

Configurare la VPN ad accesso remoto FTD con MSCHAPv2 su RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione di RSA VPN con autenticazione AAA/RADIUS tramite FMC](#)

[Configurazione di ISE per il supporto di MS-CHAPv2 come protocollo di autenticazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come abilitare il protocollo MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol versione 2) come metodo di autenticazione tramite Firepower Management Center (FMC) per client VPN ad accesso remoto con autenticazione RADIUS (Remote Authentication Dial-In User Service).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Identity Services Engine (ISE)
- Cisco AnyConnect Secure Mobility Client
- protocollo RADIUS

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per impostazione predefinita, il protocollo FTD utilizza il protocollo PAP (Password Authentication Protocol) come metodo di autenticazione con i server RADIUS per le connessioni VPN AnyConnect.

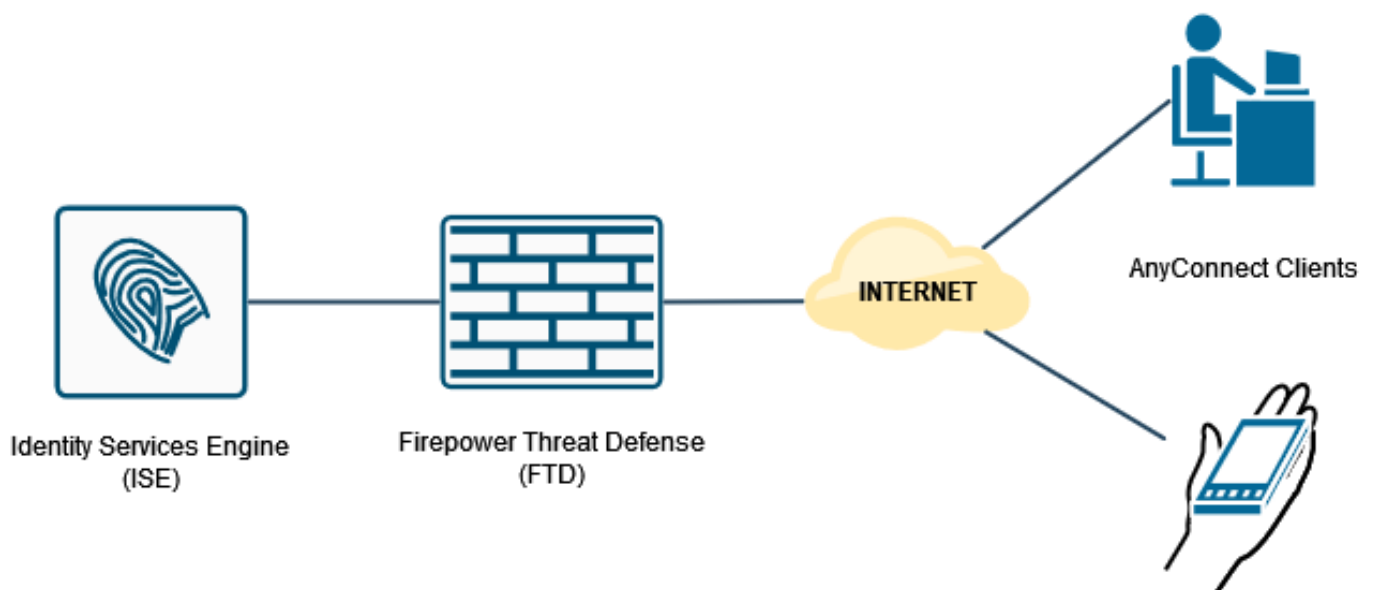
Il protocollo PAP fornisce agli utenti un metodo semplice per stabilire la propria identità con un handshake bidirezionale. La password PAP è crittografata con un segreto condiviso ed è il protocollo di autenticazione meno sofisticato. Il protocollo PAP non è un metodo di autenticazione avanzato in quanto offre una protezione ridotta da attacchi ripetuti di tipo prova ed errore.

L'autenticazione MS-CHAPv2 introduce l'autenticazione reciproca tra peer e una funzione di modifica della password.

