使用MSCHAPv2通过RADIUS配置FTD远程访问VPN

目录

简介

本文档介绍如何通过Firepower管理中心(FMC)将Microsoft质询握手身份验证协议第2版(MS-CHAPv2)启用为身份验证方法，用于具有远程身份验证拨入用户服务(RADIUS)身份验证的远程访问VPN客户端。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower威胁防御(FTD)
- Firepower管理中心(FMC)
- 身份服务引擎 (ISE)
- Cisco AnyConnect 安全移动客户端
- RADIUS协议

使用的组件

本文档中的信息基于以下软件版本：

- FMCv - 7.0.0（内部版本94）
- FTDv - 7.0.0（内部版本94）
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086

- Windows 10专业版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

默认情况下，FTD使用密码身份验证协议(PAP)作为AnyConnect VPN连接的RADIUS服务器的身份验证方法。

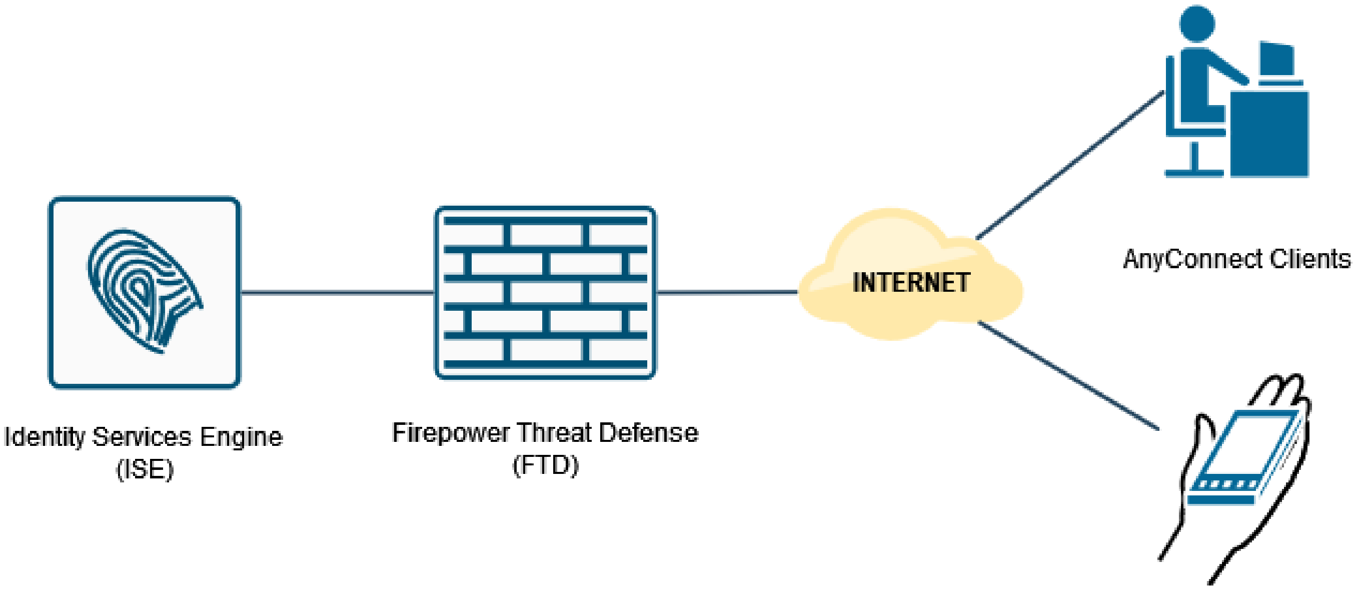
PAP为用户提供了一种简单的方法来通过双向握手建立其身份。PAP密码使用共享密钥加密，是最不完善的身份验证协议。PAP不是强身份验证方法，因为它几乎不能抵御反复的试错攻击。

MS-CHAPv2身份验证引入对等体之间的相互身份验证和更改密码功能。

要启用MS-CHAPv2作为ASA和RADIUS服务器之间用于VPN连接的协议，必须在连接配置文件中启用密码管理。启用密码管理会生成从FTD到RADIUS服务器的MS-CHAPv2身份验证请求。

