

Configurar a atribuição de endereço IP estático para usuários do AnyConnect via autorização RADIUS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar a VPN de acesso remoto com autenticação AAA/RADIUS via FMC](#)

[Configurar a política de autorização no ISE \(servidor RADIUS\)](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar a autorização RADIUS com um servidor Identity Services Engine (ISE) para que ele sempre encaminhe o mesmo endereço IP para o Firepower Threat Defense (FTD) para um usuário específico do Cisco AnyConnect Secure Mobility Client via RADIUS Attribute 8 Framed-IP-Address.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect Secure Mobility Client
- protocolo RADIUS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

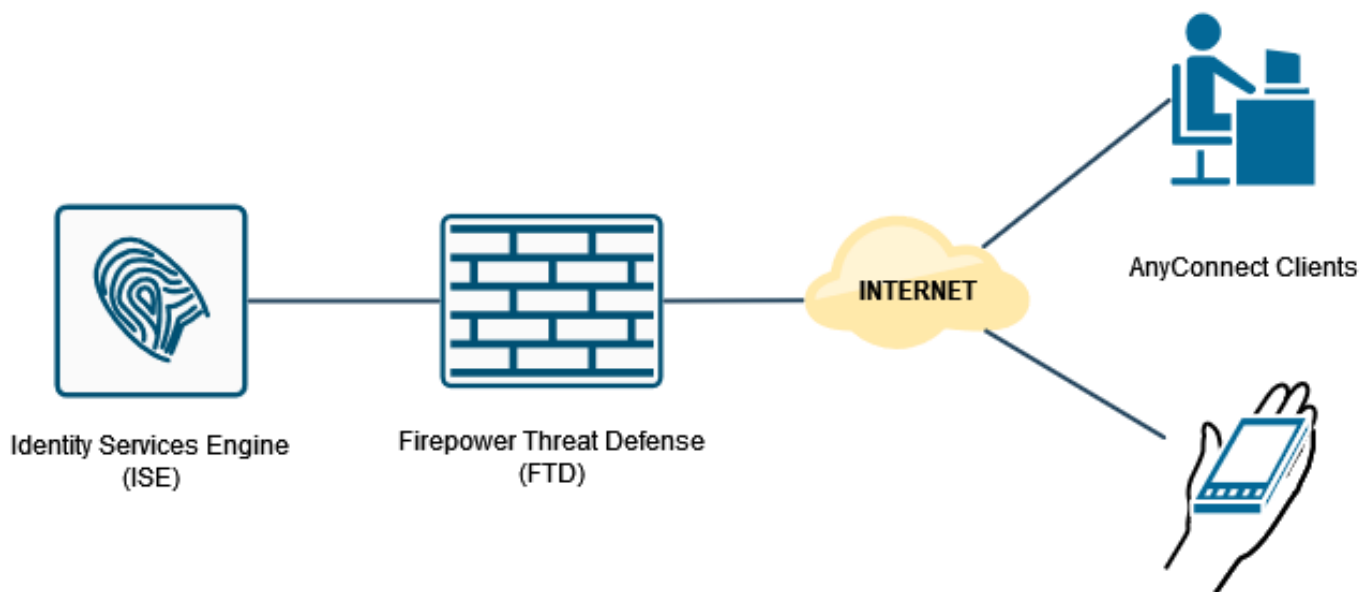
- FMCv - 7.0.0 (build 94)
- FTDv - 7.0.0 (Build 94)
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086

- 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.

Configurar

Diagrama de Rede



Configurar a VPN de acesso remoto 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](#)

A configuração de VPN de acesso remoto na CLI do 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

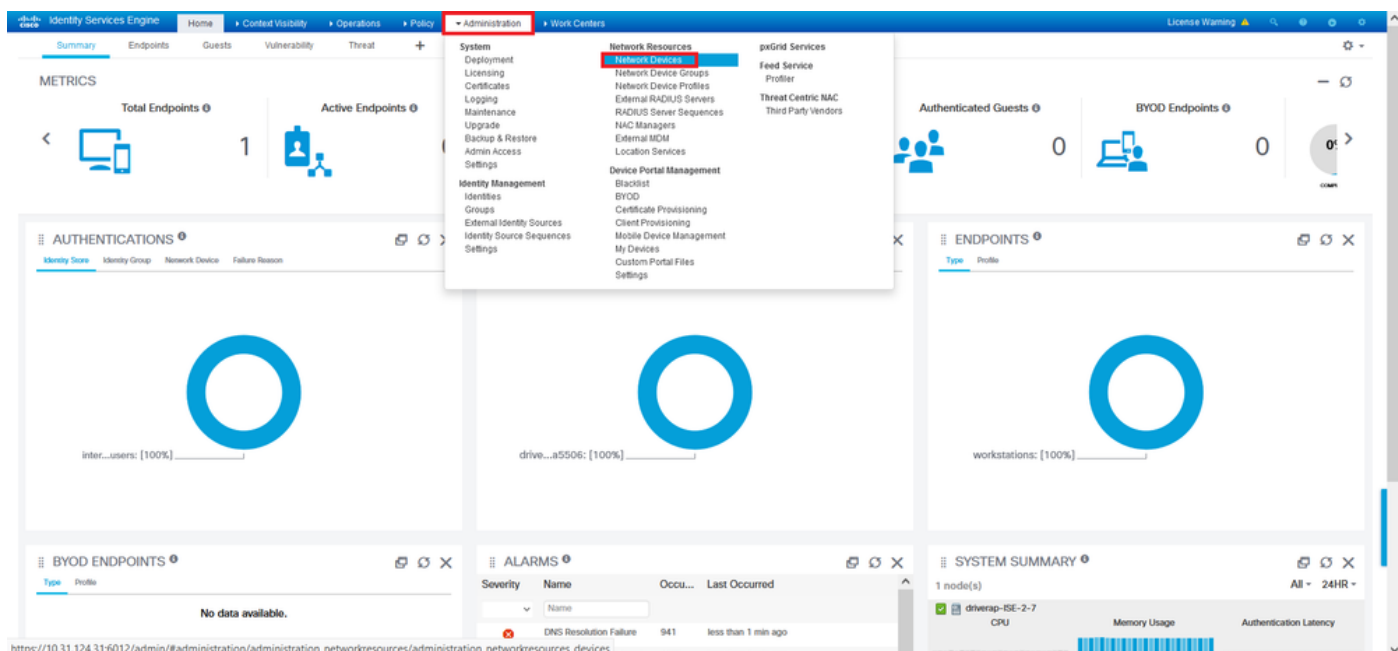
authentication-server-group ISE_Server

tunnel-group RA_VPN webvpn-attributes

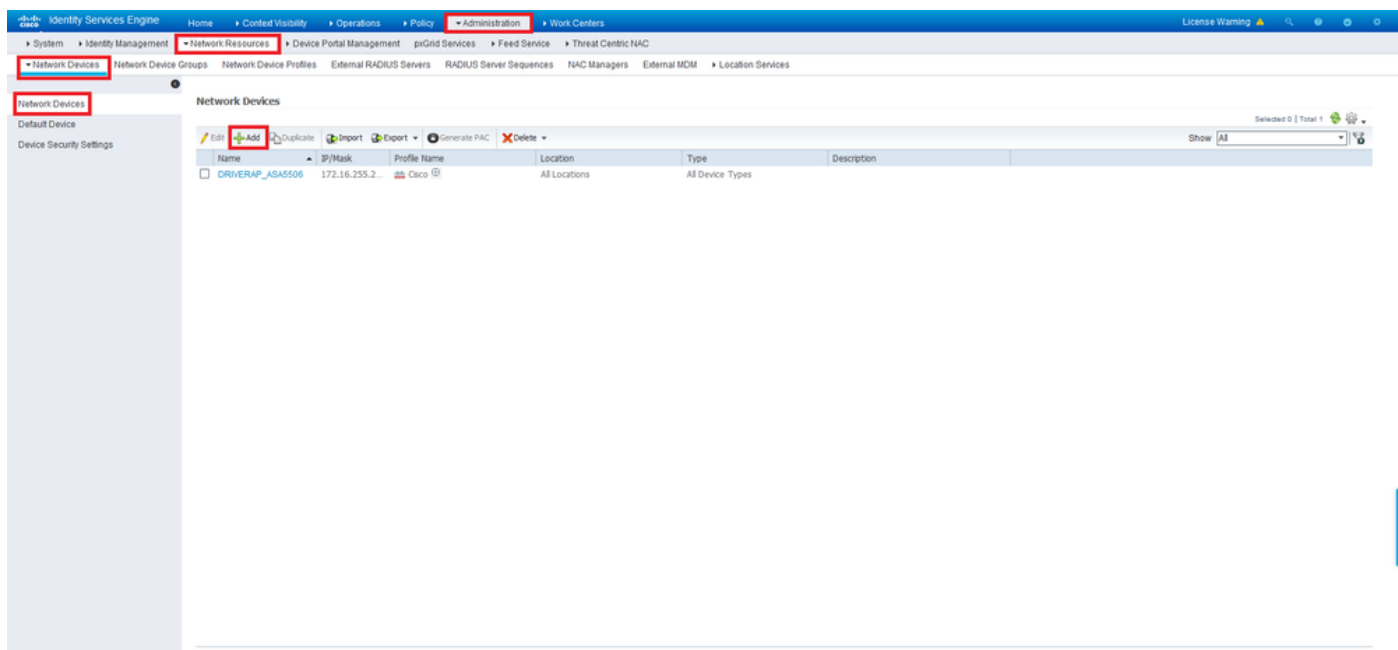
group-alias RA_VPN enable

Configurar a política de autorização no ISE (servidor RADIUS)

Etapa 1. Faça login no servidor ISE e navegue para **Administration > Network Resources > Network Devices**.