Per abilitare MS-CHAPv2 come protocollo utilizzato tra l'ASA e il server RADIUS per una connessione VPN, è necessario abilitare la gestione delle password nel profilo di connessione. L'abilitazione della gestione delle password genera una richiesta di autenticazione MS-CHAPv2 da FTD al server RADIUS.

Configurazione

Esempio di rete

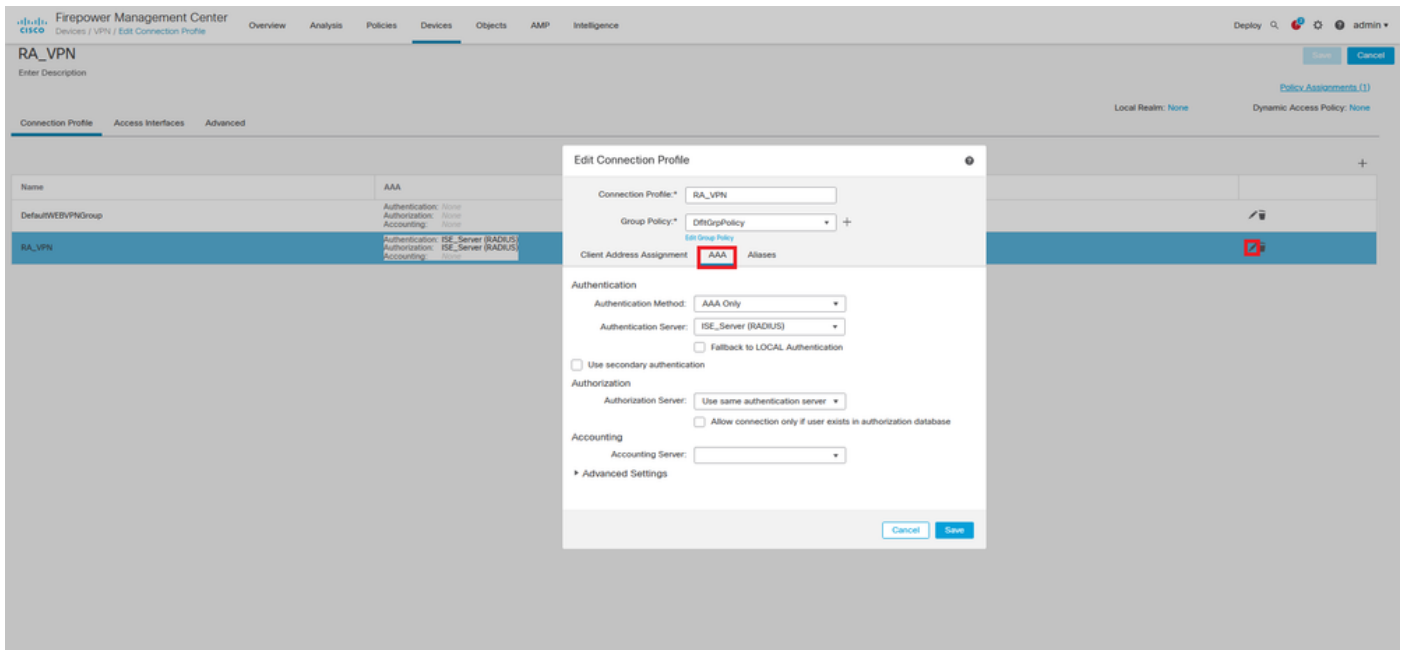


Configurazione di RSA VPN con autenticazione AAA/RADIUS tramite FMC

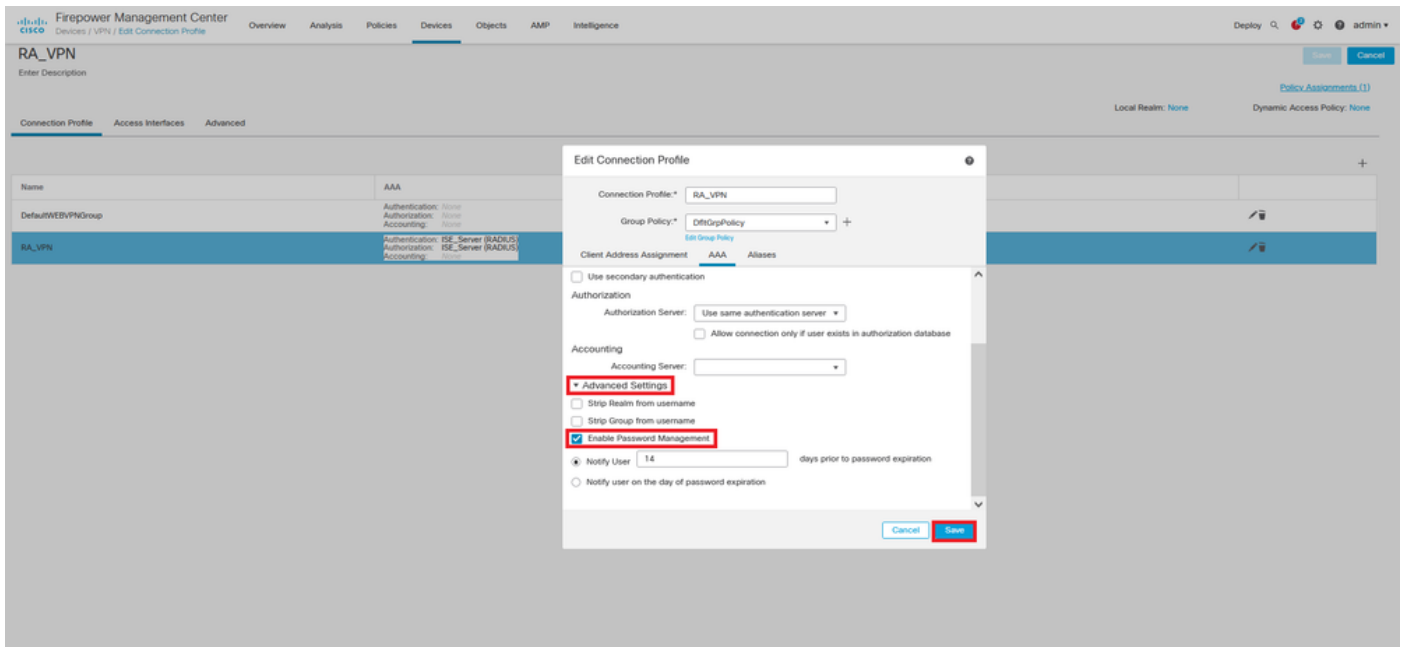
