > Resultados.** Em **Authentication > Allowed Protocols** escolha e edite **Default Network Access**.

Identity Services Engine Home + Context Visibility + Operation	ns Policy + Administration + Work Centers	Lowne Warring 📥 🧐 🧔 🔘
Policy Sets Profiling Posture Client Provisioning + Policy Elements	Policy Sets Profiling	
	Posture Client Provisioning	
Policy Sets	Policy Elements	Reset Policysel Hitcounts Reset Sare
Status Policy Set Name Description	Conditions Ensuits	Allowed Protocols / Server Sequence Hits Actions View
Search		
		+
Default Default policy set		Default Network Access + + 24 O >



Verifique se a caixa de seleção Permitir MS-CHAPv2 está marcada. Desça até o fim e salve-o.



Verificar

Navegue até sua máquina cliente onde o cliente Cisco AnyConnect Secure Mobility está instalado. Conecte-se ao headend FTD (uma máquina Windows é usada neste exemplo) e digite as credenciais do usuário.

🕥 Cisco AnyC	connect Secure Mobility Client	1000		\times
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:33			IF	v4
\$ (i)			-	ili.ili. cisco

Os registros ao vivo RADIUS no ISE mostram:

aint Profile

tion Protocol

NAS IPv4 Address 0.0.0.0

Endpoint la Calling Station Id 192.108.0.101 Windows10-Work

> Ry Store Internal Users Workstation 0480054000 MSCHAPV2

DRIVERAP_FTD_7.0 All Device Types All Locations

CI VICIV		
ivent	5200 Authentication succeeded	
Isemame	usert	
Endpoint Id	00.50.55.55.45.6F B	
Indpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Statio IP Address User 1	
uthorization Result	Statio/PaddressUser1	
uthorization Result	StatidPaddeelJae1	
utherization Result thentication Details fource Timestamp	StatidPaddwsJber1	
thentication Result	StatidPadews/ber1 2021-05-28.00.06.02.94 2021-05-28.00.06.02.94	
uthorization Result thentication Details iource Timestamp teceived Timestamp 'olicy Server	StatidPadews/her1 2021-09-26 00:00:2:94 2021-09-28 00:00:2:94 dviewsp-158-2:7	
thentication Result thentication Details fource Timestamp leceived Timestamp valicy Server tvent	StatisPadewsCkwr1 2021-08-28 00 06 02 04 2021-08-28 00 06 02 04 driwwar180-27 2020 Authentiation kuoseded	
thentication Result thentication Details fource Timestamp leceived Timestamp valicy Server tvent formation	StatisPadewolker1 2021-09-28-00-06-02-04 2021-09-28-00-06-02-04 2021-09-28-00-06-02-04 downey-058-27 2020 Authentiation successed use1	

Steps

- Stepp

 1001 Restrict RADUS AssessRepuet

 1001 Restrict RADUS AssessRepuet

 1004 Exclusion Priling Oxio
 Exclusion Beine Selection Fields

 1004 Exclusion Selector Fields

 1004 Exclusion Selector Field

 1004 Exclusion Selector Field

 1004 Exclusion Selector Field

 1004 Exclusion Selector Field

 1005 Selector Selector Source Internat Like College1005 Selector Selector Source Internative

 1005 Selector Selector Source Internative

 1005 Selector Selector Field

 1004 Exclusion Field

 1004 Exclusion

- 2027 Adventisation Pased 2017 Adventisation Pased 2017s (El Exa no commend locally previous uscassful / 2018) Evaluation for usa Adventisation Pallo 2020 Localing up Endoport in Internat Endoportin Oblance 2021 Found Endoportin In Internat Endoportin Solare 2021 Found Endoportin In Internat Endoportin Solare 2021 Round Endoportin In Internat Endoportin Solare 2021 Read Endoportin In Internat Endoportin Solare 2021 Read Endoporting International Endoporting 2020 Read Read Pallong Solarity Commendation Commendation 2020 Read Read Pallong Solarity Commendation Commendation 2020 Read Read Pallong Solarity Commendation Commendation 2020 Read Pallong Solarity Commendation 2020 Read Pallong Sol