Etapa 2. Na seção Network Devices (Dispositivos de rede), clique em **Add** para que o ISE possa processar solicitações de acesso RADIUS do FTD.



Insira os campos **Nome** do dispositivo de rede e **Endereço IP** e marque a caixa **Configurações de autenticação RADIUS**. O **segredo compartilhado** deve ser o mesmo valor que foi usado quando o objeto do servidor RADIUS no FMC foi criado.

Identity Services Engine

Home > Content Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

Name: DRIVERAP_FTD_7.0

Description:

IP Address: 192.168.0.100 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

Is PSEC Device:

Device Type: All Device Types

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: *****

Use Second Shared Secret:

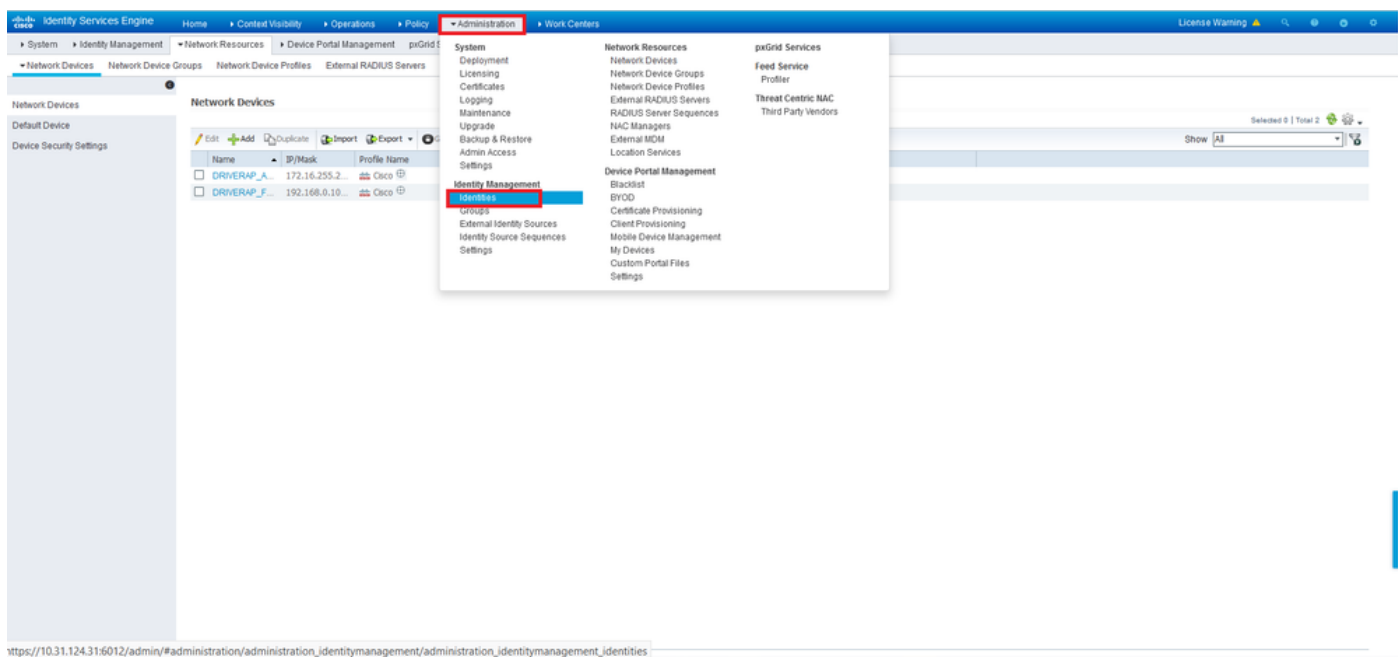
CoA Port: 1700

RADIUS DTLS Settings

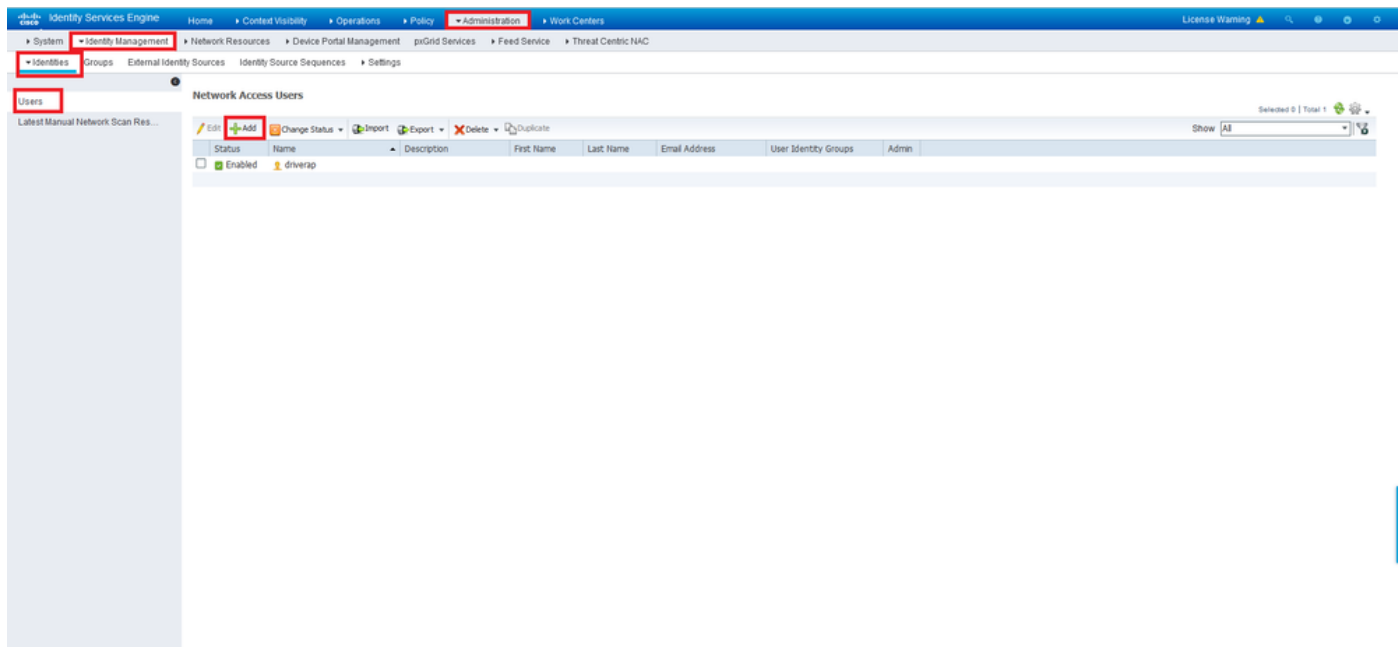
DTLS Required:

Salve-o com o botão no final desta página.

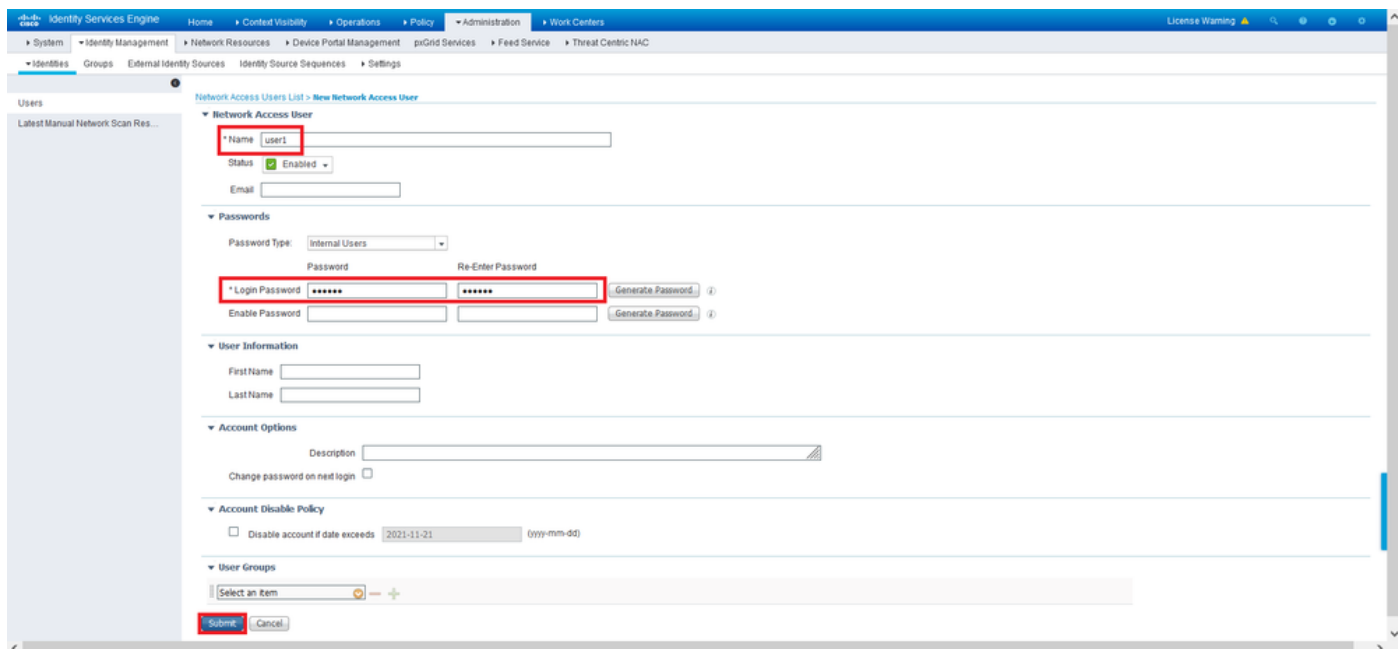
Etapa 3. Navegue até **Administração > Gerenciamento de identidades > Identidades**.



