

H3Cアクセスコントローラ

Microsoft NPSサーバーによるアクセス認証の構成例

Copyright©2022 New H3C Technologies Co.,Ltd.無断転載を禁ず。

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の承諾なく、いかなる形式または手段によっても複製または譲渡することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登録商標です。

このドキュメントの情報は、予告なしに変更されることがあります。

内容

はじめに	3
使用されているソフトウェアバージョン.....	3
例:NPS認証サーバーを使用したポータル認証の構成.....	3
ネットワーク構成	3
制約事項とガイドライン.....	4
手順	4
設定の確認.....	19
構成ファイル	20

はじめに

次の情報では、Microsoft NPSの認証サーバーソフトウェアを使用してワイヤレスクライアントを認証するようにH3Cアクセスコントローラーを構成する例を示します。この例には、Microsoft NPSベースのポータル認証および承認ACL割り当ての構成が含まれます。

使用されているソフトウェアバージョン

次の設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されたものです。

- AC:R5435P03を実行するvAC。
- NPS認証サーバー:Windows Server 2016 NPSコンポーネント。
- iMCサーバー:iMC PLAT 7.3(E0706P03)およびiMC 7.3(E0620)を実行するサーバー。

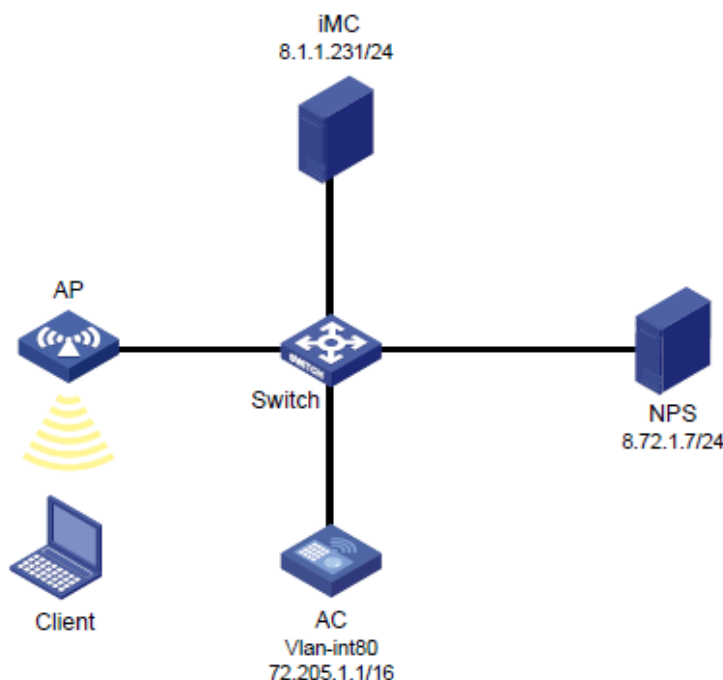
例:NPS認証サーバーを使用したポータル認証の構成

ネットワーク構成

図1に示すように、APIはスイッチを介してACに接続され、クライアントはAPを介してワイヤレスネットワークにアクセスします。

直接ポータル認証を構成して、クライアントのネットワークリソースへのアクセスを制御します。NPSサーバーをRADIUSサーバーとして使用し、iMCサーバーをポータルサーバーとして使用します。

図1 ネットワーク図



制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。

手順

ACの設定

1. RADIUSスキームを構成します。

#RADIUSスキームnpsを作成します。

```
<AC> system-view
```

```
[AC] radius scheme nps
```

#NPSサーバーをプライマリ認証およびアカウントングサーバーとして指定し、サーバーとの安全な通信のための共有キーを指定します。共有キーが、NPSサーバーで構成されている共有シークレットと同じであることを確認してください。

```
[AC-radius-nps] primary authentication 8.72.1.7 key simple 12345678
```

```
[AC-radius-nps] primary accounting 8.72.1.7 key simple 12345678
```

#NPSサーバーに送信されるユーザー名からドメイン名を除外します。

```
[AC-radius-nps] user-name-format without-domain
```

```
[AC-radius-nps] quit
```

