

FTD Remote Access VPN met MSCHAPv2 via RADIUS configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[RA VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren](#)

[ISE configureren ter ondersteuning van MS-CHAPv2 als verificatieprotocol](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe Microsoft Challenge Handshake Authentication Protocol, versie 2 (MS-CHAPv2), kan worden ingeschakeld als de verificatiemethode via Firepower Management Center (FMC) voor Remote Access VPN-clients met RADIUS-verificatie (Dial-In User Service (RADIUS)).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- FireSIGHT Management Center (FMC)
- Identity Services Engine (ISE)
- Cisco AnyConnect beveiligde mobiliteit-client
- RADIUS-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- FMCv - 7.0.0 (bouw 94)
- FTDv - 7.0.0 (gebouwd 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.2086
- Windows 10 Pro

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In de standaardinstelling gebruikt FTD Password Authentication Protocol (PAP) als de authenticatiemethode met RADIUS-servers voor AnyConnect VPN-verbindingen.

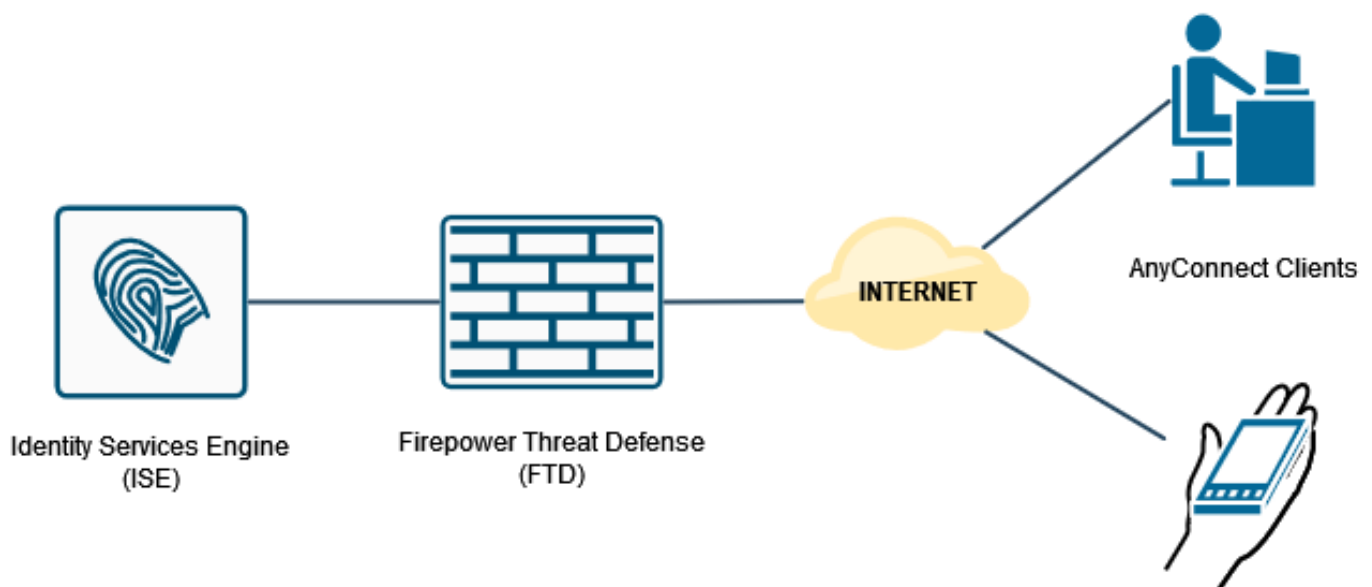
PAP biedt een eenvoudige methode voor gebruikers om hun identiteit vast te stellen met een tweevoudige handdruk. Het PAP-wachtwoord wordt versleuteld met een gedeeld geheim en is het minst gesofisticeerde verificatieprotocol. PAP is geen sterke authenticatiemethode omdat het weinig bescherming biedt tegen herhaalde trial-and-error aanvallen.

MS-CHAPv2 verificatie introduceert wederzijdse authenticatie tussen peers en een wachtwoordfunctie.

