Configurar VPN de acesso remoto FTD com MSCHAPv2 sobre RADIUS

Contents

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.

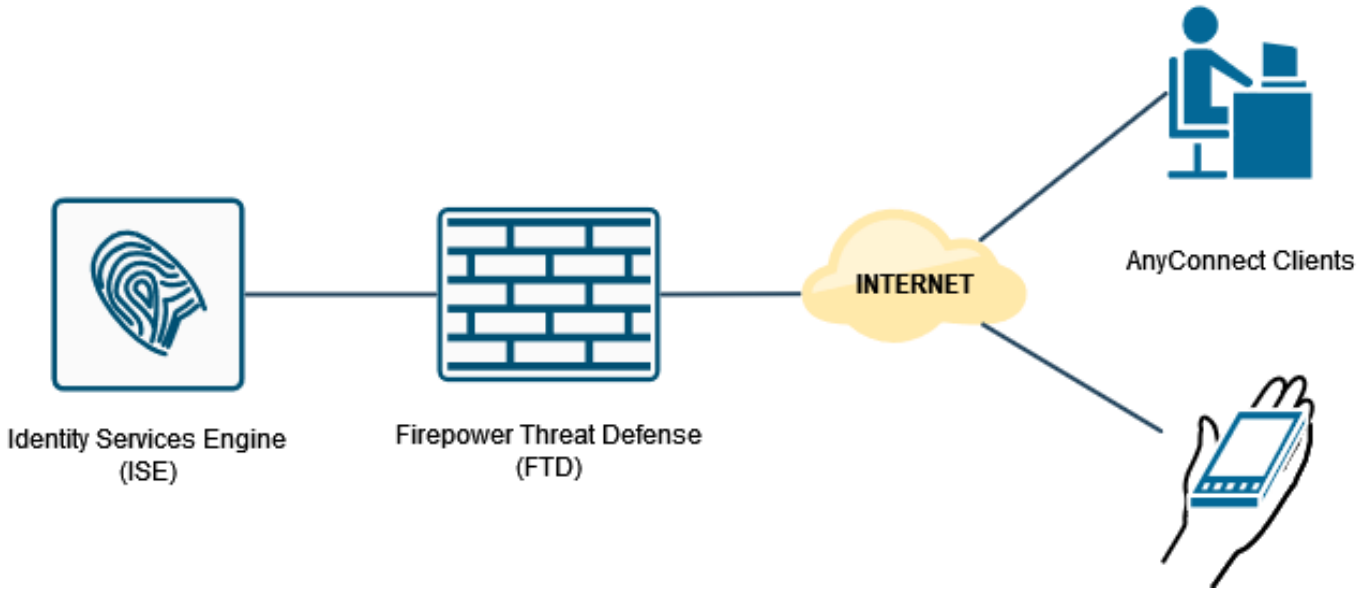
O PAP fornece um método simples para que os usuários estabeleçam sua identidade com um handshake duplo. A senha PAP é criptografada com um segredo compartilhado e é o protocolo de autenticação menos sofisticado. O PAP não é um método de autenticação forte porque oferece pouca proteção contra ataques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