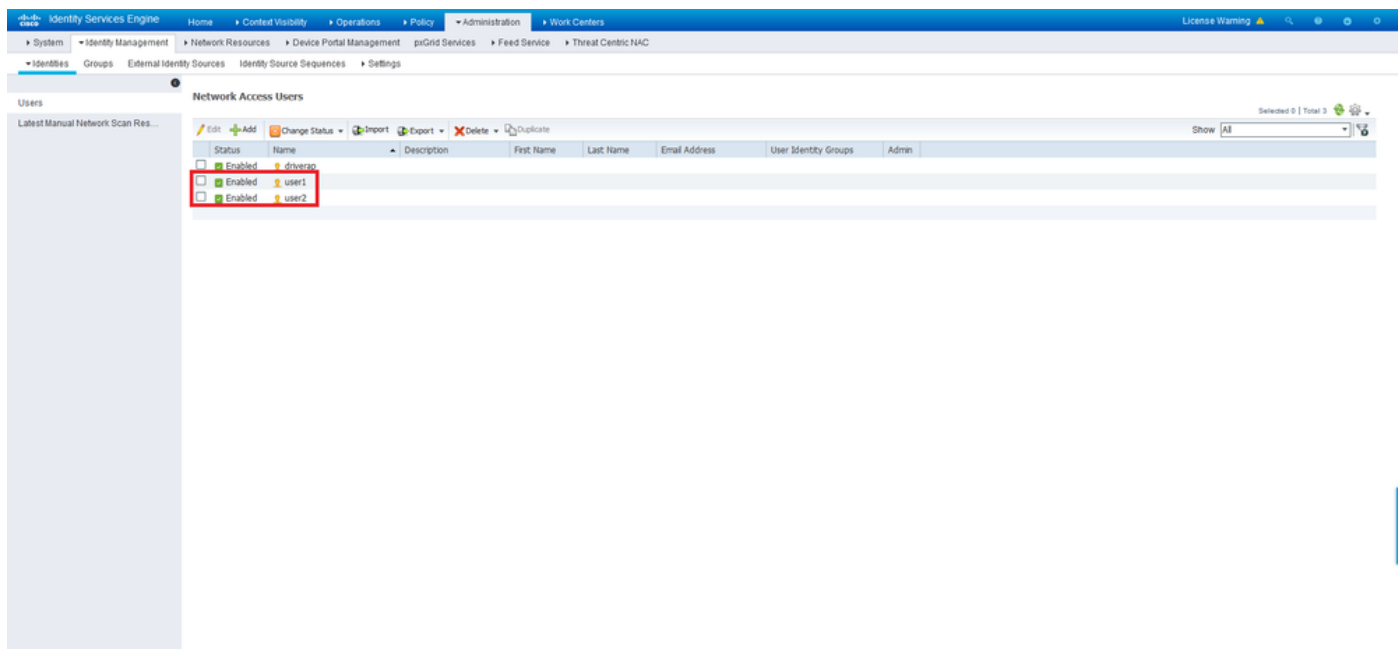
Etapa 4. Na seção **Usuários de Acesso à Rede**, clique em **Adicionar** para criar *user1* no banco de dados local do ISE.



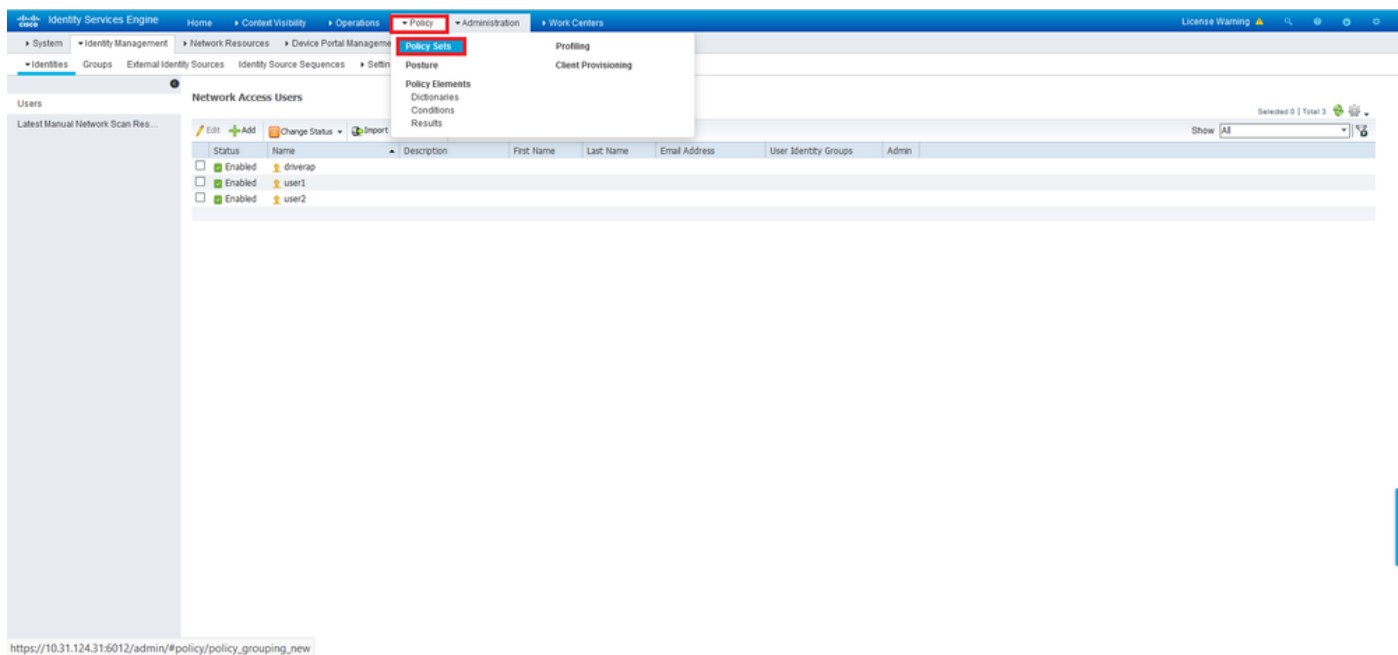
Insira o nome de usuário e a senha nos campos **Nome** e **Senha de login** e clique em **Enviar**.



Etapa 5. Repita as etapas anteriores para criar *user2*.

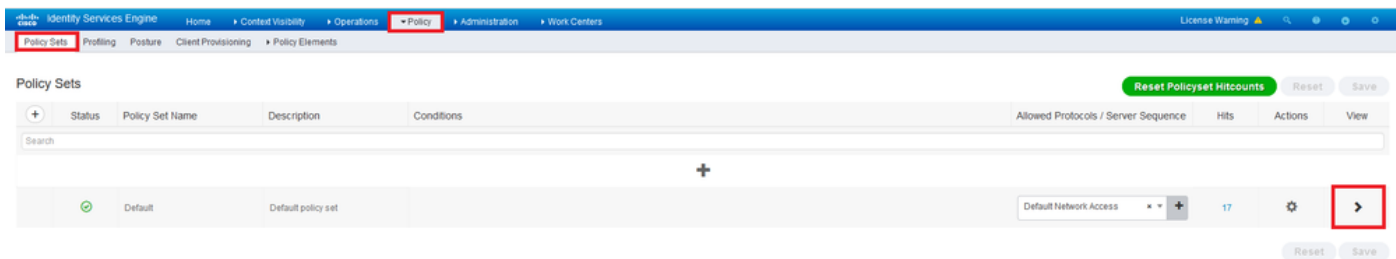


Etapa 6. Navegue até **Política > Conjuntos de políticas**.