2. ISPDメインを構成します。

#ISPDメインポータルを作成します。

```
[AC] domain portal
```

#ユーザー認証、承認、およびアカウントングの既定の方法としてRADIUSスキームnpsを使用するようにISPDメインを構成します。

```
[AC-isp-portal] authentication portal radius-scheme nps
```

```
[AC-isp-portal] authorization portal radius-scheme nps
```

```
[AC-isp-portal] accounting portal radius-scheme nps
```

```
[AC-isp-portal] quit
```

3. ポータル認証を設定します。

#ポータル認証サーバー名をimc、IPアドレスをIMCサーバーのIPアドレス、キーをプレーンテキストのポータルとして設定します。

```
[AC] portal server imc
```

```
[AC-portal-server-imc] ip 8.1.1.231 key simple portal
```

```
[AC-portal-server-imc] quit
```

#ポータルWebサーバーのURLをhttp://8.1.1.231:8080/portal/として構成します。(実際のポータルWebサーバーのURLを指定してください。)

```
[AC] portal web-server imc
```

```
[AC-portal-websvr-imc] url http://8.1.1.231:8080/portal/
```

```

[AC-portal-websvr-imc] quit
#サービステンプレートポータルを作成します。
[AC] wlan service-template portal
#サービステンプレートのSSIDを指定します。
[AC-wlan-st-portal] ssid portal_nps
#サービステンプレートで直接ポータル認証を有効にします。
[AC-wlan-st-portal] portal enable method direct
#サービステンプレートでポータルWebサーバーimcを指定します。
[AC-wlan-st-portal] portal apply web-server imc
#サービステンプレートで認証ドメインポータルを指定します。
[AC-wlan-st-portal] portal domain portal
#サービステンプレートを有効にします。
[AC-wlan-st-portal] service-template enable
[AC-wlan-st-portal] quit
#ap1という名前の手動APを設定し、そのモデルとシリアルIDを指定します。
[AC] wlan ap ap1 model WA6638-JP
[AC-wlan-ap-ap1] serial-id 219801A24F8198E0001G
[AC-wlan-ap-ap1] quit
#radio 1を有効にし、サービステンプレートポータルとVLAN 80を無線にバインドします。
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template portal vlan 80
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit

```

4. ACL 3999を設定します(必要に応じてACLを設定します)。

```

[AC] acl advanced 3999
[AC-acl-ipv4-adv-3999] rule 0 permit ip
[AC-acl-ipv4-adv-3999] quit

```

5. ACでDHCPサービスをイネーブルにし、DHCPアドレスプールを作成してクライアントにIPアドレスを割り当てます。

#VLAN 80とVLAN-interface 80を作成します。VLANインターフェイスにIPアドレス72.205.1.1とサブネットマスク255.255.0.0を割り当てます。

```

[AC] vlan 80
[AC-vlan80] quit
[AC] interface Vlan-interface 80
[AC-Vlan-interface80] ip address 72.205.1.1 255.255.0.0

