

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.

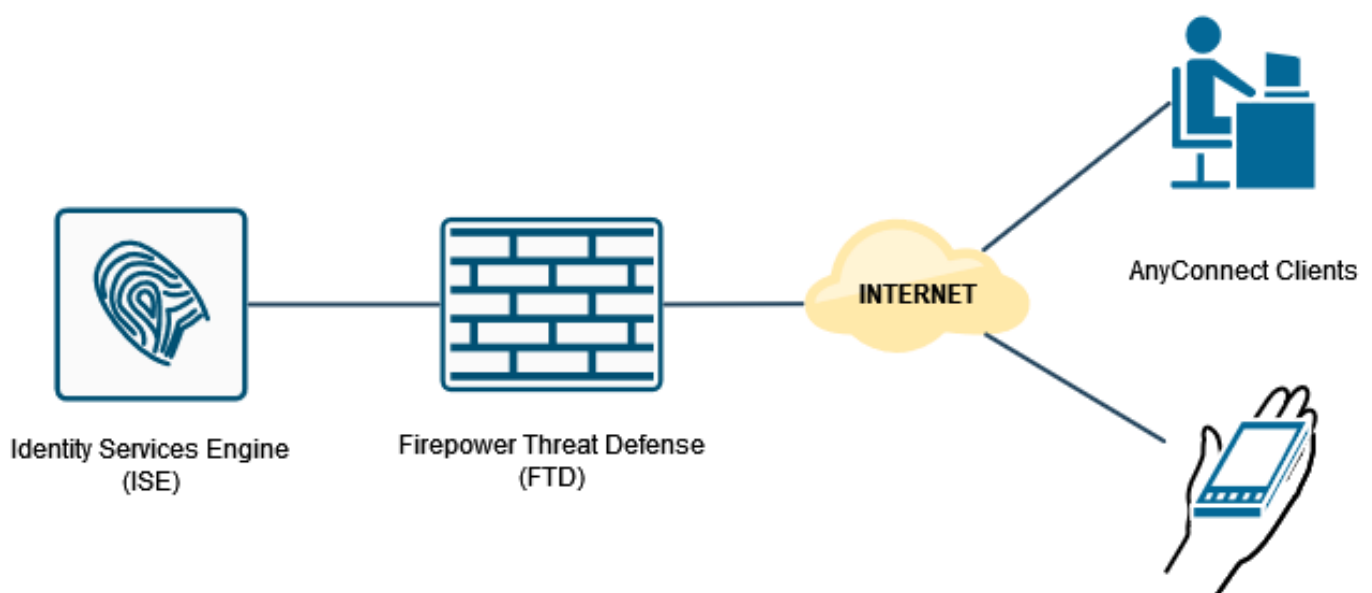
O PAP fornece um método simples para que os usuários estabeleçam sua identidade com um handshake duplo. A senha PAP é criptografada com um segredo compartilhado e é o protocolo de autenticação menos sofisticado. O PAP não é um método de autenticação forte porque oferece pouca proteção contra ataques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