Per una procedura dettagliata, fare riferimento a questo documento e a questo video:

- [Configurazione VPN ad accesso remoto AnyConnect su FTD](#)
- [Configurazione iniziale di AnyConnect per FTD gestito da FMC](#)

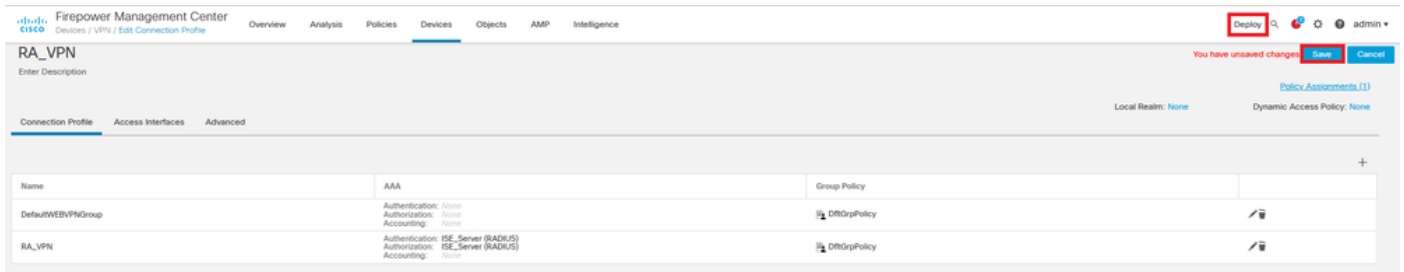
Passaggio 1. Una volta configurata la VPN ad accesso remoto, selezionare **Dispositivi > Accesso remoto**, modificare il profilo di connessione appena creato e passare alla scheda **AAA**.