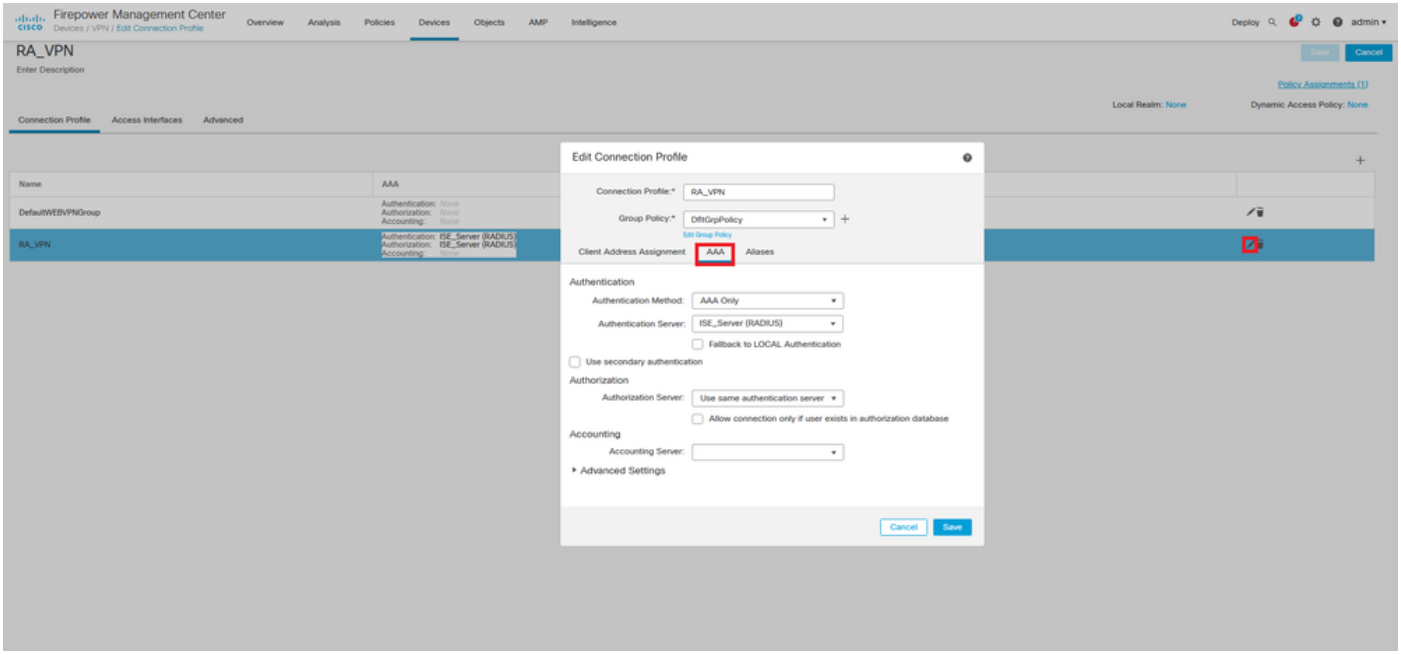
Configurar a VPN RA com autenticação AAA/RADIUS via FMC

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

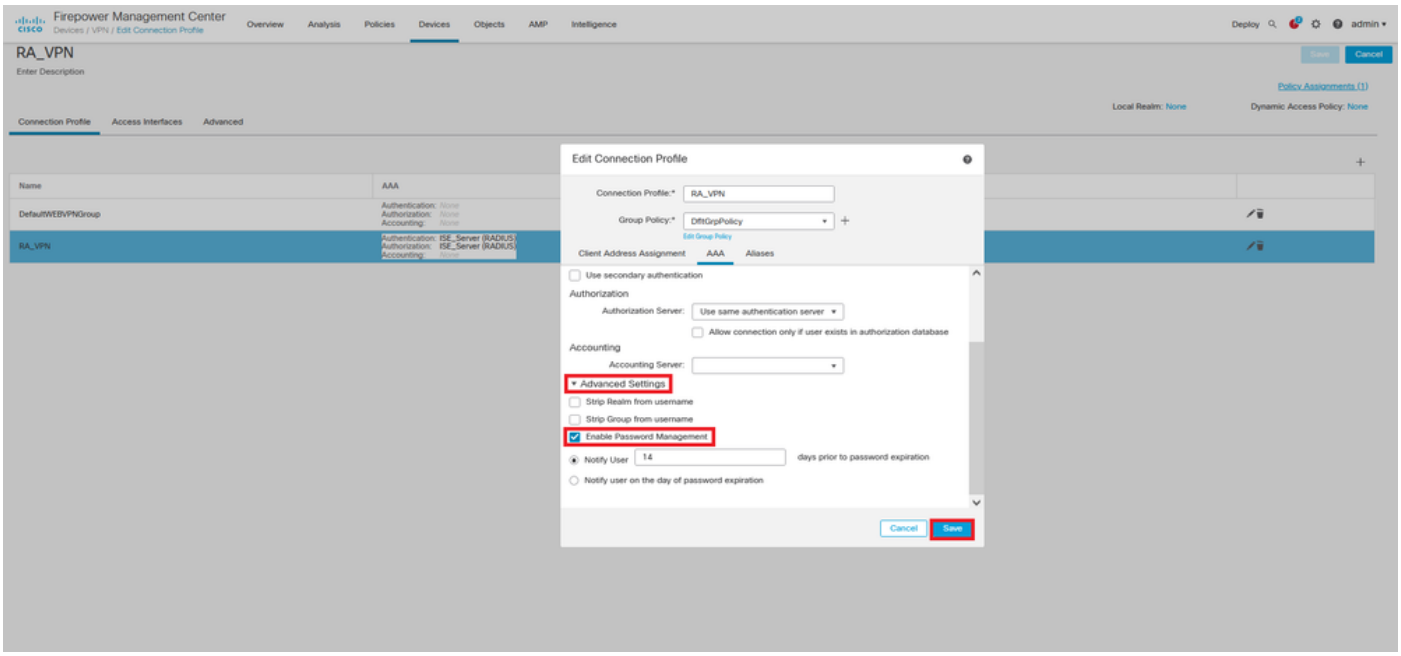
- Configuração de VPN de acesso remoto do AnyConnect no FTD