Om MS-CHAPv2 als protocol in te schakelen dat tussen de ASA en de RADIUS-server wordt gebruikt voor een VPN-verbinding, moet het wachtwoordbeheer in het verbindingsprofiel worden ingeschakeld. Bij het inschakelen van het wachtwoordbeheer wordt een aanvraag voor MS-CHAPv2-verificatie van de FTD naar de RADIUS-server gegenereerd.

Configureren

Netwerkdigram

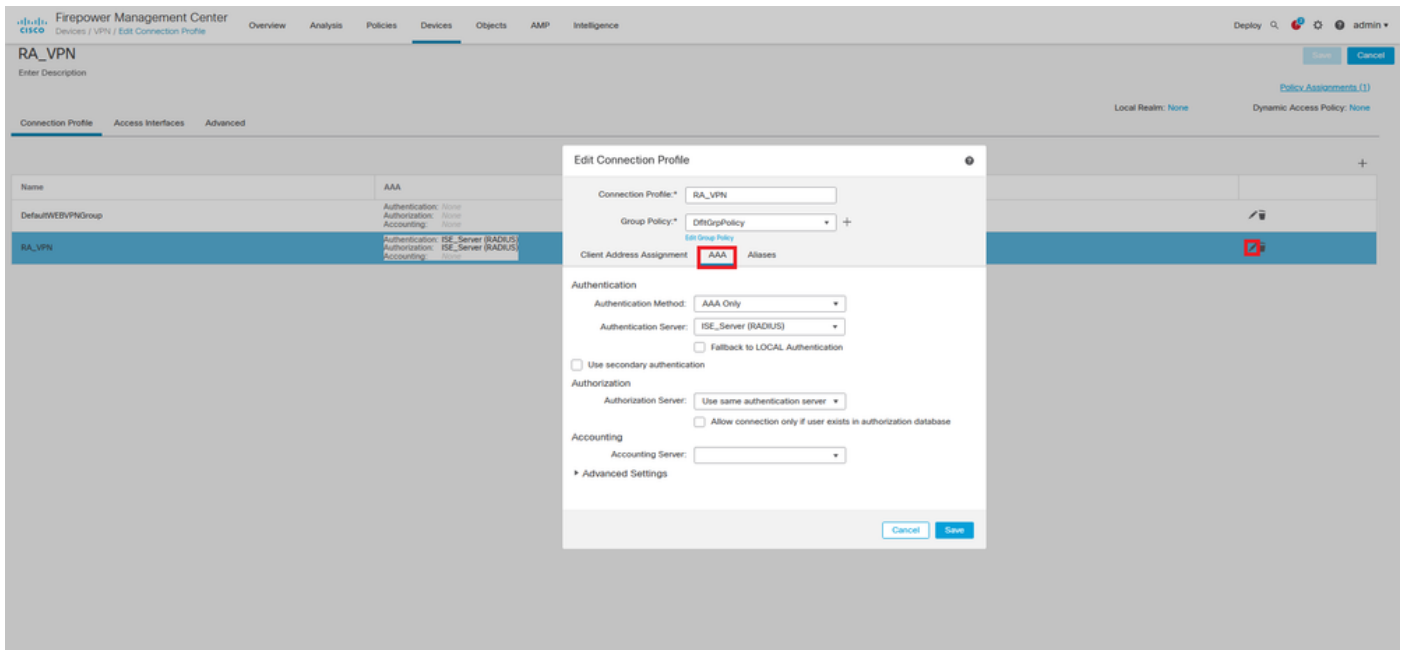


RA VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren

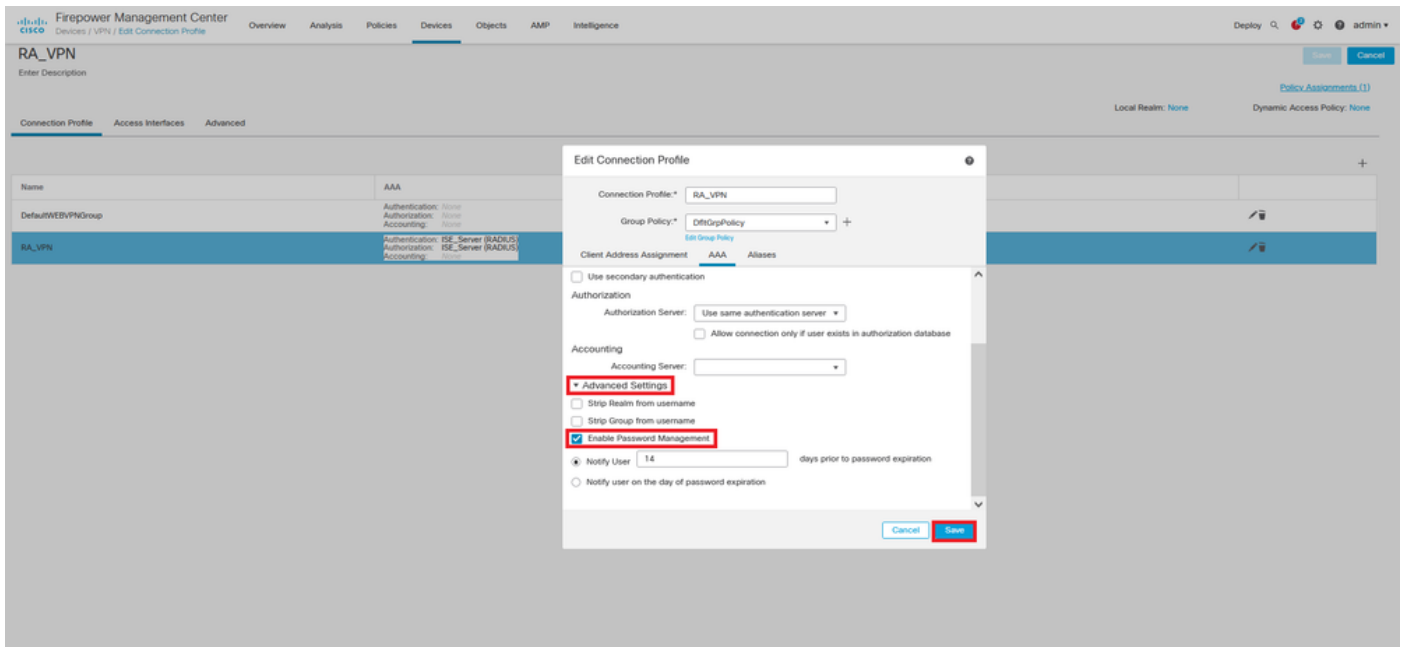
Verwijs voor een stap voor stap naar dit document en deze video:

- [AnyConnect Remote Access VPN-configuratie op FTD](#)
- [Initiële AnyConnect-configuratie voor FTD beheerd door FMC](#)

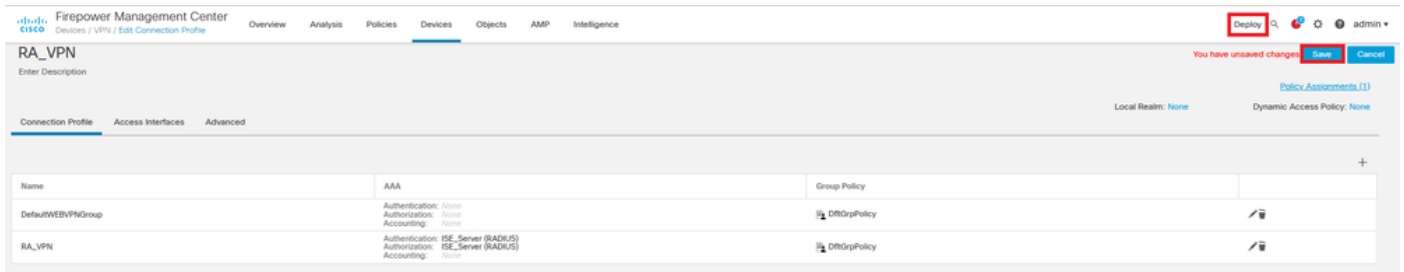
Stap 1. Nadat Remote Access VPN is geconfigureerd, navigeer naar **Apparaten > Externe toegang**, bewerk het nieuwe verbindingsprofiel en navigeer vervolgens naar het **AAA**-tabblad.