配置

网络图

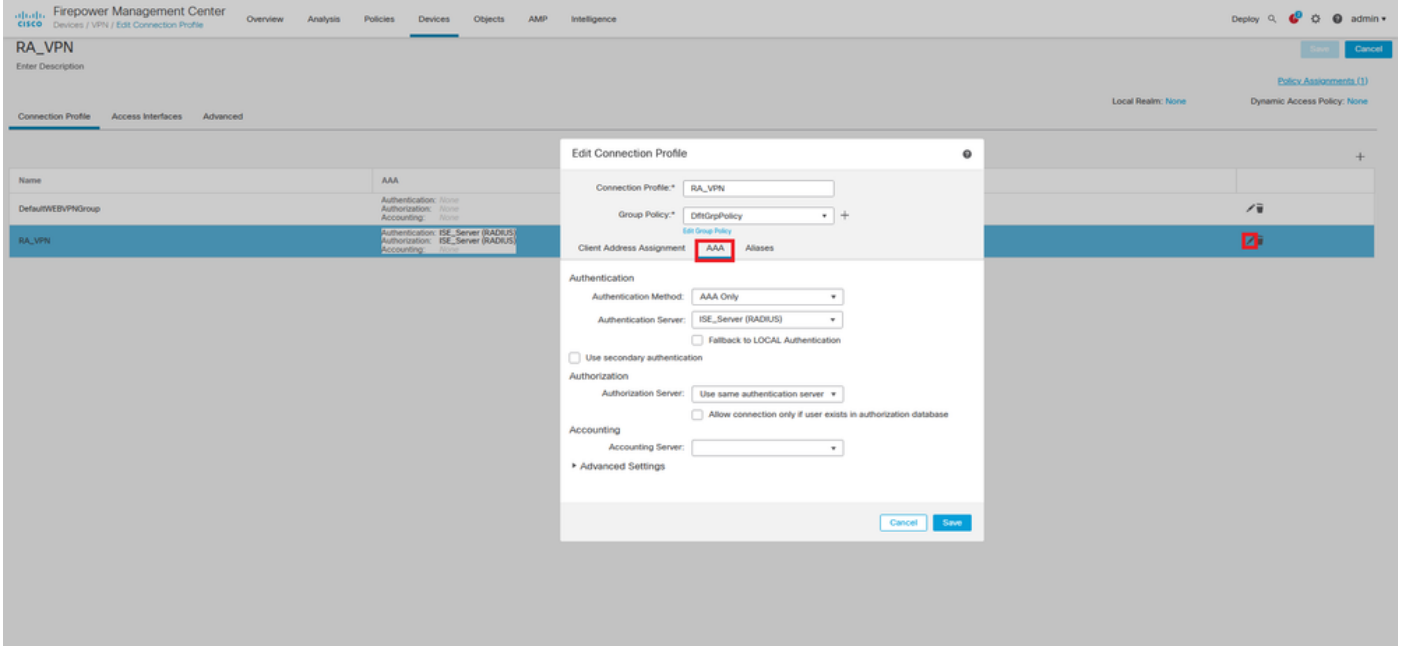


通过FMC配置RA VPN的AAA/RADIUS身份验证

有关分步过程，请参阅本文档和此视频：

- FTD上的AnyConnect远程访问VPN配置
- FTD的初始AnyConnect配置，由FMC管理

步骤1.配置Remote Access VPN后，导航至**Devices > Remote Access**，编辑新创建的连接配置文件，然后导航至**AAA选**项卡。



RA_VPN

Enter Description

Local Realm: None

Dynamic Access Policy: None

Name	AAA
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None

Edit Connection Profile

Connection Profile:* RA_VPN

Group Policy:* DfltGrpPolicy

Client Address Assignment | AAA | Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE_Server (RADIUS)