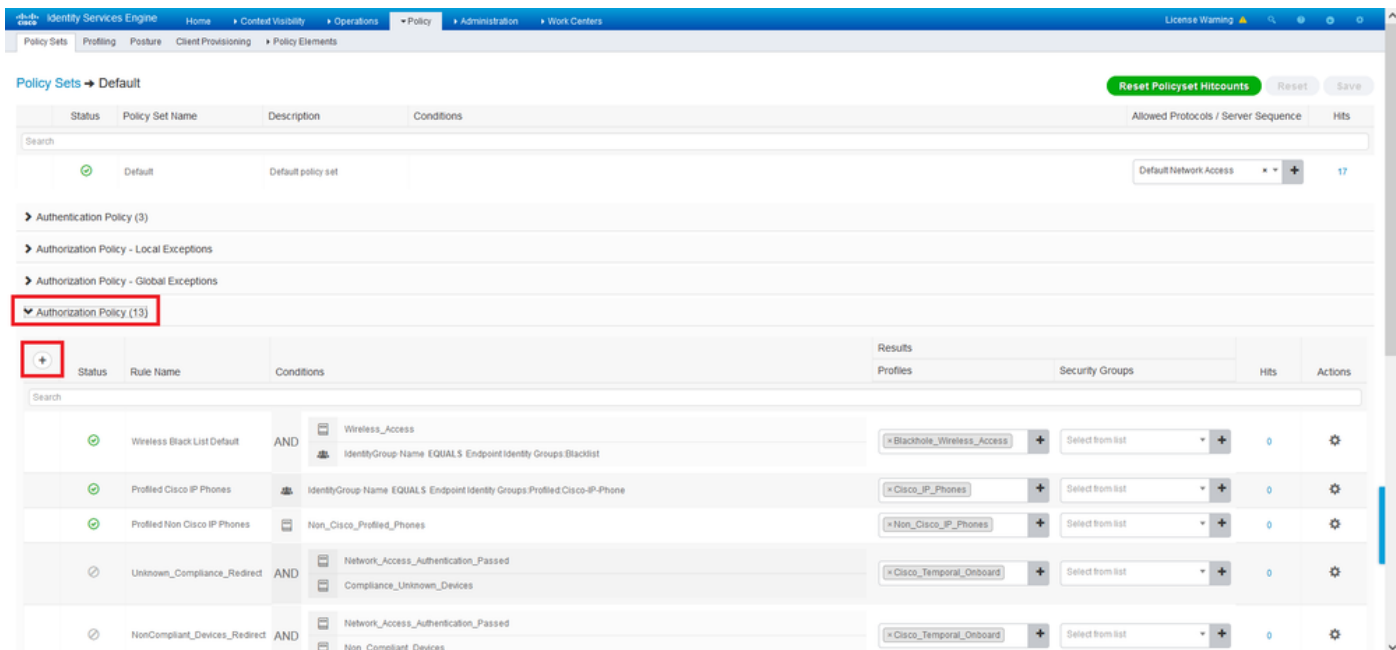


https://10.31.124.31:6012/admin/#policy/policy_grouping_new

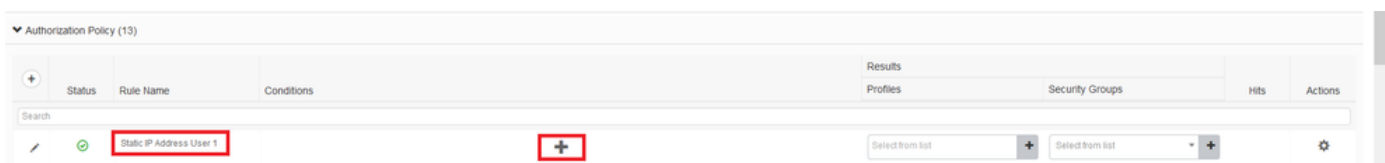
Passo 7. Clique na seta > no lado direito da tela.



Etapa 8. Clique na seta > ao lado de **Política de autorização** para expandi-la. Agora, clique no símbolo + para adicionar uma nova regra.



Forneça um nome para a regra e selecione o + símbolo na coluna **Condições**.



Clique na caixa de texto Editor de atributos e clique no ícone **Assunto**. Role para baixo até encontrar o atributo *Nome de usuário RADIUS* e escolha-o.

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MAC_in_SAN

Network_Access_Authentication_Passwd

Non_Cisco_Profined_Phones

Non_Compliant_Devices

Switch_Local_Web_Authentication

Switch_Web_Authentication

Editor

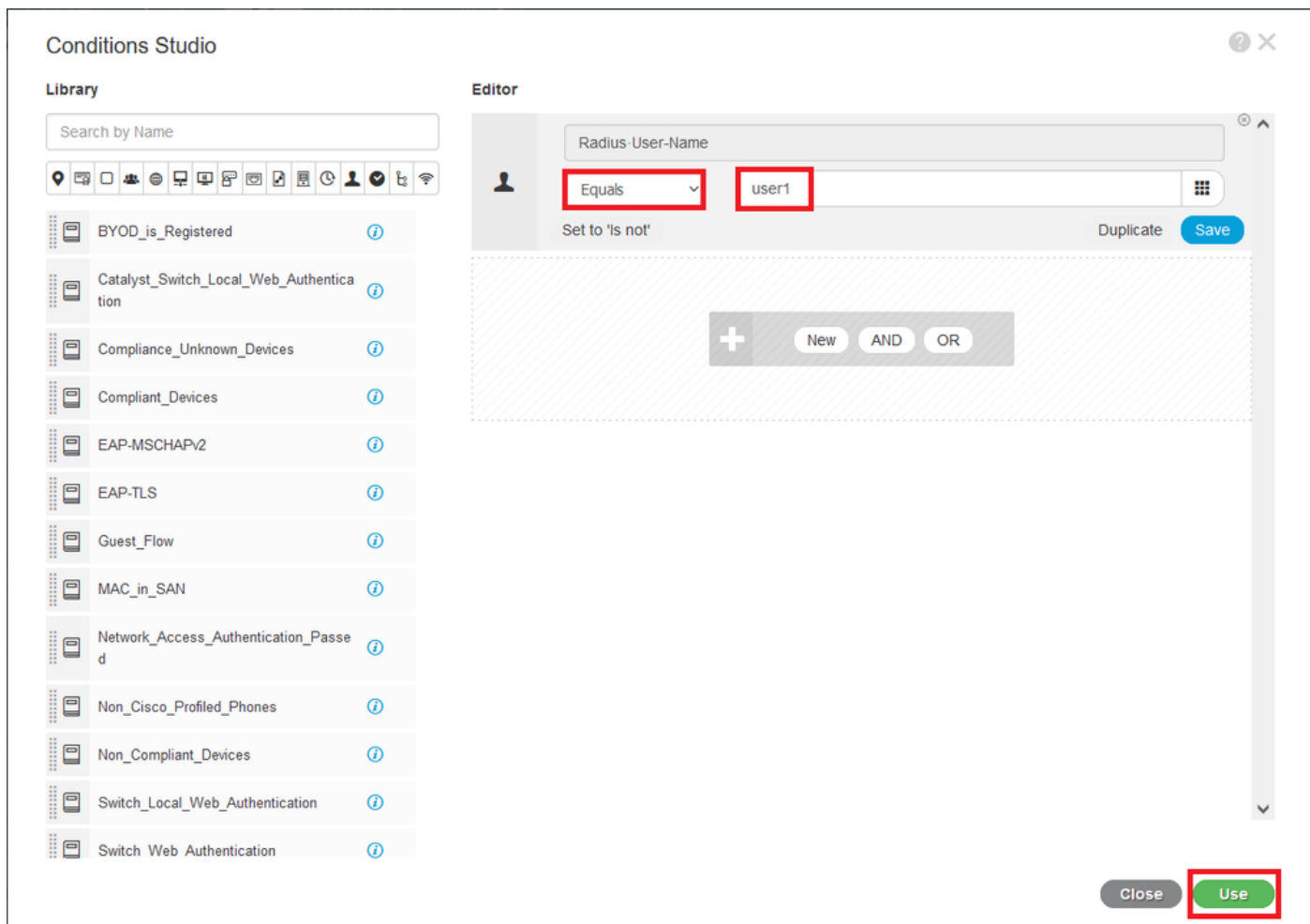
Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Microsoft	MS-HCAP-User-Name	60	
Motorola-Symbol	Symbol-User-Group	12	
Network Access	AD-User-DNS-Domain		
Network Access	AD-User-Join-Point		
Network Access	UserName		
PassiveID	PassiveID_Username		
Radius	User-Name	1	
Radius	User-Password	2	
Ruckus	Ruckus-User-Groups	1	

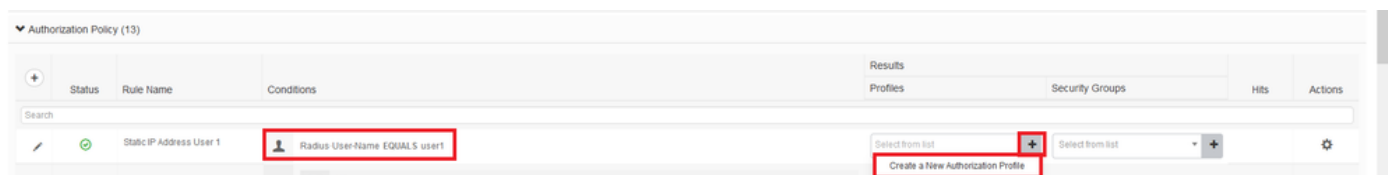
Close Use

Mantenha **Igual** ao operador e digite *user1* na caixa de texto ao lado dele. Clique em **Usar** para salvar o atributo.