Vul het gedeelte **Geavanceerde instellingen** uit en klik op het vakje **Wachtwoordbeheer** inschakelen. Klik op **Opslaan**.



Opslaan en implementeren.



Remote Access VPN-configuratie op FTD CLI is:

```
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

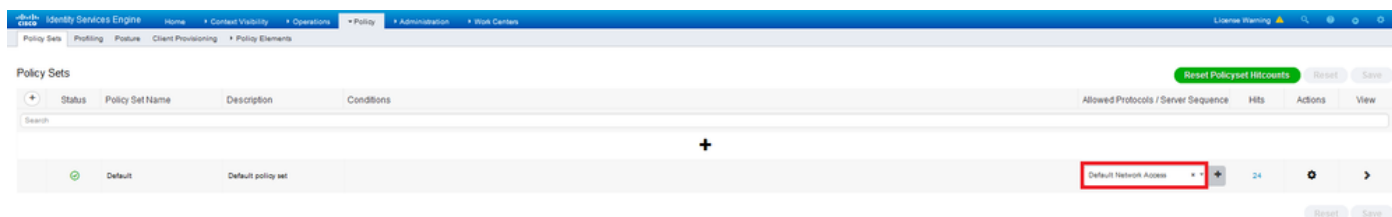
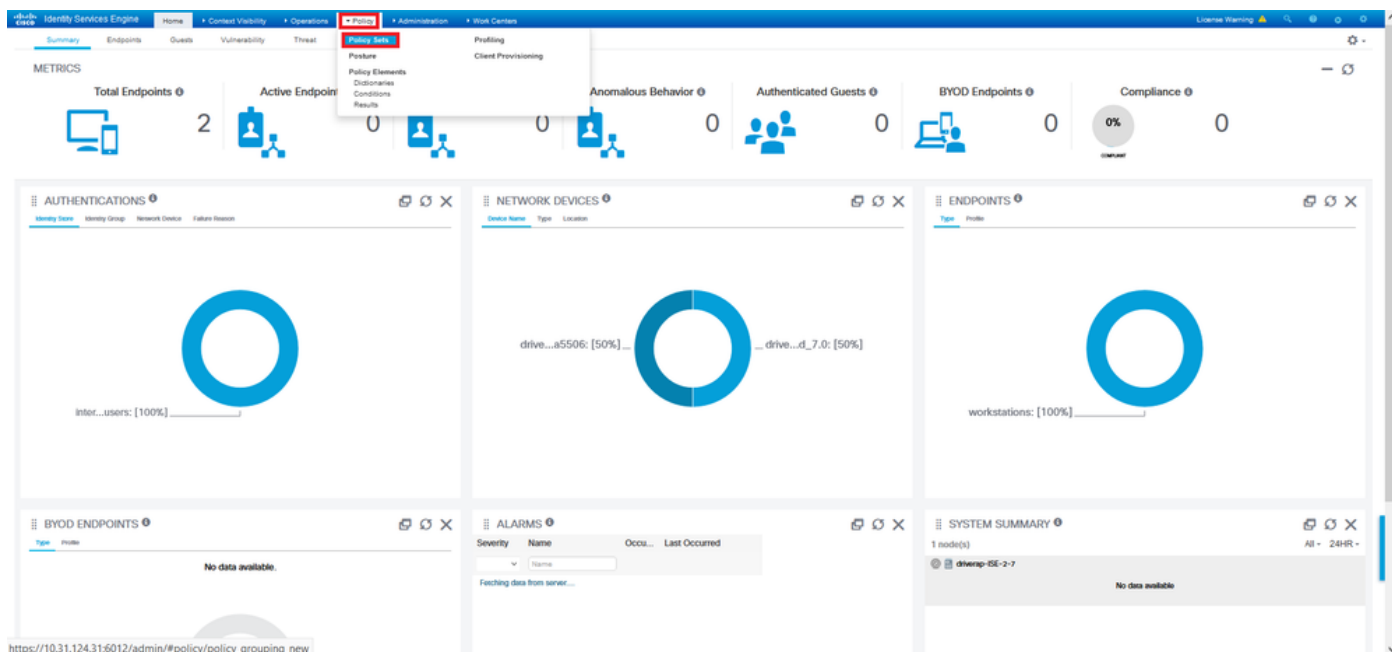
```
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