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

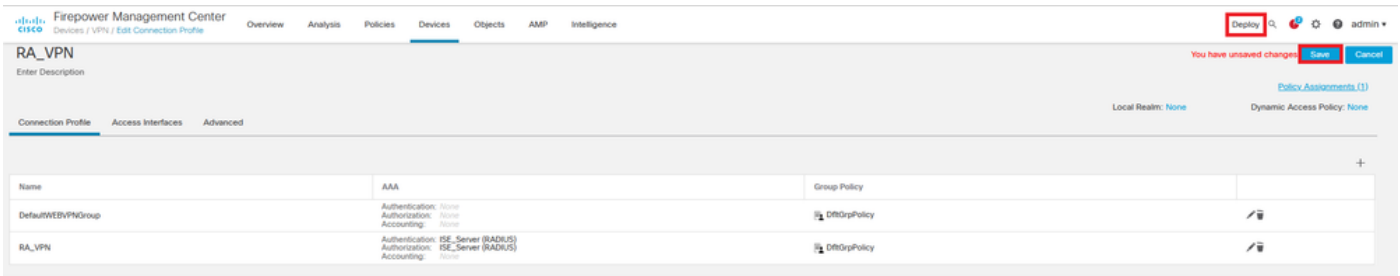
Etapa 1. Depois que a VPN de acesso remoto estiver configurada, navegue para **Dispositivos > Acesso remoto**, edite o perfil de conexão recém-criado e navegue até a guia **AAA**.



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
```

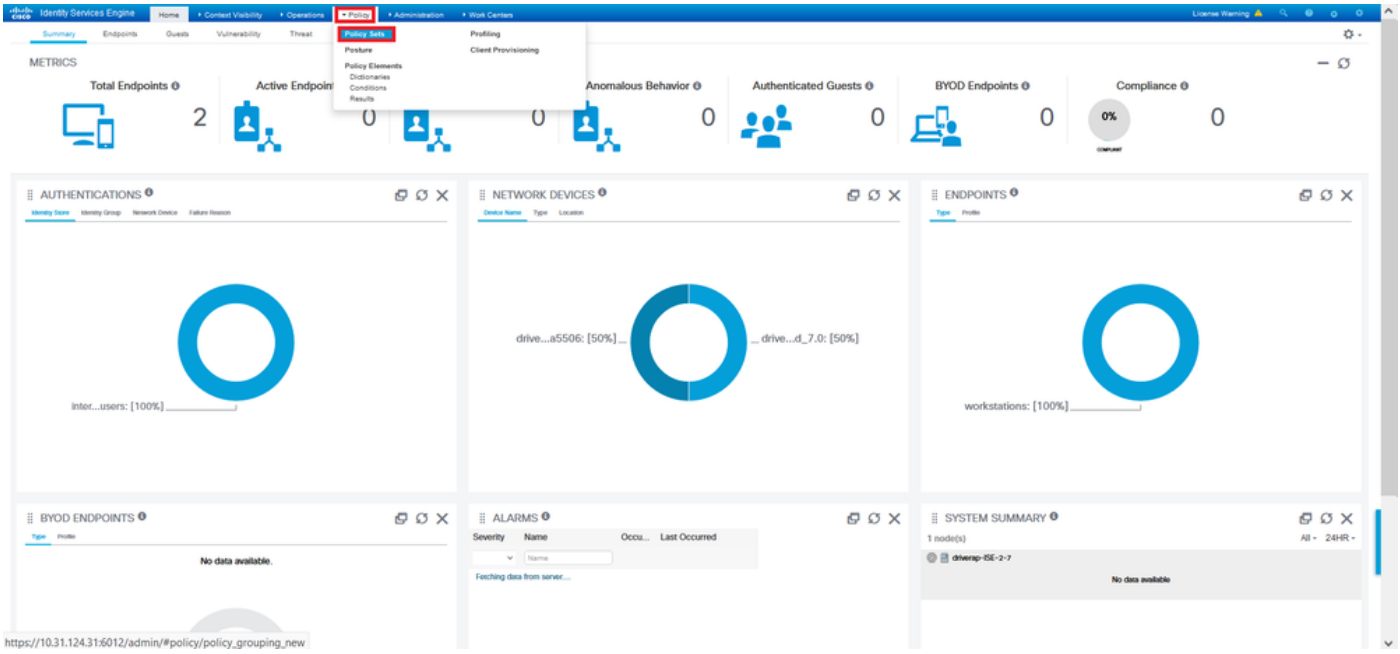
```
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