A condição para esta regra está agora definida.

Etapa 9. Na coluna **Results/Profiles**, clique no símbolo + e escolha **Create a New Authorization Profile**.



Forneça um **Nome** e mantenha **ACCESS_ACCEPT** como o **Tipo de Acesso**. Role para baixo até a seção **Configurações de atributos avançados**.

Add New Standard Profile

Authorization Profile

* Name: StaticIPAddressUser1

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐ (i)

Passive Identity Tracking: ☐ (i)

Common Tasks

☐ DACL Name

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

< >

Save Cancel

Clique na seta laranja e escolha **Radius > Framed-IP-Address**—[8].

Add New Standard Profile

Service Template: ☐

Track Movement: ☐ (i)

Passive Identity Tracking: ☐ (i)

Common Tasks

☐ DACL Name

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

Advanced Attributes Setting

Radius: Framed-IP-Address

Attributes Details

Access Type = ACCESS_ACCEPT

Framed-IP-Address =

< >

Save Cancel

Digite o endereço IP que você deseja atribuir estaticamente a este usuário e clique em **Salvar**.

Add New Standard Profile

Service Template ☐

Track Movement ☐ (i)

Passive Identity Tracking ☐ (i)

Common Tasks

☐ Airespace IPv6 ACL Name

☐ ASA VPN

☐ AVC Profile Name

☐ UPN Lookup

Advanced Attributes Settings

Radius:Framed-IP-Address = 10.0.50.101

Attributes Details

Access Type = ACCESS_ACCEPT
Framed-IP-Address = 10.0.50.101

Save **Cancel**

Etapa 10. Agora, escolha o perfil de autorização recém-criado.

Authorization Policy (13)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	Static IP Address User 1	Radius-User-Name EQUALS user1	Selected from list	Selected from list		
+	Wireless Black List Default	AND Wireless_Access IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	DenyAccess	Selected from list	0	
+	Profiled Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco IP-Phone	Non_Cisco_IP_Phones	Selected from list	0	
+	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	StaticIPaddressUser1	Selected from list	0	

A regra de autorização está agora definida. Click **Save**.

Policy Sets → Default

Reset Policyset Hitcounts **Reset** **Save**

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
+	Default	Default policy set		Default Network Access	17

Authentication Policy (3)

Authorization Policy - Local Exceptions

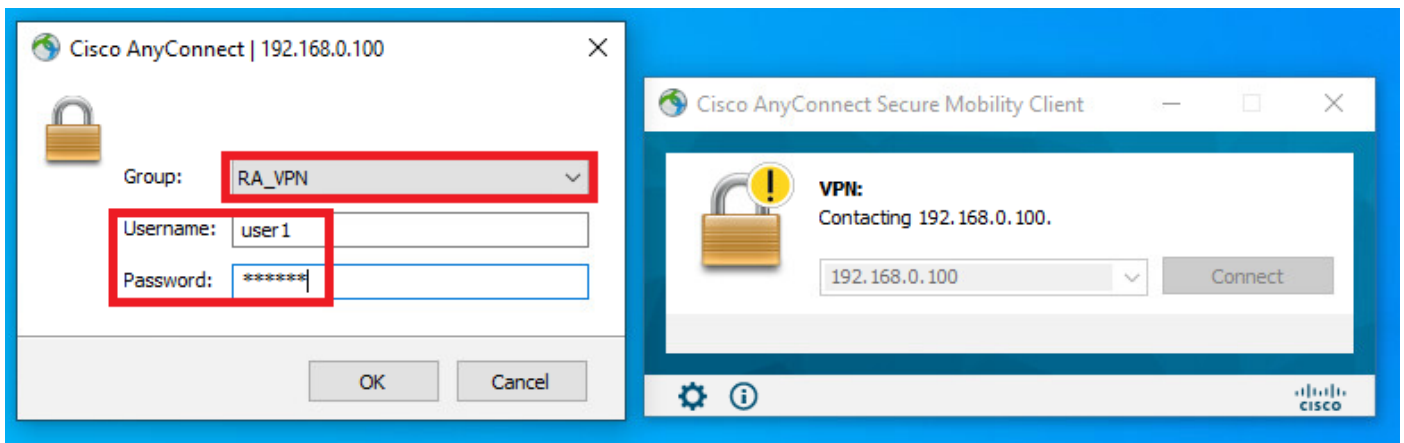
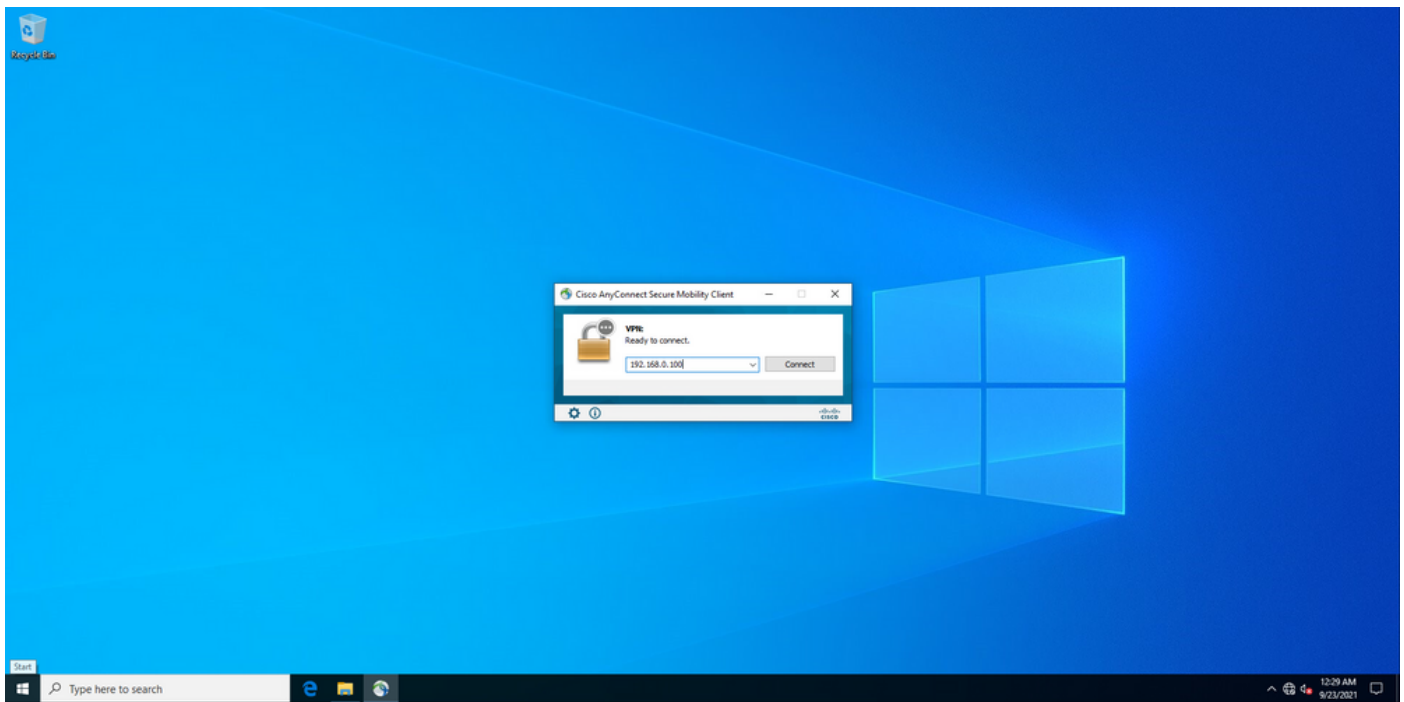
Authorization Policy - Global Exceptions

Authorization Policy (13)

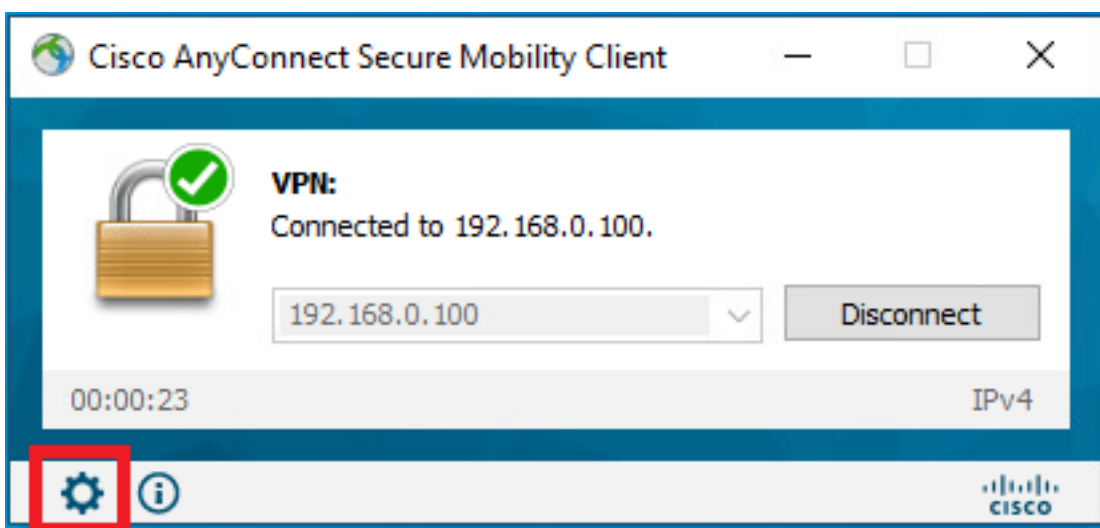
Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
+	Static IP Address User 1	Radius-User-Name EQUALS user1	StaticIPaddressUser1	Selected from list		