ISE configureren ter ondersteuning van MS-CHAPv2 als verificatieprotocol

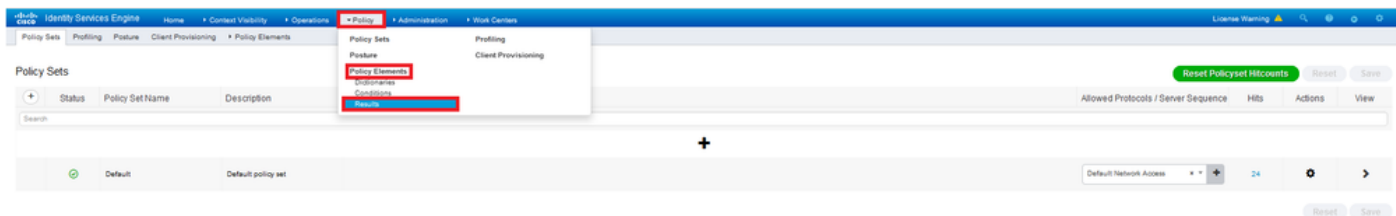
Aangenomen wordt dat:

1. De FTD is al toegevoegd als netwerkapparaat op ISE zodat het RADIUS-toegangs aanvragen van de FTD kan verwerken.
2. Er is ten minste één gebruiker beschikbaar voor ISE om de AnyConnect-client te authenticeren.

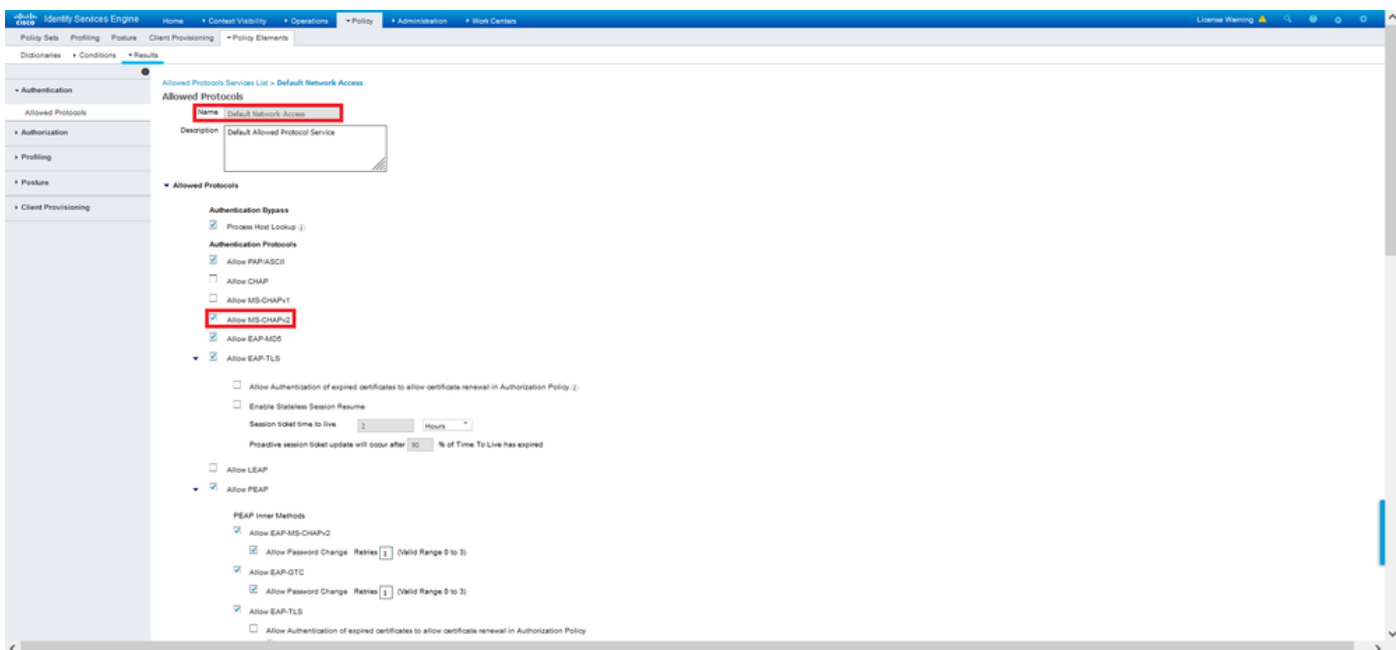
Stap 2. Navigeer naar **beleid > Beleidsformaten** en vind het **toegestane** beleid van **Protocollen** dat aan de beleidsset is toegevoegd en waar uw AnyConnect-gebruikers echt zijn bevonden. In dit voorbeeld is slechts één beleidsset aanwezig, zodat het beleid in kwestie *standaard netwerktoegang* is.