□ Fallback to LOCAL Authentication

□ Use secondary authentication

Authorization

Authorization Server: Use same authentication server

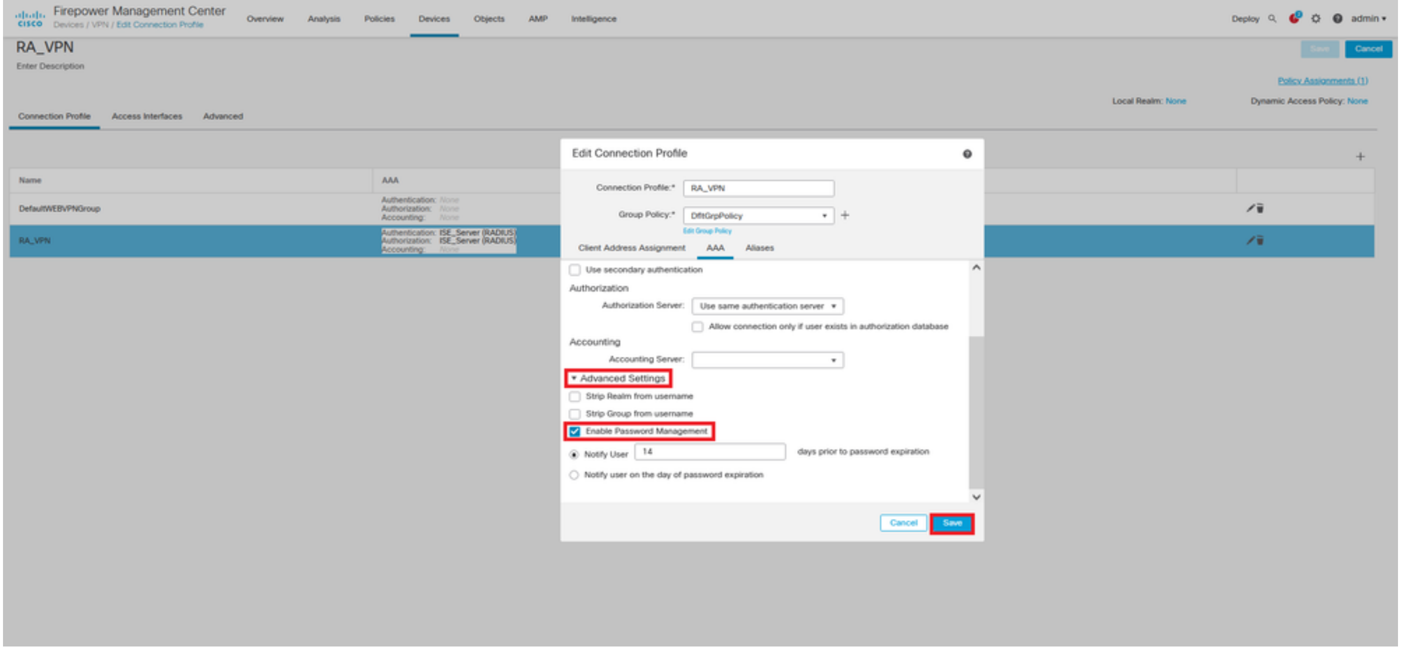
□ Allow connection only if user exists in authorization database

Accounting

Accounting Server:

▸ Advanced Settings

展开“高**级设置**”部分，然后单**击“启用密码**管理”复选框。Click **Save**.



Edit Connection Profile

Connection Profile:* RA_VPN

Group Policy:* DfltGrpPolicy

Client Address Assignment | AAA | Aliases

□ Use secondary authentication

Authorization

Authorization Server: Use same authentication server

□ Allow connection only if user exists in authorization database

Accounting

Accounting Server:

▾ Advanced Settings

□ Strip Realm from username

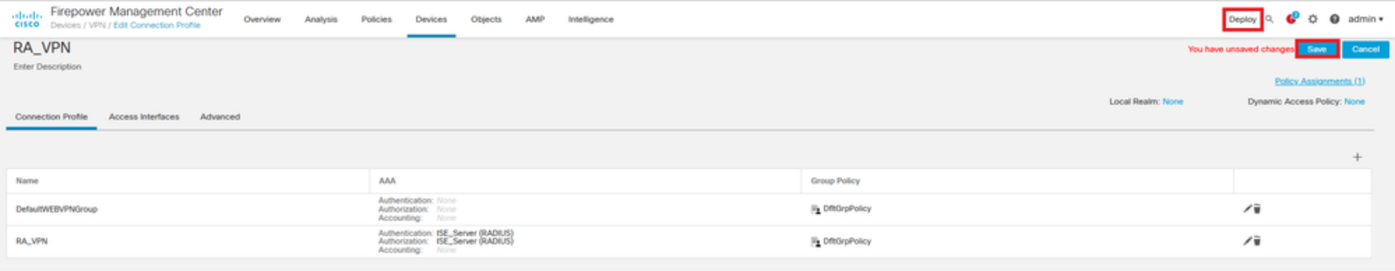
□ Strip Group from username

☑ Enable Password Management

● Notify User 14 days prior to password expiration

○ Notify user on the day of password expiration

保存并部署。



RA_VPN

Enter Description

You have unsaved changes

Local Realm: None

Dynamic Access Policy: None

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
RA_VPN	Authentication: ISE_Server (RADIUS) Authorization: ISE_Server (RADIUS) Accounting: None	DfltGrpPolicy

FTD CLI上的远程访问VPN配置为：

```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0

interface GigabitEthernet0/0
```