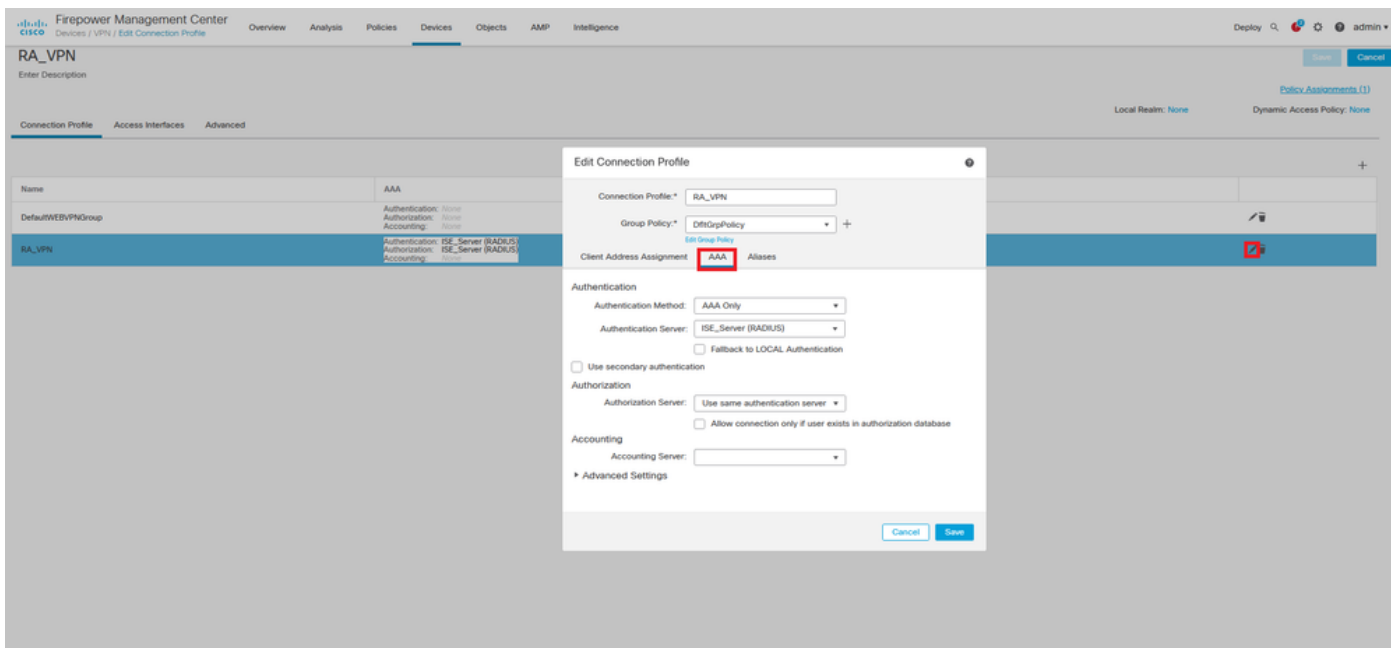
Configurar a VPN RA com autenticação AAA/RADIUS via FMC

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

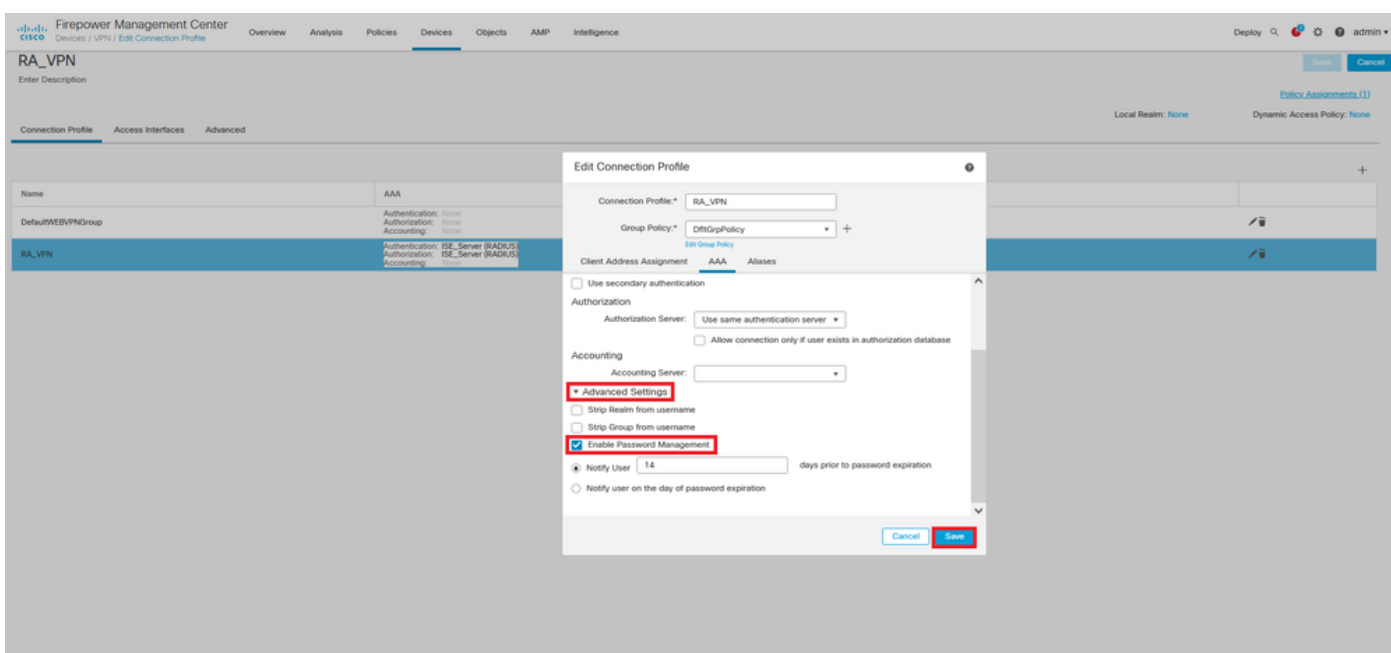
- [Configuração de VPN de acesso remoto do AnyConnect no FTD](#)