2	Identity Services Engine	
	NAS Port Type	litual
	Authorization Profile	Ita5idPaddressUser1
	Response Time	131 milliseconds
	Other Attributes	
	ConfigWersionId	147
	DestinationPort	1812
	Protocol	Radius
	NAS-Port	57344
	Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
	MS-CHAP-Challenge	01.41:04.11.45.b1.41.5b.4d.b5.97.1b.b7.fe.e8.c8
	MS-CHAP2-Response	00 00 65 da 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
	CVPH2000/ASA/PIX7x-Tunnel- Group Name	RA_VPN
	NetworkDeviceProfileId	b0099505-3150-4215-a00e-0753645b/50c
	IsThirdPartyDeviceFlow	false
	CVPN3000/ASA/PIX7x-Client-Type	2
	AcsSessionID	driverap-15E-2-7/417494978/25
	SelectedAuthenticationIdentityStores	Internal Users
	SelectedAuthenticationIdentityStores	All_AD_Join_Points
	SelectedAuthenticationIdentityStores	Guest Users
	Authentication Status	AuthenticationPassed
	IdentityPolicyMatchedRule	Default
	AuthorizationPolicyMatchedRule	Static IP Address User 1
	1SEPolicySettlame	Default
	Identity SelectionMatchedRule	Default
	D7LSSupport	Unknown
	HostidentityGroup	Endpoint Identity Groups Profiled Workstation
	Network Device Profile	Cisco

-	
cisco-av-pair	profile-name+Windows10-Workstation
Class	CACS dba800540000a00081525o49 driverap-ISE-2-7/417494978/25
Framed-IP-Address	10.0.50.101
esult	
CiscoAVPair	Inder-Understandung globan 1993 BBROOF DES VIZOOE 243 14667 484.42.0422068.) under State 2017 1976 1272 1976 12.042 118.4408598 C717E 370388 C000P 44.4402 6830 544. subtransio-Inder 24.000 40006 2000 1525 48. (solar subtransio-Inder 24.000 40.0000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.000 40.0000 40.000 40.0000 40.000 40.000 40.000 40.000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.0000 40.00000 40.0000 40.0000 40.0000 40.0000400 40.0000 40
	mdm-til-mdw/da-platform=uin, mdm-til-mdw/da-platform=uin, mdm-til-mdwraia-publionaeu mdm-til-maine-publionaeu mdm-til-ma-suae-agent-AnyConneat Windows 4.10.2028s, mdm-til-maine-to-to-to-to-to-to-to-to-to-to-to-to-to-
Called-Station-ID	192.168.0.100
CPMSessionID	c0a800640000a00061525o49
Device IP Address	192.108.0.100
RADIUS Username	user1
EnableFlag	Evabled
oevice type	Unite types being types
Device Type	Device Type#All Device Types IPSEC#Is IPSEC Device#No

Observação: o comando test aaa-server authentication sempre usa PAP para enviar

solicitações de autenticação ao servidor RADIUS, não há como forçar o firewall a usar MS-CHAPv2 com esse comando.

firepower# test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXX INFORMAÇÕES: Tentando testar a autenticação para o endereço IP (172.16.0.8) (tempo limite: 12 segundos) INFORMAÇÕES: Autenticação Bem-Sucedida

Note: Não modifique os **atributos ppp de grupo de túnel** via Flex-config, pois isso não afeta os Protocolos de autenticação negociados sobre RADIUS para conexões VPN (SSL e IPSec) do AnyConnect.

tunnel-group RA_VPN ppp-attribute no authentication pap chap de autenticação authentication ms-chap-v1 no authentication ms-chap-v2 no authentication eap-proxy

Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

Em FTD:

• debug radius all No ISE:

• Registros ao vivo RADIUS