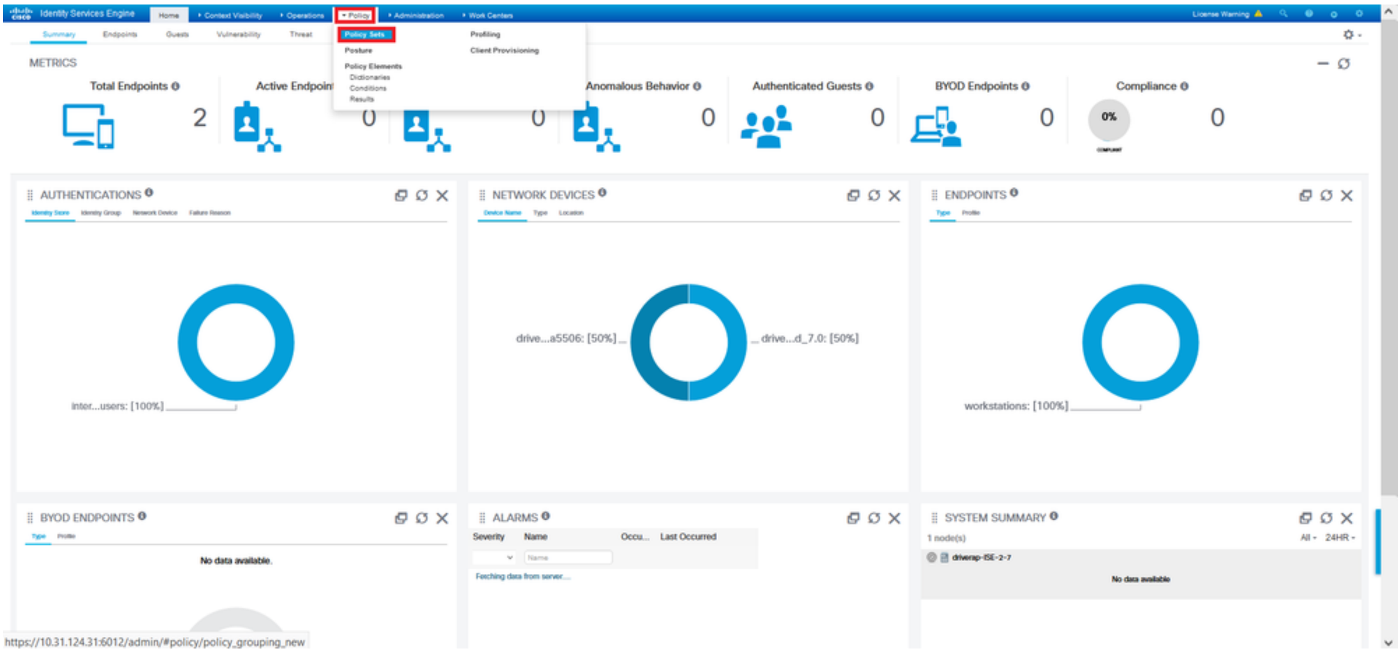
```
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0

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
```

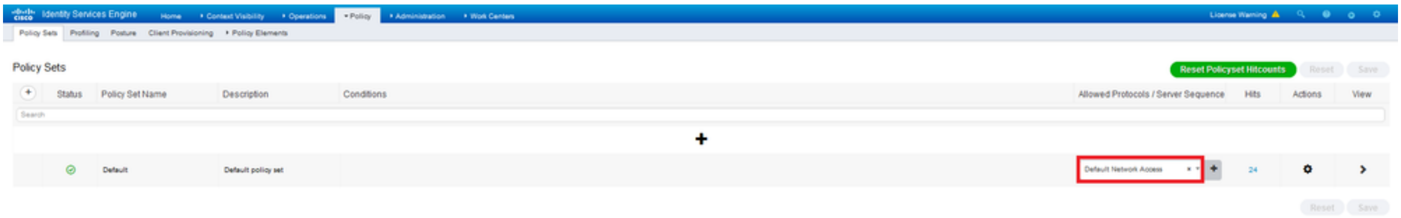
将ISE配置为支持MS-CHAPv2作为身份验证协议

假设：

1. FTD已添加为ISE上的网络设备，因此它可以处理来自FTD的RADIUS访问请求。
2. ISE至少有一个用户可用于验证AnyConnect客户端。

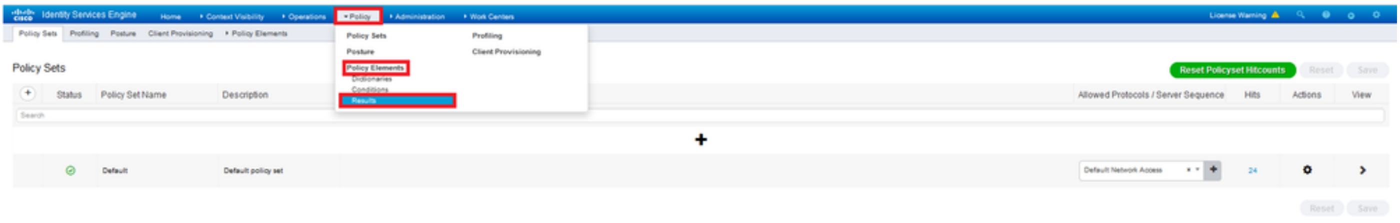
步骤2.导航至Policy **> Policy Sets**，并找到**Allowed Protocols** policy attached to Policy Set，在其中对AnyConnect用户进行身份验证。在本示例中，仅存在一个策略集，因此所讨论的策略是*默认网络访问*。