Espandere la sezione **Impostazioni avanzate** e fare clic sulla casella di controllo **Abilita gestione password**. Fare clic su **Salva**.



Salvataggio e distribuzione.



La configurazione VPN ad accesso remoto nella CLI FTD è:

```
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

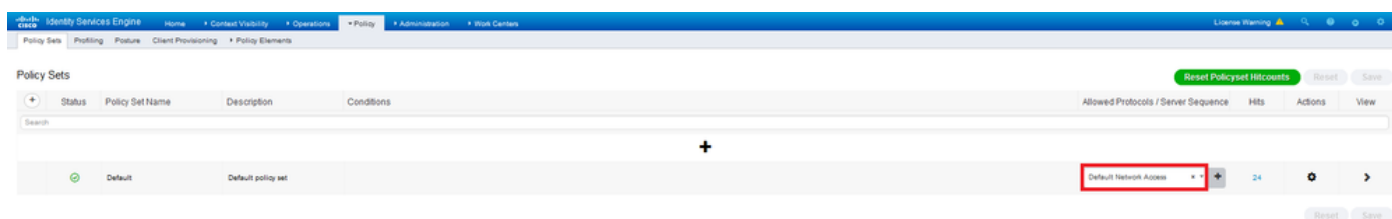
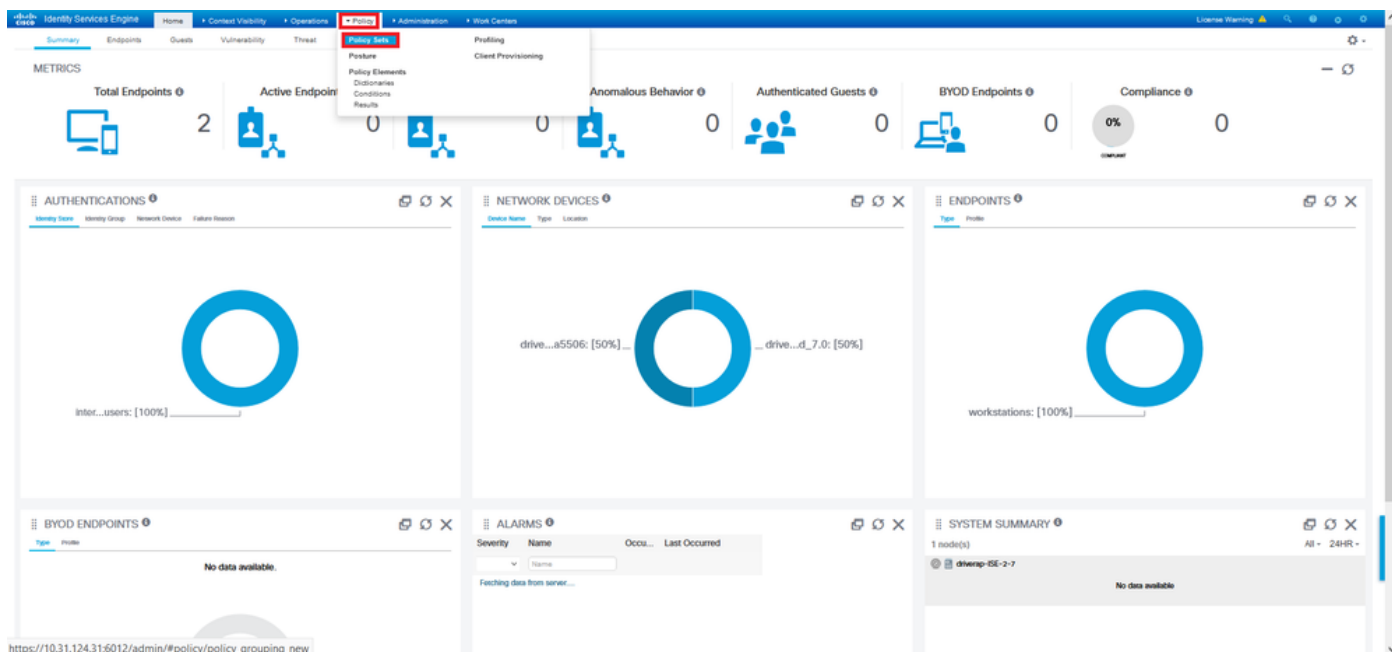
```
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