- [Configuração inicial do AnyConnect para o FTD gerenciado pela FMC](#)

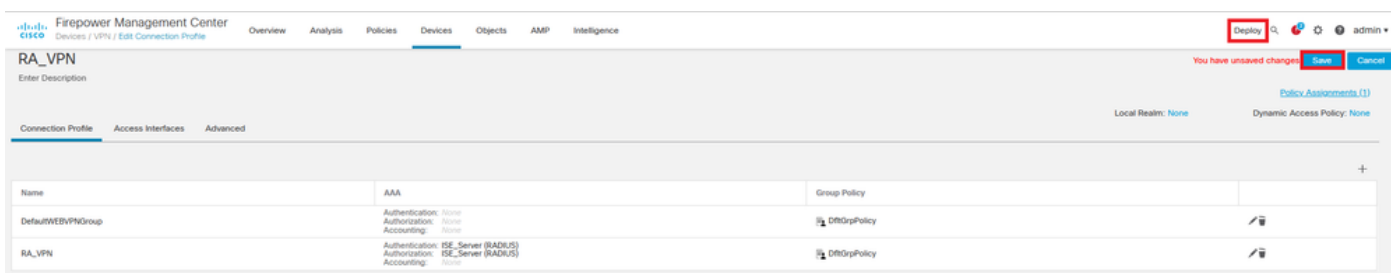
Etapa 1. Depois que a VPN de acesso remoto estiver configurada, navegue para **Dispositivos > Acesso remoto**, edite o perfil de conexão recém-criado e navegue até a guia **AAA**.



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



Salvar e implantar.