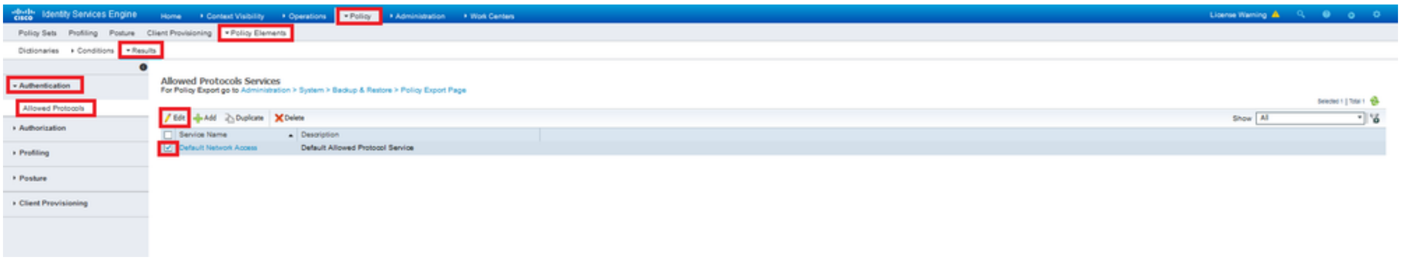




Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Default	Default policy set		Default Network Access	24	⚙	>

步骤3.导航至Policy > **Policy Elements > Results。**在Authentication > Allowed **Protocols下，选择并编辑Default Network Access。**

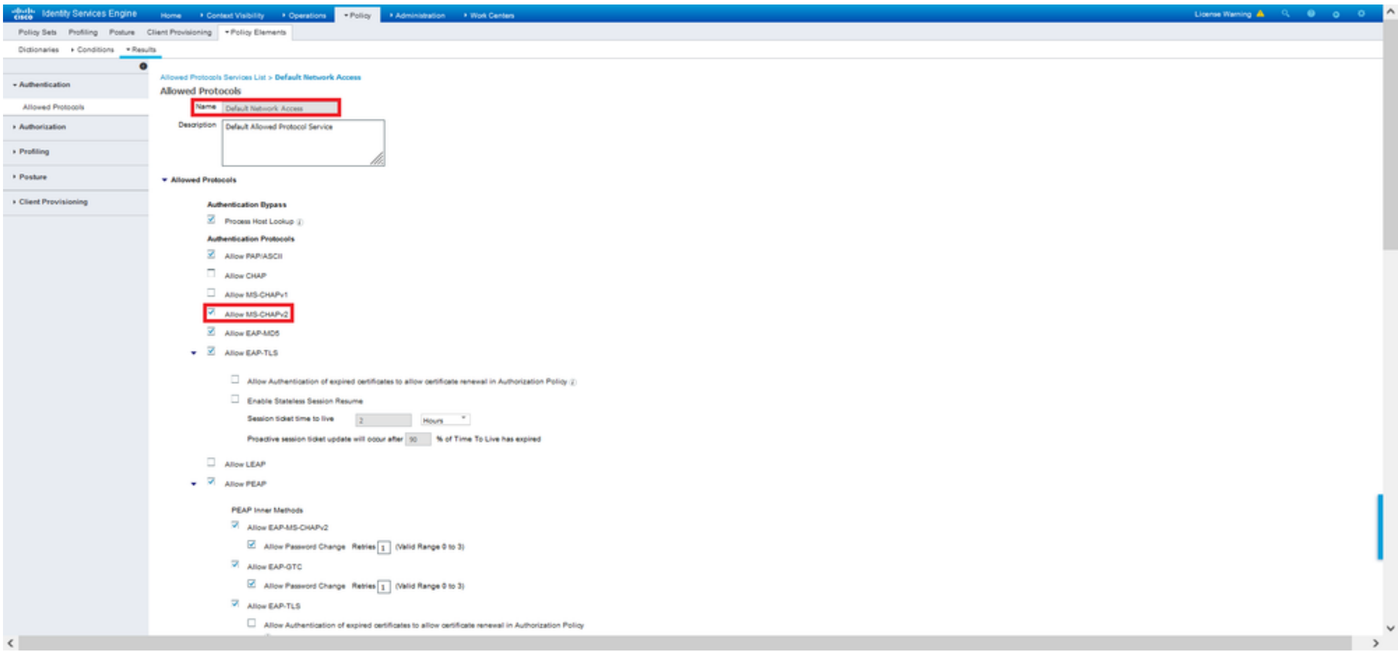




Allowed Protocols Services
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Service Name	Description
Default Network Access	Default Allowed Protocol Service