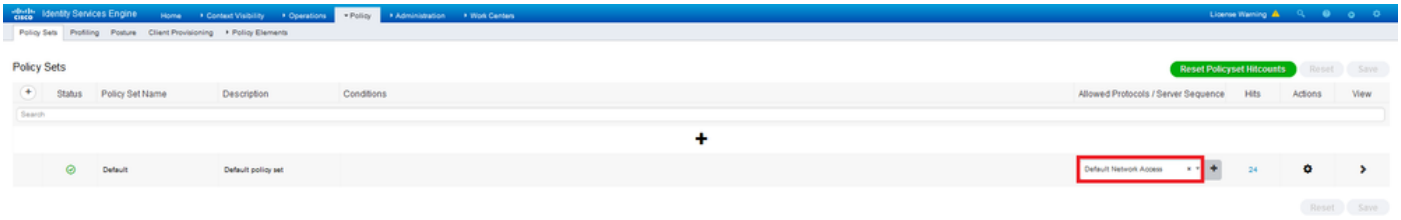
Configurar o ISE para suportar MS-CHAPv2 como protocolo de autenticação

Pressupõe-se que:

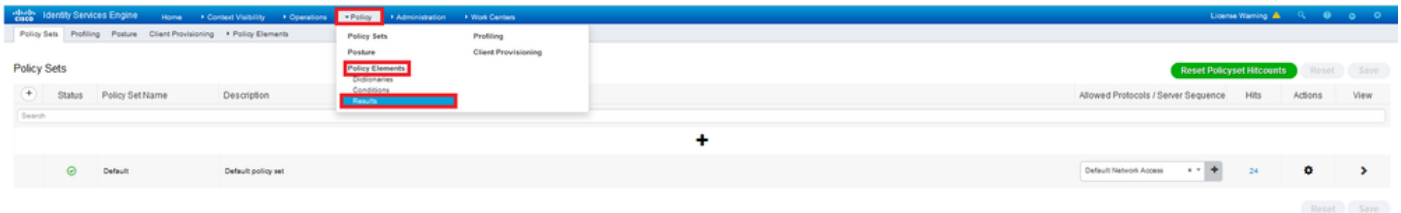
1. O FTD já foi adicionado como um dispositivo de rede no ISE para poder processar solicitações de acesso RADIUS do FTD.
2. Há pelo menos um usuário disponível para o ISE autenticar o cliente AnyConnect.

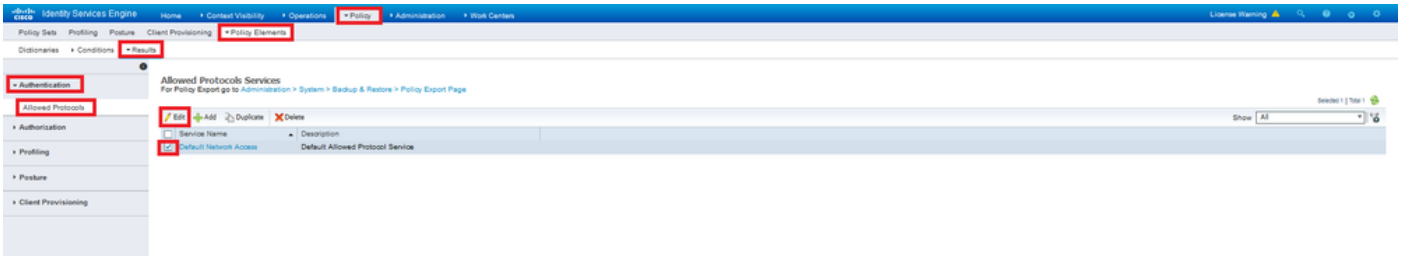
Etapa 2. Navegue até **Policy > Policy Sets** e encontre a política **Allowed Protocols** anexada ao conjunto de políticas onde seus usuários do AnyConnect são autenticados. Neste exemplo, apenas um Conjunto de políticas está presente, de modo que a política em questão é o *Acesso de rede padrão*.