Configurazione di ISE per il supporto di MS-CHAPv2 come protocollo di autenticazione

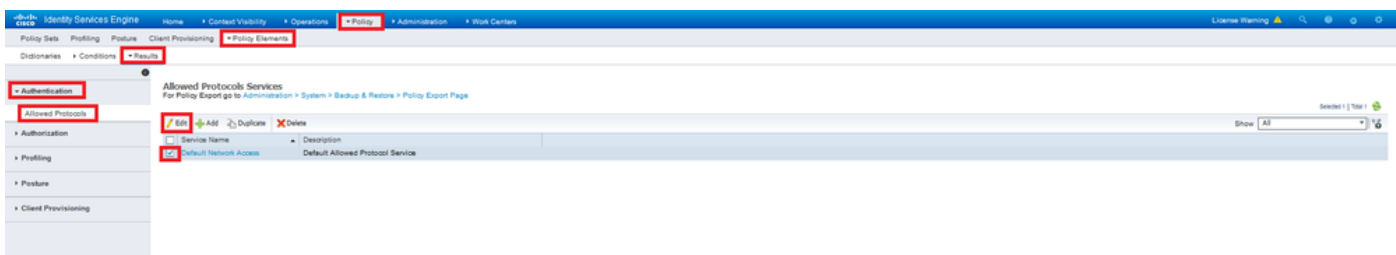
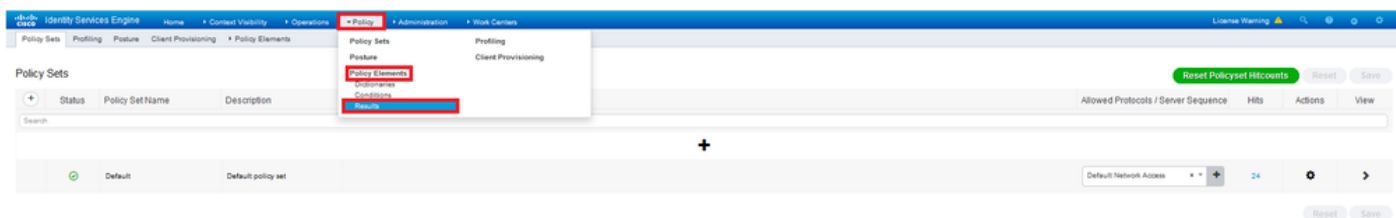
Si presume che:

1. L'FTD è già stato aggiunto come dispositivo di rete su ISE in modo che possa elaborare le richieste di accesso RADIUS dall'FTD.
2. Per autenticare il client AnyConnect, ISE può usare almeno un utente.