确保选中**“允许MS-CHAPv2”**复选框。向下滚动并**保存**。



Allowed Protocols Services List > **Default Network Access**

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

□ Allow CHAP

□ Allow MS-CHAPv1

☑ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

□ Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-GTC

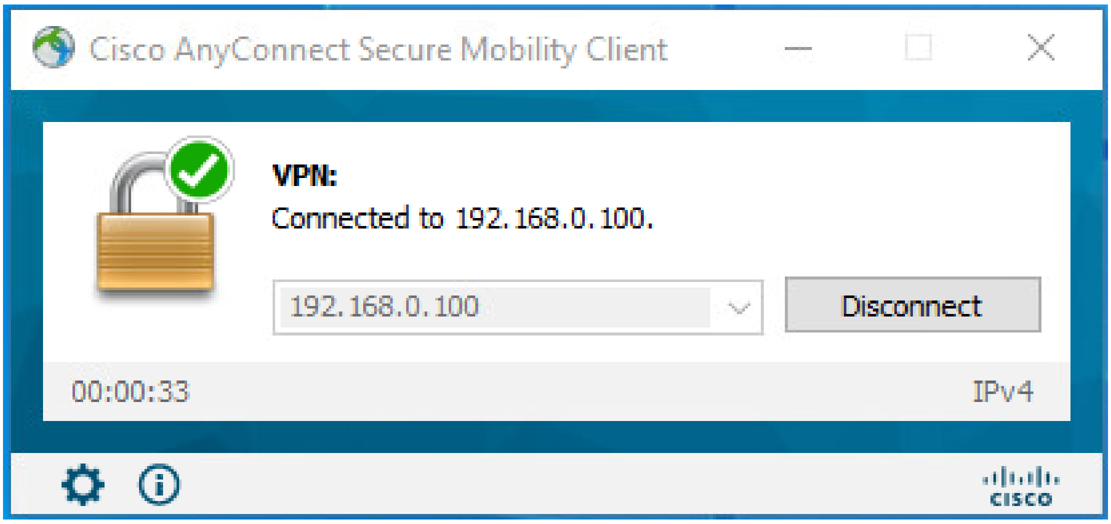
☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

验证

导航至安装Cisco AnyConnect安全移动客户端的客户端计算机。连接到FTD头端（本示例中使用Windows计算机）并键入用户凭证。



VPN:

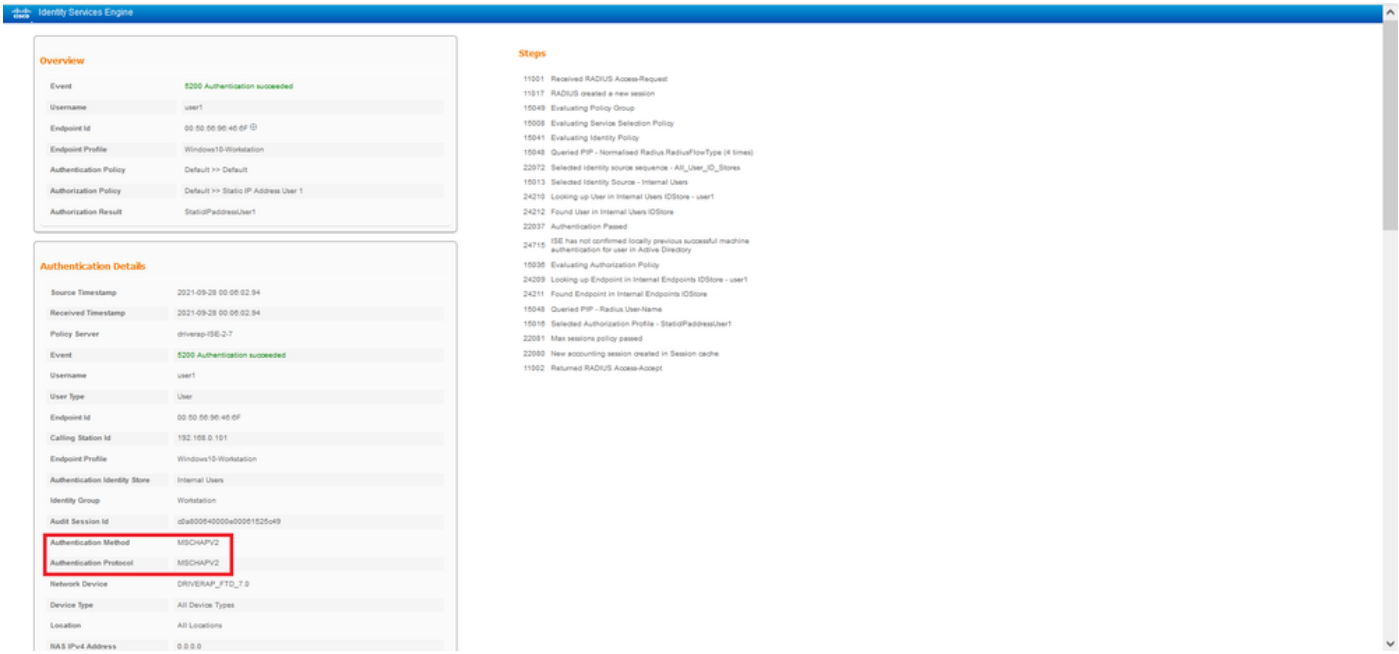
Connected to 192.168.0.100.