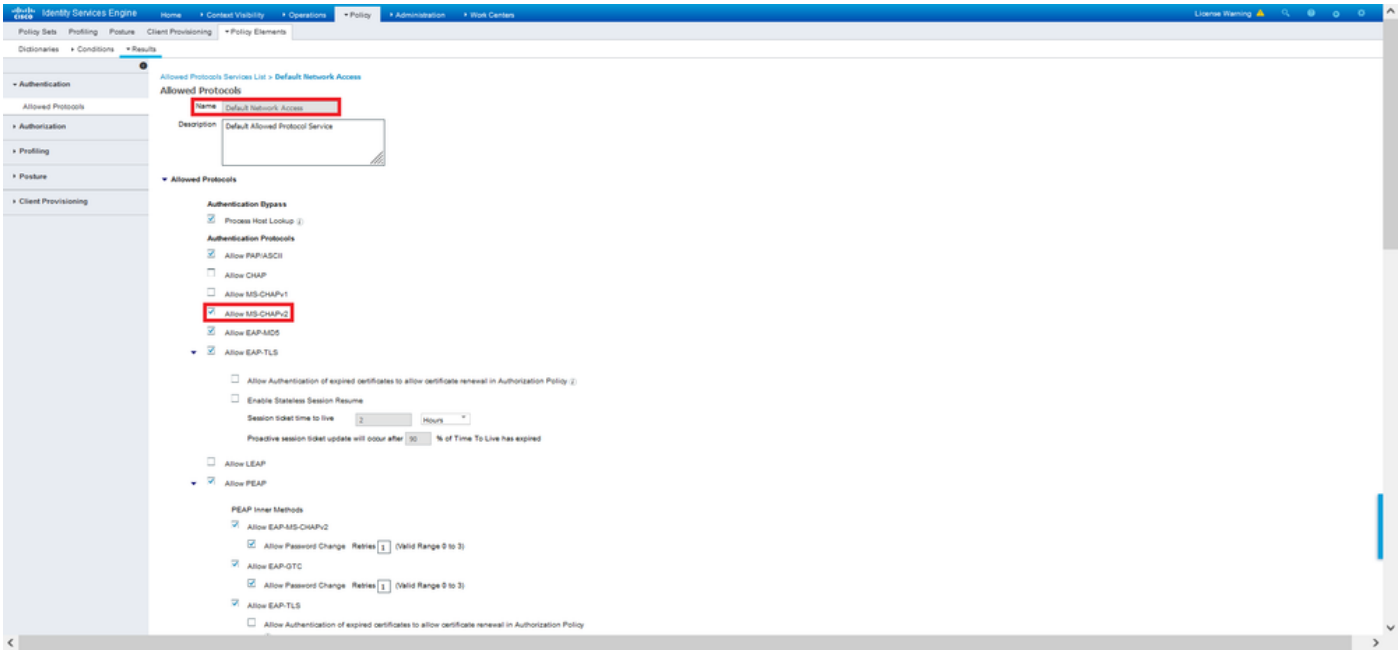


Etapa 3. Navegue até **Política > Elementos de política > Resultados.** Em **Authentication > Allowed Protocols** escolha e edite **Default Network Access**.