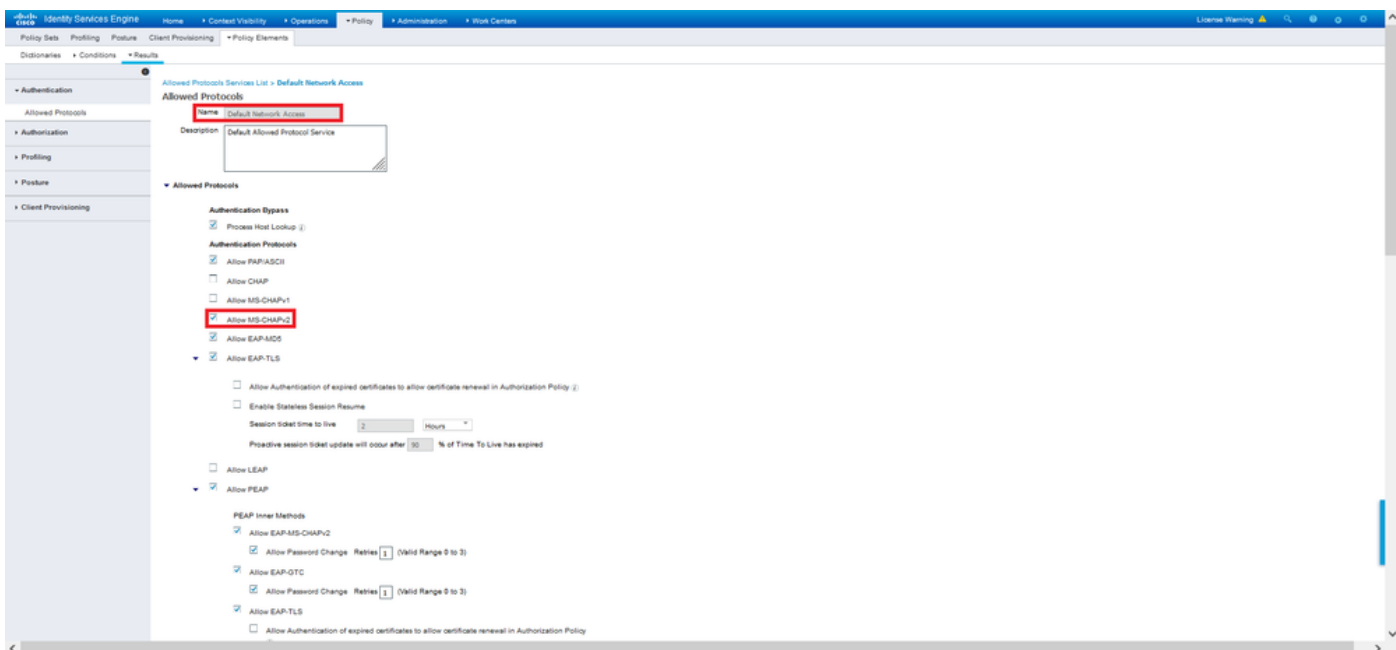
Passaggio 2. Passare a **Criterio > Set di criteri** e individuare il criterio **Protocolli autorizzati** associato al set di criteri in cui sono autenticati gli utenti AnyConnect. In questo esempio è presente un solo set di criteri, pertanto il criterio in questione è *Accesso di rete predefinito*.



Passaggio 3. Passare a **Criterio > Elementi criteri > Risultati**. In **Autenticazione > Protocolli consentiti** scegliere e modificare **Accesso alla rete predefinito**.

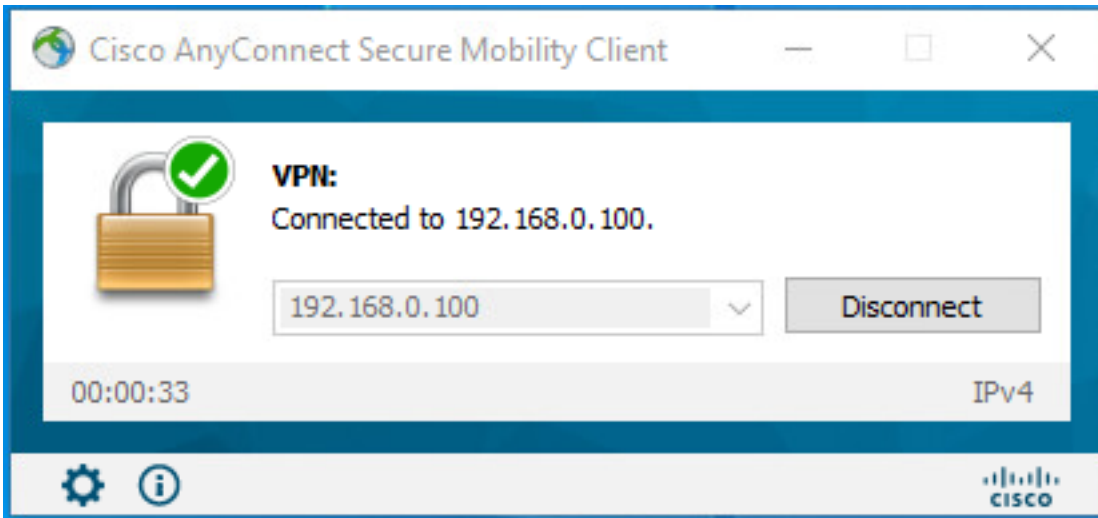


Verificare che la casella di controllo **Consenti MS-CHAPv2** sia selezionata. Scorri fino in fondo e salva.