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
```

password-management

tunnel-group RA_VPN webvpn-attributes

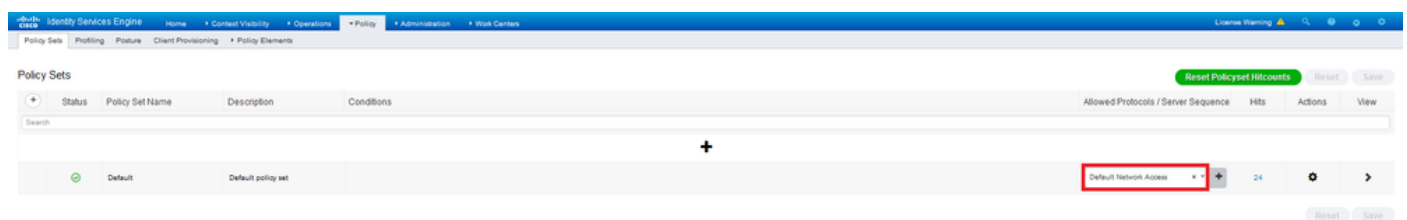
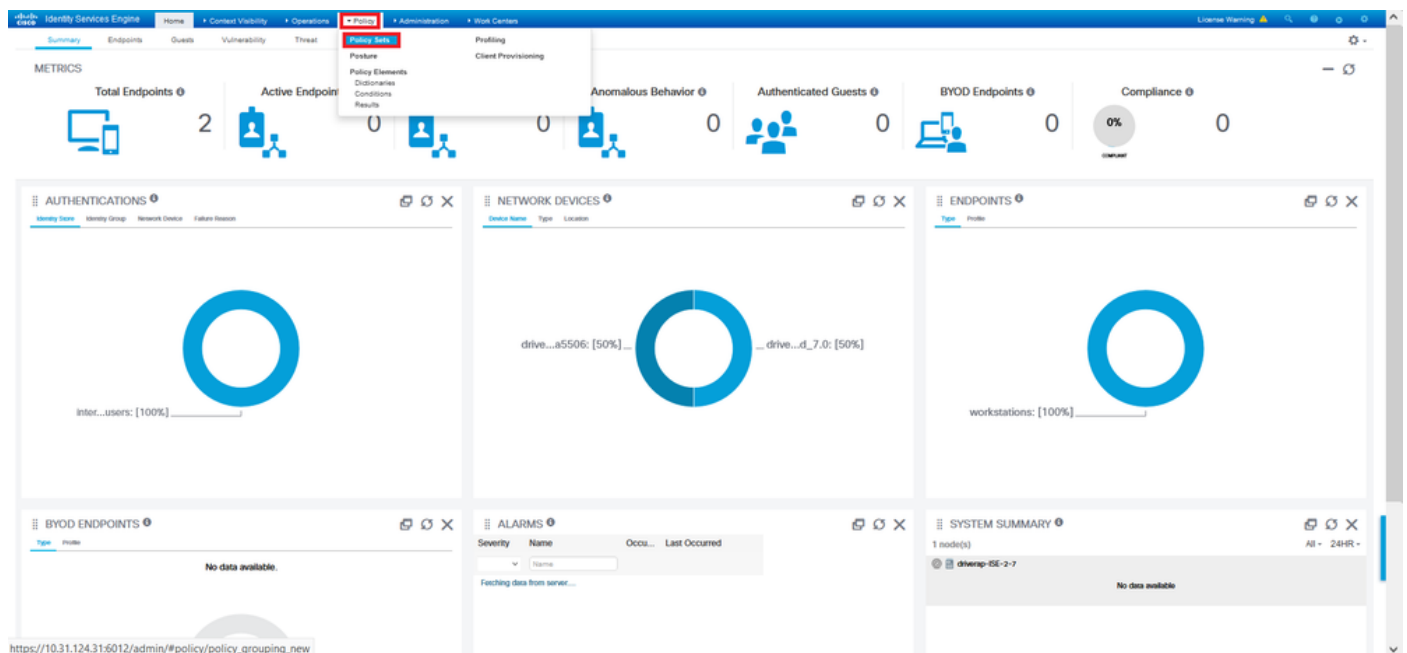
group-alias RA_VPN enable

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

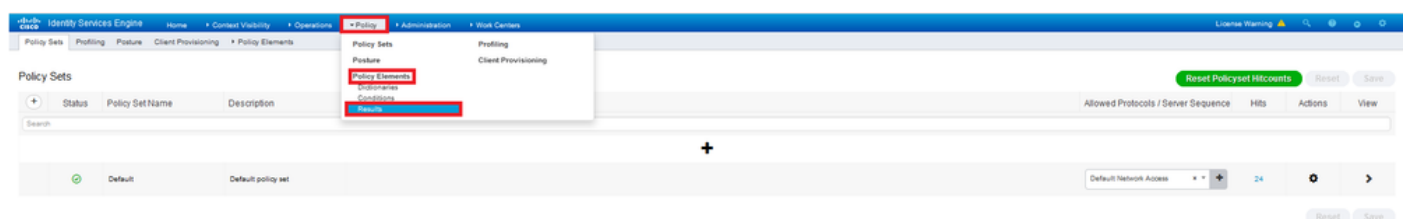
Pressupõe-se que:

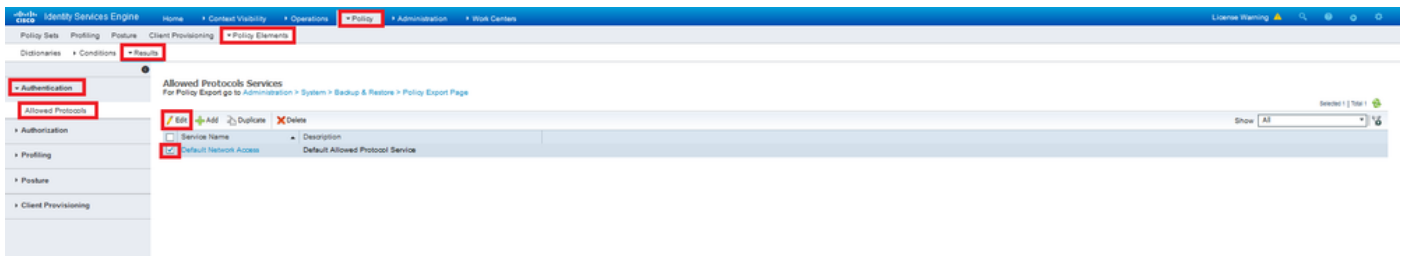
1. O FTD já foi adicionado como um dispositivo de rede no ISE para poder processar solicitações de acesso RADIUS do FTD.
2. Há pelo menos um usuário disponível para o ISE autenticar o cliente AnyConnect.

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*.

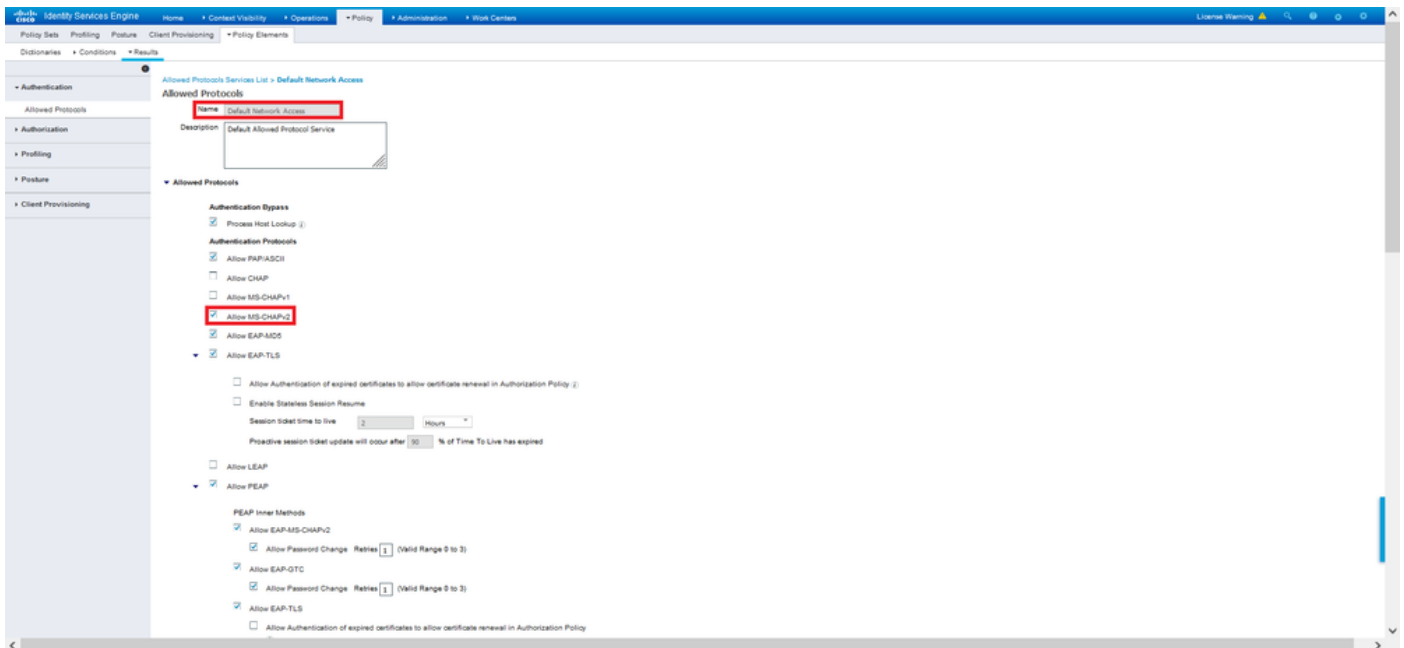


Etapa 3. Navegue até **Política > Elementos de política > Resultados**. Em **Authentication > Allowed Protocols** escolha e edite **Default Network Access**.



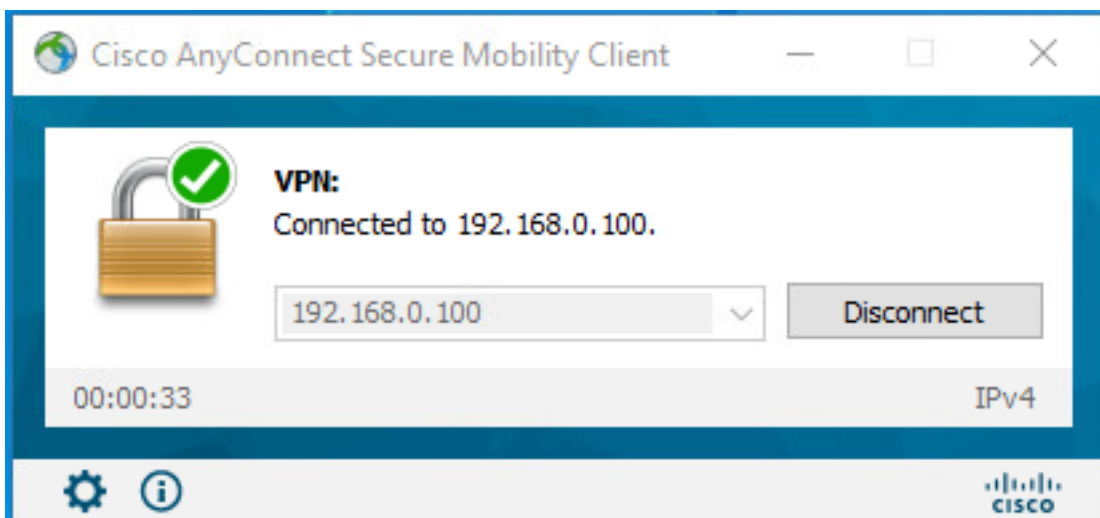


Verifique se a caixa de seleção **Permitir MS-CHAPv2** está marcada. Desça até o fim e **salve-o**.



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.