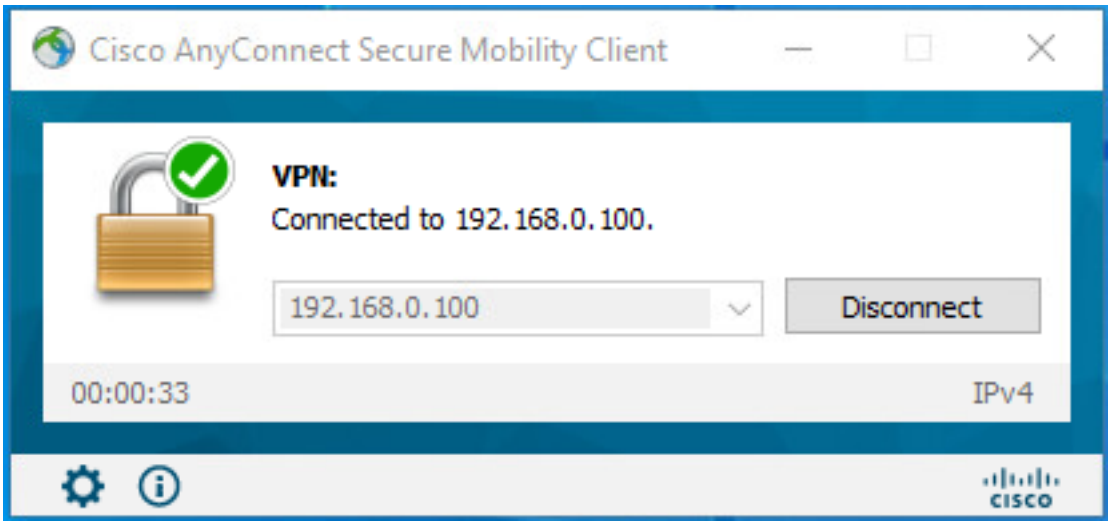


Verifique se a caixa de seleção **Permitir MS-CHAPv2** está marcada. Desça até o fim e **salve**-o.