Verifica

Passare al computer client in cui è installato il client Cisco AnyConnect Secure Mobility. Connettersi all'headend FTD (nell'esempio riportato viene utilizzato un computer Windows) e digitare le credenziali dell'utente.



I login RADIUS Live ad ISE mostrano:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:50:56:96:45:6F:0D
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:0D
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c9a30054000a50061525049
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
10043 Queried PIP - Normalised Radius RadiusIppType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
10013 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
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-CHAP-Challenge	0F 4F 54 4F 45 0F 4F 55 4C 5D 57 1C 57 56 4B 0B
MS-CHAP2-Response	00 00 00 00 40 20 44 45 4F 12 17 6A 20 6C 4F 19 45 4B 00 00 00 00 00 00 00 00 00 41 29 52 30 5A 20 41 09 47 50 3C 0E 8A 73 32 4B 50 54 27 00 54 99
CVR3000ASA/POX+ Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	9009905-3150-4215-a80e-6753645a056c
IsThirdPartyDeviceFlow	false
CVR3000ASA/POX+ Client-Type	2
Acx SessionID	driverap-ISE-0-71417494978-25
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISE Policy Set Name	Default
Identity Selection Matched Rule	Default
DTLS Support	Unknown
Host Identity Group	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
CPMSessionID	ida80064000a000e1525a9
Called Station ID	192.168.0.100
CiscoAVPair	m3m0u#device:platformmin m3m0u#device:macr00:50:50:50:45:01 m3m0u#device:platform:version10.0.18.202 m3m0u#device:publicmacr00:50:50:50:45:01 m3m0u#device:agent:AnyConnect@Windows 4 10 2208 m3m0u#device:oper#VMware, Inc. VMware Virtual Platform m3m0u#device:uid gidbaf158f885cc0f52f3f2c0e2431455f4bAA2AE2C0B3 m3m0u#device:u# user#C58483701F98782F816F124821184408986C717E37D188C200F 84A3CB8E2344 a:0:session-cpm#ida80064000a000e1525a9 ip source-ip#192.168.0.101 008-pub#vsa

Result	
Framed IP Address	10.0.50.101
Class	CACS ida80064000a000e1525a9@vswrap-ISE-2.7417494978/25
cisco-av-pair	profile-name#Windows10-Rotation
MS-CHAP2-Success	00 53 30 33 30 33 40 33 30 37 30 34 42 43 40 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	
-----------------------	--

Nota: il comando **test di autenticazione aaa-server** utilizza sempre PAP per inviare le richieste di autenticazione al server RADIUS. Non è possibile forzare il firewall a utilizzare MS-CHAPv2 con questo comando.

firepower# test di autenticazione aaa-server ISE_Server host 172.16.0.8 nomeutente user1 password XXXXXX

INFORMAZIONI: Tentativo di verifica dell'autenticazione sull'indirizzo IP (172.16.0.8) (timeout: 12 secondi)

INFORMAZIONI: Autenticazione riuscita

Nota: Non modificare gli attributi **ppp del gruppo di tunnel** tramite Flex-config perché non ha effetto sui protocolli di autenticazione negoziati su RADIUS per le connessioni AnyConnect VPN (SSL e IPsec).

tunnel-group RA_VPN ppp-attributes
nessuna pagina di autenticazione
autenticazione chap
autenticazione ms-chap-v1
nessuna autenticazione ms-chap-v2
nessuna autenticazione eap-proxy

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Su FTD

- debug radius all

ISE:

- Registri attivi RADIUS