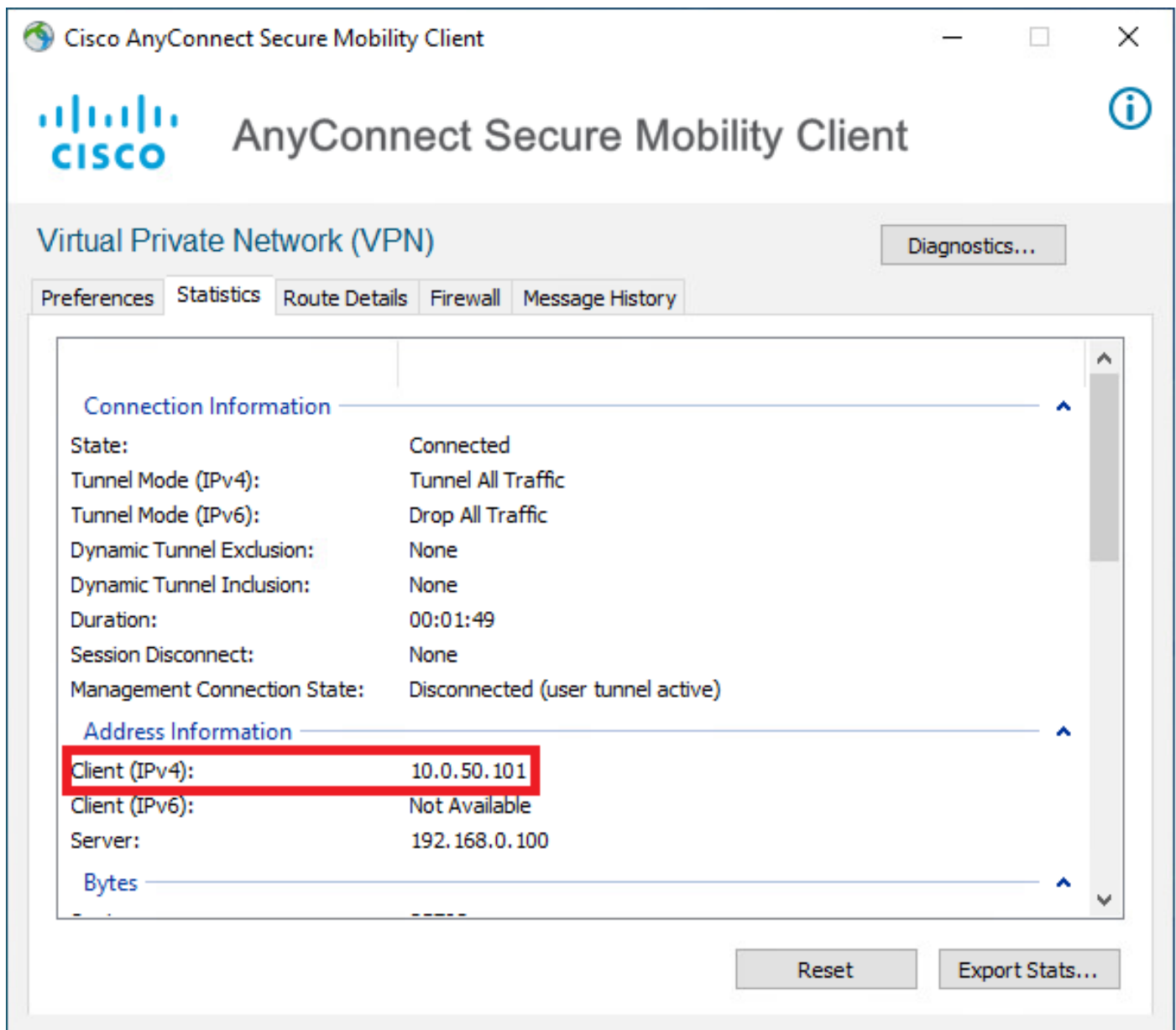
Verificar

Etapa 1. Navegue até sua máquina cliente onde o cliente Cisco AnyConnect Secure Mobility está instalado. Conecte-se ao headend FTD (uma máquina Windows é usada aqui) e insira as credenciais *user1*.



Clique no ícone da engrenagem (canto inferior esquerdo) e navegue até a guia **Estatística**. Confirme na seção **Informações de Endereço** que o endereço IP atribuído é realmente o configurado na política de autorização do ISE para este usuário.





A saída do comando **debug radius all** no FTD mostra:

```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0x9000)
radius mkreq: 0x13
alloc_rip 0x0000145d043b6460
new request 0x13 --> 3 (0x0000145d043b6460)
got user 'user1'
got password
add_req 0x0000145d043b6460 session 0x13 id 3
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101
```

RADIUS packet decode (authentication request)

RADIUS packet decode (response)

Raw packet data (length = 136).....

```

02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 | .....AK..X...1
7d aa 38 1e 01 07 75 73 65 72 31 08 06 0a 00 32 | }.8...user1....2
65 19 3d 43 41 43 53 3a 63 30 61 38 30 30 36 34 | e.=CACS:c0a80064
30 30 30 30 61 30 30 30 36 31 34 62 63 30 32 64 | 0000a000614bc02d
3a 64 72 69 76 65 72 61 70 2d 49 53 45 2d 32 2d | :driverap-ISE-2-
37 2f 34 31 37 34 39 34 39 37 38 2f 32 31 1a 2a | 7/417494978/21.*
00 00 00 09 01 24 70 72 6f 66 69 6c 65 2d 6e 61 | .....$profile-na
6d 65 3d 57 69 6e 64 6f 77 73 31 30 2d 57 6f 72 | me=Windows10-Wor
6b 73 74 61 74 69 6f 6e | kstation

```

Parsed packet data.....

Radius: Code = 2 (0x02)

Radius: Identifier = 3 (0x03)

Radius: Length = 136 (0x0088)

Radius: Vector: 0CAF1C414BC4A658DEF392317DAA381E

Radius: Type = 1 (0x01) User-Name

Radius: Length = 7 (0x07)

Radius: Value (String) =

75 73 65 72 31 | user1

Radius: Type = 8 (0x08) Framed-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 10.0.50.101 (0x0A003265)

Radius: Type = 25 (0x19) Class

Radius: Length = 61 (0x3D)

Radius: Value (String) =

43 41 43 53 3a 63 30 61 38 30 30 36 34 30 30 30 | CACS:c0a80064000

30 61 30 30 30 36 31 34 62 63 30 32 64 3a 64 72 | 0a000614bc02d:dr

69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4

31 37 34 39 34 39 37 38 2f 32 31 | 17494978/21

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 42 (0x2A)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 36 (0x24)

Radius: Value (String) =

70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win

64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati

6f 6e | on

rad_procpkt: ACCEPT

Got AV-Pair with value profile-name=Windows10-Workstation

RADIUS_ACCESS_ACCEPT: normal termination

RADIUS_DELETE

remove_req 0x0000145d043b6460 session 0x13 id 3

free_rip 0x0000145d043b6460

radius: send queue empty

Os registros FTD mostram:

firepower#

<omitted output>

Sep 22 2021 23:52:40: %FTD-6-725002: Device completed SSL handshake with client

Outside_Int:192.168.0.101/60405 to 192.168.0.100/443 for TLSv1.2 session

Sep 22 2021 23:52:48: %FTD-7-609001: Built local-host Outside_Int:172.16.0.8

Sep 22 2021 23:52:48: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 :
user = user1

Sep 22 2021 23:52:48: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user
= user1

Sep 22 2021 23:52:48: %FTD-6-113008: **AAA transaction status ACCEPT : user = user1**

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.radius["1"]["1"] = user1

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.radius["8"]["1"] = 167785061

Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute

```

aaa.radius["25"]["1"] = CACS:c0a800640000c000614bc1d0:driverap-ISE-2-7/417494978/23
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.grouppolicy = DfltGrpPolicy
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.ipaddress = 10.0.50.101
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username = user1
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username1 = user1
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.username2 =
Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute
aaa.cisco.tunnelgroup = RA_VPN
Sep 22 2021 23:52:48: %FTD-6-734001: DAP: User user1, Addr 192.168.0.101, Connection AnyConnect:
The following DAP records were selected for this connection: DfltAccessPolicy
Sep 22 2021 23:52:48: %FTD-6-113039: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101>
AnyConnect parent session started.
<omitted output>
Sep 22 2021 23:53:17: %FTD-6-725002: Device completed SSL handshake with client
Outside_Int:192.168.0.101/60412 to 192.168.0.100/443 for TLSv1.2 session
Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv4 address request' message
queued
Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv6 address request' message
queued
Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv4 address
request'
Sep 22 2021 23:53:17: %FTD-6-737010: IPAA: Session=0x0000c000, AAA assigned address 10.0.50.101,
succeeded
Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv6 address
request'
Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: no IPv6 address
available from local pools
Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: callback failed
during IPv6 request
Sep 22 2021 23:53:17: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User
<user1> IP <192.168.0.101> No IPv6 address available for SVC connection
Sep 22 2021 23:53:17: %FTD-7-609001: Built local-host Outside_Int:10.0.50.101
Sep 22 2021 23:53:17: %FTD-5-722033: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> First
TCP SVC connection established for SVC session.
Sep 22 2021 23:53:17: %FTD-6-722022: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> TCP
SVC connection established without compression
Sep 22 2021 23:53:17: %FTD-7-746012: user-identity: Add IP-User mapping 10.0.50.101 -
LOCAL\user1 Succeeded - VPN user
Sep 22 2021 23:53:17: %FTD-6-722055: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101>
Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086
Sep 22 2021 23:53:17: %FTD-4-722051: Group

```

Os registros RADIUS Live no ISE mostram:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:50:56:96:40:0F (0)
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

Authentication Details

Source Timestamp	2021-09-22 23:53:19.72
Received Timestamp	2021-09-22 23:53:19.72
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00:50:56:96:40:0F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	d8a800540000d00014bctd0
Authentication Method	PAP_ASCM
Authentication Protocol	PAP_ASCM
Network Device	DRIVERAP_FTD_7.0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

Steps

11001 Received RADIUS AccessRequest
11017 RADIUS created a new session
15049 Evaluating Policy Group
15050 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15040 Queried PIP - Normalised Radius RadiusFlowType (4 times)
22072 Selected identity source sequence - All_User_ID_Store
15013 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
15030 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
15040 Queried PIP - Radius User Name
15010 Selected Authorization Profile - StaticIPAddressUser1
22081 Max session policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS AccessAccept

Identity Services Engine

NAS Port Type

Virtual

Authorization Profile

StaticIPAddressUser1

Response Time

51 milliseconds

Other Attributes

ConfigVersionId	146
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000ASAPFOF-Tunnel-Group-Name	RA_VPN
OriginalUsername	user1
NetworkDeviceProfileId	30059905-3150-4210-a80e-6753445f550c
IsThirdPartyDeviceFlow	false
CVPN3000ASAPFOF-Client-Type	2
AcctSessionID	driverap-ISE-2-71417494378/23
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
Location	LocationAll Locations
Device Type	DeviceTypeAll Device Types

IPSEC

IPSECOnly IPSEC Device#0

EnableFlag

Enabled

RADIUS Username

user1

Device IP Address

192.168.0.100

CPM SessionID

d8a800540000d00014bctd0

Called Station ID

192.168.0.100

CiscoWPAir

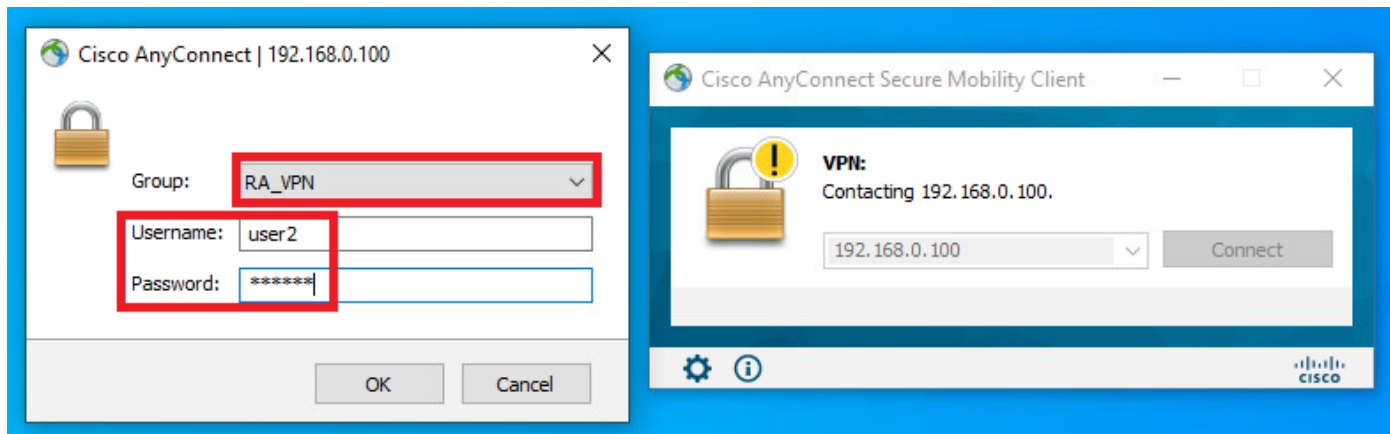
mdu-dmdevice-platform=win,
mdu-dmdevice-manufacturer=00:50:56:96:40:0F,
mdu-dmdevice-platform-version=10.0.13362,
mdu-dmdevice-public-manufacturer=00:50:56:96:40:0F,
mdu-dmdevice-user-agent=AnyConnect Windows 4.10.02080,
mdu-dmdevice-type=VMware, Inc. VMware Virtual Platform,
mdu-dmdevice-vendor=global=15F8E8C0F62F3F2C0E2431459F4BA2AE2C9B3,
mdu-dmdevice-uid=3C384D7071F907B2F810F124621184408596C717E370386C030F
945C0880344,
acct-session-id=d8a800540000d00014bctd0,
ip-source-ip=192.168.0.101,
coa-push=true

Result

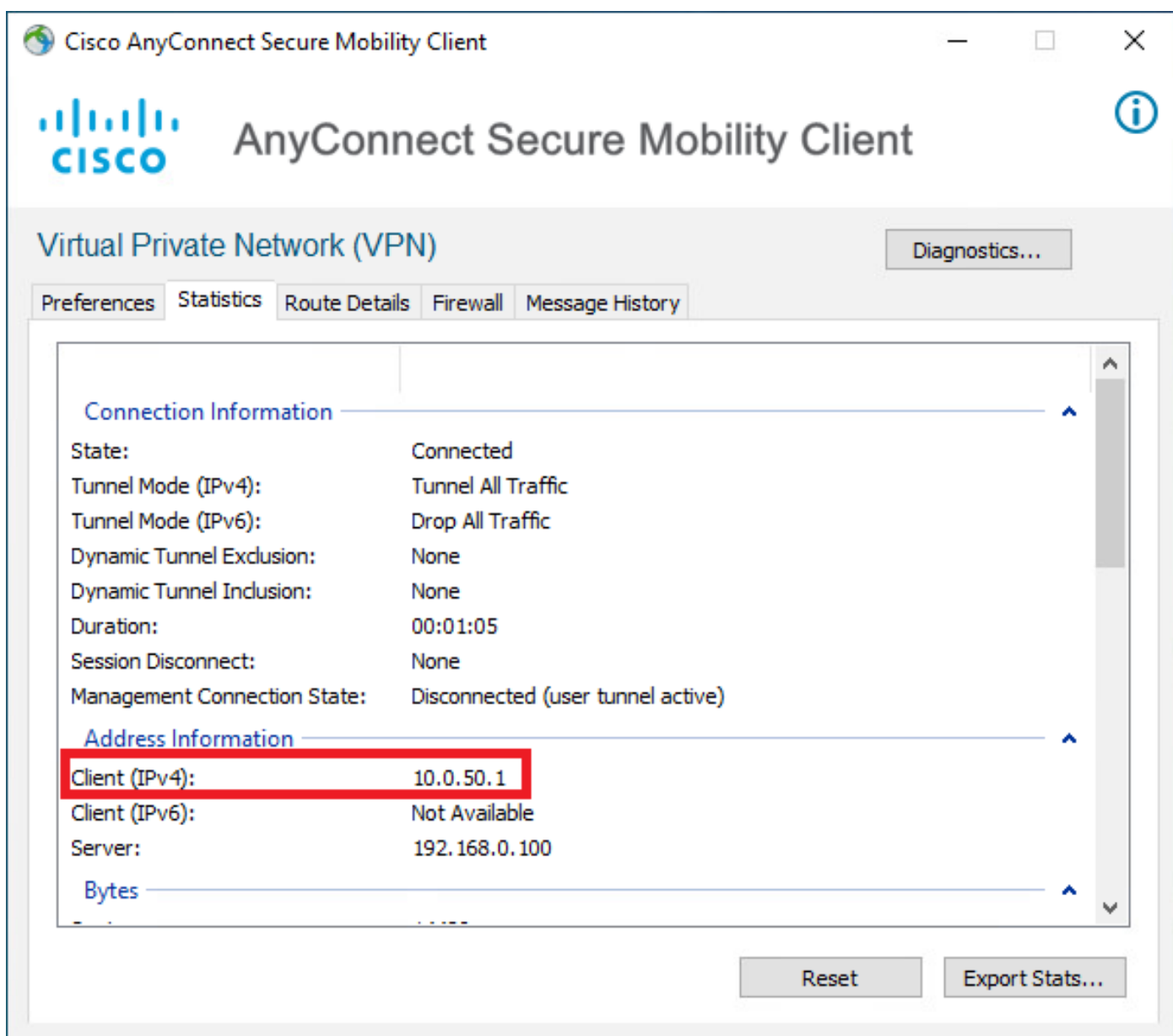
Framed IP Address	10.0.0.101
Class	CACS-d8a800540000d00014bctd0 driverap-ISE-2-71417494378/23
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events

Etapa 2. Conecte-se ao headend FTD (uma máquina Windows é usada aqui) e insira as credenciais *do usuário2*.