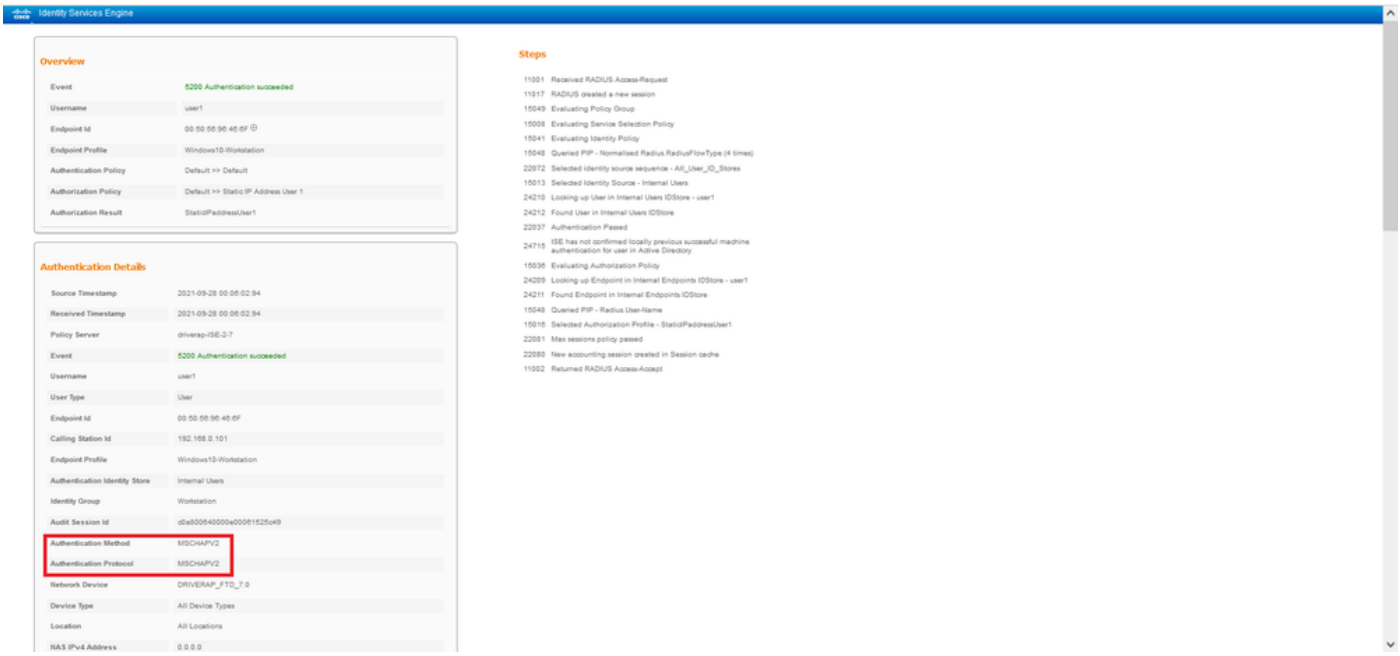


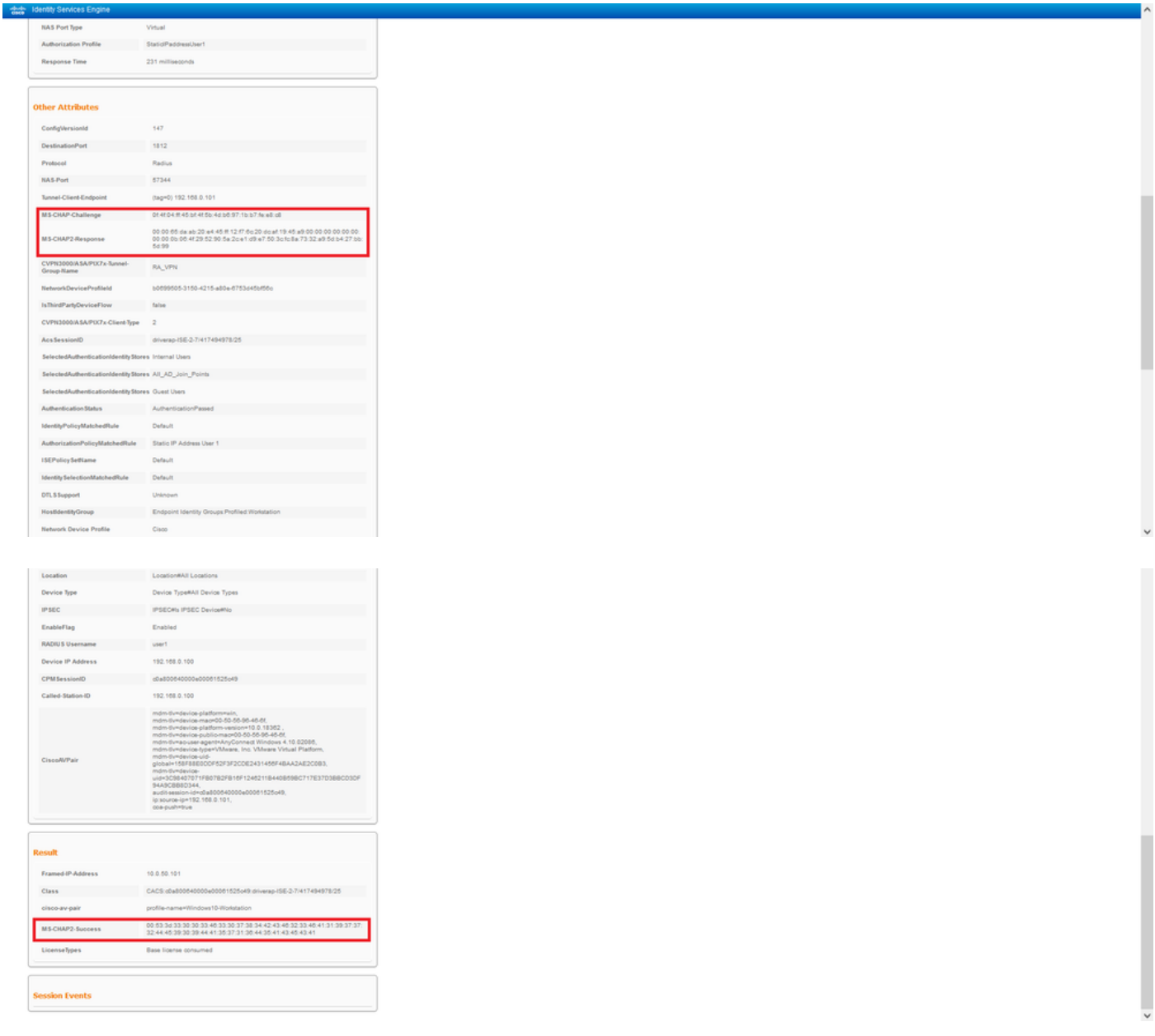
Verificar

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:





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