Os registros ao vivo RADIUS no ISE mostram:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00 50 50 90 40 0F 0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15058 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15043 Queried PIP - Normalised RADIUS Radius/ForType (4 times)
- 22072 Selected Identity source sequence - All_User_ID_Stores
- 15019 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - user1
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 24719 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore - user1
- 24211 Found Endpoint in Internal Endpoints IDStore
- 15043 Queried PIP - RADIUS User-Name
- 15018 Selected Authorization Profile - StaticIPAddressUser1
- 22081 Max session policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Authentication Details

Source Timestamp	2021-09-28 00:06:02.94
Received Timestamp	2021-09-28 00:06:02.94
Policy Server	drivrap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00 50 50 90 40 0F 0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	d8a30054000a000e1225a49
Authentication Method	MSCHAPV2
Authentication Protocol	MSCHAPV2
Network Device	DRIVERAP_JTD_7-0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

Identity Services Engine

Other Attributes

ConfigVersionId	147
DestinationPort	1812
Protocol	Radius
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
MS-CHAP-Challenge	0F 4F54 9F 45 0F 4F 50 42 50 97 19 57 5E A8 08
MS-CHAP2-Response	00 00 00 00 00 20 04 45 8 12 07 8a 20 20 a1 19 45 a0 00 00 00 00 00 00 00 00 05 4f 29 52 90 5a 2ca1 d9 a7 50 3c f0 8a 73 32 a9 50 54 27 00 5a 99
CVPR3000ASAPROTA Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	b0099005-3150-4215-a80a-d753a45b850a
IsThirdPartyDeviceFlow	false
CVPR3000ASAPROTA Client-Type	2
AcxSessionId	drivrap-ISE-2-7-1417494978-25
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLS Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco

Result

Framed IP Address	10.0.50.101
Class	CACS-d8a30054000a000e1225a49 drivrap-ISE-2-7-1417494978-25
class-av-pair	profile-name=Windows10-Workstation
MS-CHAP2-Success	00 53 3a 33 30 33 40 33 30 37 38 34 42 43 45 32 33 45 41 31 39 37 37 32 44 48 39 39 38 44 41 39 37 31 38 44 38 41 43 48 43 41
LicenseTypes	Basic license consumed

Session Events

NAS Port Type	Virtual
Authorization Profile	StaticIPAddressUser1
Response Time	231 milliseconds

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 XXXXXX
```

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