A seção **Address Information** mostra que o endereço IP atribuído é, de fato, o primeiro endereço IP disponível no pool local IPv4 configurado via FMC.



A saída do comando **debug radius all** no FTD mostra:

```
firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
```

```
np_svc_destroy_session(0xA000)
radius mkreq: 0x15
alloc_rip 0x0000145d043b6460
new request 0x15 --> 4 (0x0000145d043b6460)
got user 'user2'
got password
add_req 0x0000145d043b6460 session 0x15 id 4
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101
```

RADIUS packet decode (authentication request)

RADIUS packet decode (response)

```
-----
Raw packet data (length = 130).....
02 04 00 82 a6 67 35 9e 10 36 93 18 1f 1b 85 37 | .....g5..6.....7
b6 c3 18 4f 01 07 75 73 65 72 32 19 3d 43 41 43 | ...0..user2.=CAC
53 3a 63 30 61 38 30 30 36 34 30 30 30 62 30 | S:c0a800640000b0
30 30 36 31 34 62 63 30 61 33 3a 64 72 69 76 65 | 00614bc0a3:drive
72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 31 37 34 | rap-ISE-2-7/4174
39 34 39 37 38 2f 32 32 1a 2a 00 00 00 09 01 24 | 94978/22.*.....$
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win
64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati
6f 6e | on
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 4 (0x04)
Radius: Length = 130 (0x0082)
Radius: Vector: A667359E103693181F1B8537B6C3184F
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 32 | user2
Radius: Type = 25 (0x19) Class
Radius: Length = 61 (0x3D)
Radius: Value (String) =
43 41 43 53 3a 63 30 61 38 30 30 36 34 30 30 30 | CACS:c0a800640000
30 62 30 30 30 36 31 34 62 63 30 61 33 3a 64 72 | 0b000614bc0a3:dr
69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4
31 37 34 39 34 39 37 38 2f 32 32 | 17494978/22
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 42 (0x2A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 36 (0x24)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win
64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati
6f 6e | on
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Windows10-Workstation
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x0000145d043b6460 session 0x15 id 4
free_rip 0x0000145d043b6460
radius: send queue empty
```

Os registros FTD mostram:

<omitted output>

Sep 22 2021 23:59:26: %FTD-6-725002: Device completed SSL handshake with client
Outside_Int:192.168.0.101/60459 to 192.168.0.100/443 for TLSv1.2 session
Sep 22 2021 23:59:35: %FTD-7-609001: Built local-host Outside_Int:172.16.0.8
Sep 22 2021 23:59:35: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 :
user = user2
Sep 22 2021 23:59:35: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user
= user2
Sep 22 2021 23:59:35: %FTD-6-113008: AAA transaction status ACCEPT : user = user2
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.radius["1"]["1"] = user2
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.radius["25"]["1"] = CACS:c0a800640000d000614bc367:driverap-ISE-2-7/417494978/24
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.cisco.grouppolicy = DfltGrpPolicy
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: **Session Attribute**
aaa.cisco.username = user2
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.cisco.username1 = user2
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.cisco.username2 =
Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute
aaa.cisco.tunnelgroup = RA_VPN
Sep 22 2021 23:59:35: %FTD-6-734001: DAP: User user2, Addr 192.168.0.101, Connection AnyConnect:
The following DAP records were selected for this connection: DfltAccessPolicy
Sep 22 2021 23:59:35: %FTD-6-113039: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101>
AnyConnect parent session started.

<omitted output>

Sep 22 2021 23:59:52: %FTD-6-725002: Device completed SSL handshake with client
Outside_Int:192.168.0.101/60470 to 192.168.0.100/443 for TLSv1.2 session
Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv4 address request' message
queued
Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv6 address request' message
queued
Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv4 address
request'
Sep 22 2021 23:59:52: %FTD-5-737003: IPAA: Session=0x0000d000, DHCP configured, no viable
servers found for tunnel-group 'RA_VPN'
Sep 22 2021 23:59:52: %FTD-7-737400: **POOLIP: Pool=AC_Pool, Allocated 10.0.50.1 from pool**
Sep 22 2021 23:59:52: %FTD-7-737200: **VPNFIIP: Pool=AC_Pool, Allocated 10.0.50.1 from pool**
Sep 22 2021 23:59:52: %FTD-6-737026: **IPAA: Session=0x0000d000, Client assigned 10.0.50.1 from**
local pool AC_Pool
Sep 22 2021 23:59:52: %FTD-6-737006: **IPAA: Session=0x0000d000, Local pool request succeeded for**
tunnel-group 'RA_VPN'
Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv6 address
request'
Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: no IPv6 address
available from local pools
Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: callback failed
during IPv6 request
Sep 22 2021 23:59:52: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User
<user2> IP <192.168.0.101> No IPv6 address available for SVC connection
Sep 22 2021 23:59:52: %FTD-7-609001: Built local-host Outside_Int:10.0.50.1
Sep 22 2021 23:59:52: %FTD-5-722033: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> First
TCP SVC connection established for SVC session.
Sep 22 2021 23:59:52: %FTD-6-722022: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> TCP
SVC connection established without compression
Sep 22 2021 23:59:52: %FTD-7-746012: **user-identity: Add IP-User mapping 10.0.50.1 - LOCAL\user2**
Succeeded - VPN user
Sep 22 2021 23:59:52: %FTD-6-722055: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101>
Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086
Sep 22 2021 23:59:52: %FTD-4-722051: **Group**

Os registros RADIUS Live no ISE mostram:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user2
Endpoint Id	00:50:56:96:45:6F:D
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2021-09-23 00:00:06:488
Received Timestamp	2021-09-23 00:00:06:488
Policy Server	drivewap-ISE-2-7
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	00:50:56:96:45:6F:D
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	cba800540000d00014bc367
Authentication Method	PAP_ASCSI
Authentication Protocol	PAP_ASCSI
Network Device	DRIVERAP_FT0_7-8
Device Type	All Device Types
Location	All Locations
NAS IP v4 Address	0.0.0.0

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15048 Queried PIP - Normalised Radius RadiusType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user2
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 - user2
24219 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Radius User Name
15048 Queried PIP - Radius NAS-Port Type
15048 Queried PIP - Endpoints Logical Profile
15048 Queried PIP - Network Access Authentication Status
15016 Selected Authorization Profile - PermitAccess
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

Identity Services Engine

NAS Port Type

Virtual

Authorization Profile

PermitAccess

Response Time

202 milliseconds

Other Attributes

ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel Client Endpoint	(tag=0) 192.168.0.101
CVPR3000ASA/PO7x-Tunnel-Group Name	RA_VPN
OriginalUsername	user2
NetworkDeviceProfileId	b0899005-3150-4215-a80e-6753445f856c
IsThirdPartyDeviceFlow	false
CVPR3000ASA/PO7x-Client Type	2
AccSessionID	drivewap-ISE-2-7-1417494978-24
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_join_Frinds
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLS Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	DeviceTypeAll Device Types

IPSEC

IPSECv2 IPSEC DeviceId

Name

Endpoint Identity Groups Profiled Workstation

EnableFlag

Enabled

RADIUS Username

user2

Device IP Address

192.168.0.100

CPM Session ID

cba800540000d00014bc367

Called Station ID

192.168.0.100

CiscoAvPair

mdu-device-platform:mdu-device-mac=00:50:56:96:45:6F:D
mdu-device-platform-req=win10.18362
mdu-device-public-mac=00:50:56:96:45:6F:D
mdu-device-user-agent=WinConnect Windows 4.10.22086
mdu-device-type=VMware, Inc. VMware Virtual Platform
mdu-device-uid=global=159f88e50cf52f3f2c0e2431459f48aa2ae2c0b3
mdu-device-uid=3C3840771F80782F816F124521184406596C717E37088CC03DF94A9C886244
audit-session-id=cba800540000d00014bc367
id-source-ip=192.168.0.101
id-source-mac=

Result

Class	CACS cba800540000d00014bc367 drivewap-ISE-2-7-1417494978-24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Session Events

Note: Você deve usar diferentes intervalos de endereços IP para atribuição de endereços IP no pool local de IP FTD e nas políticas de autorização ISE para evitar conflitos de endereço IP duplicado entre seus AnyConnect Clients. Neste exemplo de configuração, o FTD foi configurado com um pool local IPv4 de 10.0.50.1 a 10.0.50.100 e o servidor ISE atribui endereço IP estático de 10.0.50.101.

Troubleshoot

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

No DTF:

- **debug radius all**

No ISE:

- Registros ao vivo RADIUS