Stap 3. Navigeer in op **beleid > Beleidselementen > Resultaten**. Onder **Verificatie > Geboden protocollen** kiezen en bewerken **standaard netwerktoegang**.

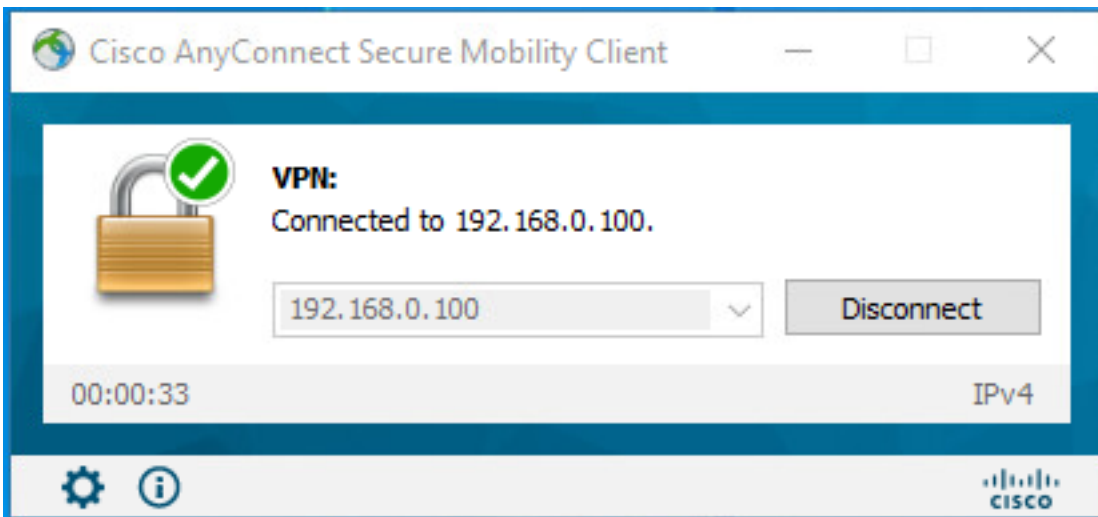


Controleer of het aanvinkvakje **Toestaan MS-CHAPv2** is ingeschakeld. Scrolt helemaal naar beneden en **bewaar** het.



Verifiëren

Navigeer naar uw clientmachine waar Cisco AnyConnect Secure Mobility client is geïnstalleerd. Sluit aan op het FTD head-end (een Windows-machine wordt in dit voorbeeld gebruikt) en typt de gebruikersreferenties.