192.168.0.100

00:00:33

IPv4

ISE上的RADIUS实时日志显示：



Identity Services Engine

Overview

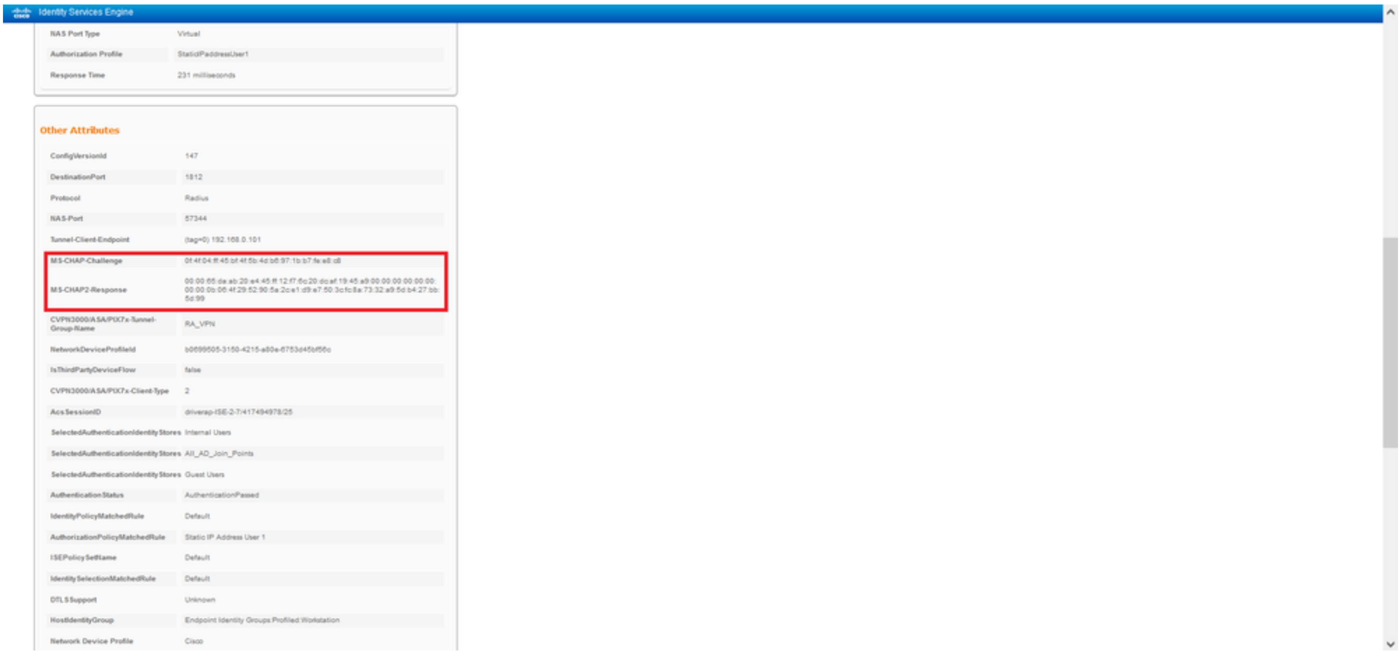
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:50:56:96:46:6F
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPaddressUser1

Authentication Details

Source Timestamp	2021-09-28 00:06:02.94
Received Timestamp	2021-09-28 00:06:02.94
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00:50:56:96:46:6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c0a800640000e00061525c49
Authentication Method	MSCHAPV2
Authentication Protocol	MSCHAPV2
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 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.RadiusFlowType (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 - user1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
24715	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
15048	Queried PIP - Radius.User-Name
15016	Selected Authorization Profile - StaticIPaddressUser1
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept

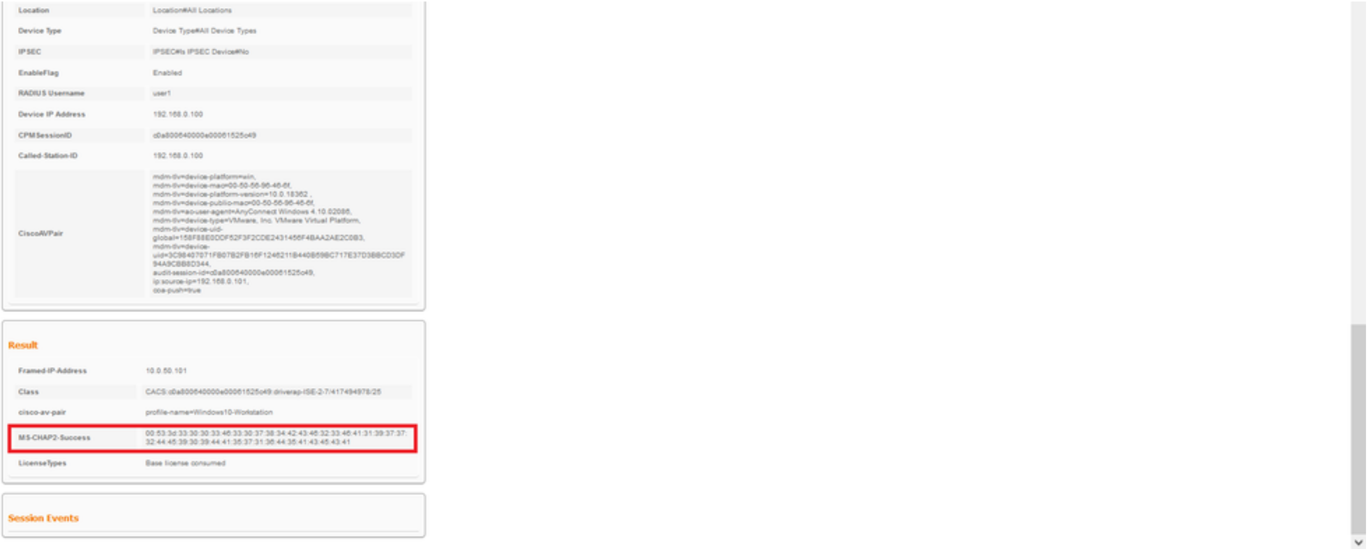


Identity Services Engine

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:04:ff:45:bf:4f:5b:4d:b6:97:1b:b7:fe:e8:c8
MS-CHAP2-Response	00:00:65:da:ab:20:e4:45:ff:12:f7:6c:20:dc:af:19:45:a9:00:00:00:00:00:00:00:00:0b:06:4f:29:52:90:5a:2c:e1:d9:e7:50:3c:fc:8a:73:32:a9:5d:b4:27:bb:5d:99
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/25
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled:Workstation
Network Device Profile	Cisco



Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPMSessionID	c0a800640000e00061525c49
Called-Station-ID	192.168.0.100

CiscoAVPair	mdm-tlv=device-platform=win,
	mdm-tlv=device-mac=00-50-56-96-46-6f,
	mdm-tlv=device-platform-version=10.0.18362 ,
	mdm-tlv=device-public-mac=00-50-56-96-46-6f,
	mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.02086,
	mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform,
	mdm-tlv=device-uid-global=158F88E0DDF52F3F2CDE2431456F4BAA2AE2C0B3,
	mdm-tlv=device-uid=3C98407071FB07B2FB16F1246211B440B598C717E37D3BBCD3DF94A9CBB8D344,
	audit-session-id=c0a800640000e00061525c49,
	ip:source-ip=192.168.0.101,
	coa-push=true

Result

Framed-IP-Address	10.0.50.101
Class	CACS:c0a800640000e00061525c49:driverap-ISE-2-7/417494978/25
cisco-av-pair	profile-name=Windows10-Workstation
MS-CHAP2-Success	00:53:3d:33:30:30:33:46:33:30:37:38:34:42:43:46:32:33:46:41:31:39:37:37:32:44:45:39:30:39:44:41:35:37:31:36:44:35:41:43:45:43:41
LicenseTypes	Base license consumed

Session Events

注意：test aaa-server authentication命令始终使用PAP向RADIUS服务器发送身份验证请求

，无法强制防火墙使用此命令使用MS-CHAPv2。

```
firepower# test aaa-server authentication ISE_Server host 172.16.0.8 username user1
password XXXXX
信息：尝试对IP地址(172.16.0.8)进行身份验证测试(超时：12 秒)
信息：身份验证成功
```

注意：请勿通过**Flex-config修改隧道组ppp-attributes**，因为这对通过RADIUS协商的AnyConnect VPN（SSL和IPSec）连接的身份验证协议没有影响。

```
tunnel-group RA_VPN ppp-attributes
 no authentication pap
 身份验证CHAP
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

故障排除

本节提供可用于排除配置故障的信息。

在F上TD:

- **debug radius all**

在ISE上：

- RADIUS实时日志