De RADIUS Live Logs op ISE laten zien:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00 50 56 96 45 6F 0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

Authentication Details

Source Timestamp	2021-09-28 00:06:02.94
Received Timestamp	2021-09-28 00:06:02.94
Policy Server	driverap-ISE-0-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00 50 56 96 45 6F 0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c9a30054000a50061525a9
Authentication Method	MSCHAPV2
Authentication Protocol	MSCHAPV2
Network Device	DRIVERAP_FT12_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
10049 Evaluating Policy Group
10001 Evaluating Service Selection Policy
10041 Evaluating Identity Policy
10040 Queried PIP - Normalised Radius RadiusIofType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
10010 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user1
24212 Found User in Internal Users IDStore - user1
22037 Authentication Passed
24719 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
10030 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
10048 Queried PIP - Radius User-Name
10010 Selected Authorization Profile - StaticIPAddressUser1
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	StaticIPAddressUser1
Response Time	231 milliseconds

Other Attributes

ConfigVersionId	147
DestinationPort	1812
Protocol	Radius
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
MS-CHAPv2-Challenge	0F 4F 54 4F 45 0F 4F 55 4C 5D 57 1C 57 56 4B 0B
MS-CHAPv2-Response	00 00 00 00 40 20 44 45 4F 12 17 6A 20 6A 19 45 49 00 00 00 00 00 00 00 00 00 4F 29 52 30 5A 20 41 09 x7 50 3c f0 8a 73 32 a9 50 b4 27 5c 5d 99
CVPR3000ASAPOD7x-Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	90099005-3150-4215-a80e-6753645a056c
IsThirdPartyDeviceFlow	false
CVPR3000ASAPOD7x-Client-Type	2
Acx-Session-Id	driverap-ISE-0-71417494978-25
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

Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#All IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM Session ID	idba80064000a00001525a9
Called Station ID	192.168.0.100
CiscoAVPair	<pre> mgn-du#device:platform: mgn-du#device:mac-00:50:50:90:45:01 mgn-du#device:platform:version:10.0.18202 mgn-du#device:public-mac-00:50:50:90:45:01 mgn-du#device:agent:AnyConnect:Windows 4.10.0200 mgn-du#device:type:VMware, Inc. VMware Virtual Platform mgn-du#device:uid: gidba1158f888cc0f52f3f2c0e2431455f4baa2ae2c0b3 mgn-du#device: user-0584e37071f98782f816f124621184408986c717e37d988c200f 84A3CB8E2344 a:0:session-cpm-idba80064000a00001525a9 ip source-ip=192.168.0.101 008-pub#vise </pre>

Result	
Framed IP Address	10.0.50.101
Class	CACS idba80064000a00001525a9 avirap-ISE-2:7417494978:25
cisco-av-pair	profile-name#Windows10-Rotation
MS-CHAPv2-Success	00 53 30 33 30 33 40 33 30 37 30 34 42 43 45 32 33 40 41 31 39 37 37 32 44 45 39 30 39 44 41 35 37 31 36 44 35 41 43 45 43 41
LicenseType	Base license consumed

Session Events	
-----------------------	--

Opmerking: de opdracht voor verificatie op de testaaa-server gebruikt PP altijd om authenticatieverzoeken naar de RADIUS-server te verzenden, er is geen manier om de firewall te dwingen MS-CHAPv2 met deze opdracht te gebruiken.

Firepower# test AAA-server verificatie ISE_Server host 172.16.0.8 gebruikersnaam1 wachtwoord XXXXXX

INFORMATIE: Probeert de verificatietest naar IP-adres (172.16.0.8) (tijdelijke oplossing: 12 seconden)

INFORMATIE: Verificatiesucces

Opmerking: Wijzig geen tunnels-group PPP-eigenschappen via Flex-fig omdat dit geen effect heeft op de verificatieprotocollen die via RADIUS zijn onderhandeld voor AnyConnect VPN-verbindingen (SSL en IPsec).

tunnelgroep RA_VPN ppp-eigenschappen

geen authenticatiepagina

legalisatietak

Verificatie ms-chap-v1

geen authenticatie ms-chap-v2

geen authenticatie-eap-proxy

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

AanTD:

- **Straal verwijderen**

Op ISE:

- **RADIUS-live logbestanden**