```

```
[AC-Vlan-interface80] quit
#DHCPサービスを有効にします。

[AC] dhcp enable
#80という名前のDHCPアドレスプールを作成します。

[AC] dhcp server ip-pool 80
[AC-dhcp-pool-80] quit
#DHCPアドレスプールで、動的割り当てのサブネットを72.205.0.0/16に指定します。

[AC-dhcp-pool-80] network 72.205.0.0 mask 255.255.0.0
#DHCPアドレスプールでゲートウェイアドレスを72.205.1.1として指定します。

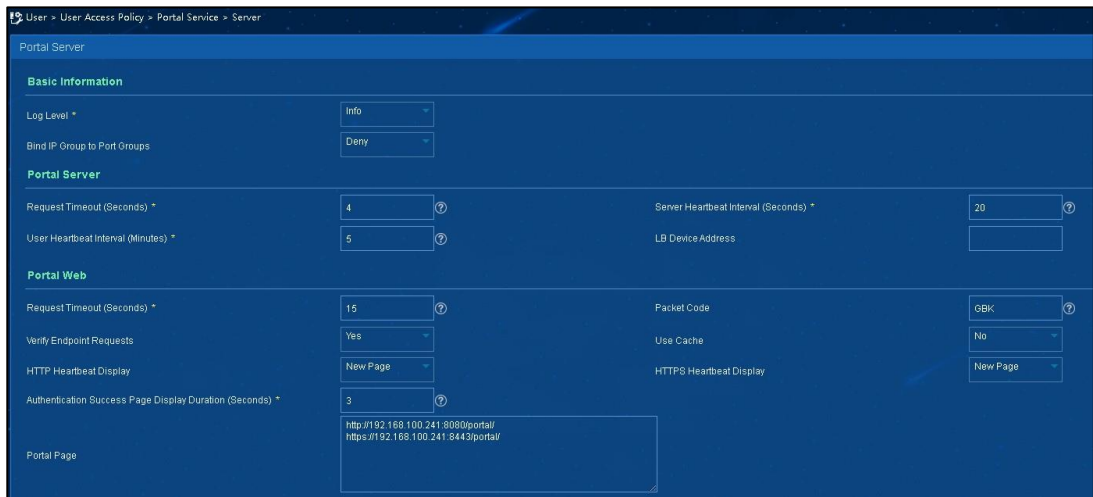
[AC-dhcp-pool-80] gateway-list 72.205.1.1
#DHCPアドレスプールでDNSサーバアドレスを72.205.1.1として指定します。

[AC-dhcp-pool-80] dns-list 72.205.1.1
[AC-dhcp-pool-80] quit
```

IMCサーバー(ポータルサーバー)の設定

1. ポータルサーバーを構成します。
 - a. IMCにログインし、**User**タブをクリックします。
 - b. 図2に示すように、ナビゲーションツリーから**User Access Policy > Portal Service > Server**を選択して、ポータルサーバー構成ページを開きます。
 - c. 必要に応じてポータルサーバーのパラメーターを構成します。
 - d. **OK**をクリックします。

図2 ポータルサーバーの構成



2. IPアドレスグループを設定します。
 - a. ナビゲーションツリーから**User Access Policy > Portal Service > IP Group**を選択して、ポータルIPアドレスグループの設定ページを開きます。
 - b. **Add**をクリックすると、図3のようなページが開きます。
 - c. IPグループの開始IPアドレスと終了IPアドレスを入力します。クライアントIPアドレスがIPグループ内にあることを確認します。

- d. サービスグループを選択します。
この例では、既定のグループ**Ungrouped**を使用します。
- e. **Action**リストから**Normal**を選択します。
- f. **OK**をクリックします。

図3 IPアドレスグループの追加

3. ポータルデバイスを追加します。
 - a. ナビゲーションツリーから**User Access Policy > Portal Service > Device**を選択して、ポータルデバイス設定ページを開きます。
 - b. **Add**をクリックすると、図4のようなページが開きます。
 - c. デバイス名(ACの名前)を入力します。
 - d. ポータルサーバーと情報を交換するACのインターフェイスのIPアドレスを入力します。
 - e. キーを入力します。このキーは、ACに設定されているキーと同じである必要があります。この例では、**Portal**です。
 - f. **Access Method**リストから **Directly Connected**を選択します。
 - g. 他のパラメータには既定の設定を使用します。
 - h. **OK**をクリックします。

図4 ポータルデバイスの追加

4. ポータルデバイスをIPアドレスグループに関連付けます。
 - a. 図5に示すように、デバイスの**Port Group Information Management**アイコンをクリック

して、ポートグループ設定ページを開きます。

b. 図6に示すように、**Add**をクリックしてページを開きます。

c. ポートグループ名を入力します。

d. 設定されたIPアドレスグループを選択します。

ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ内にある必要があります。

e. 他のパラメータには既定の設定を使用します。

f. **OK**をクリックします。

図5 Devicelist

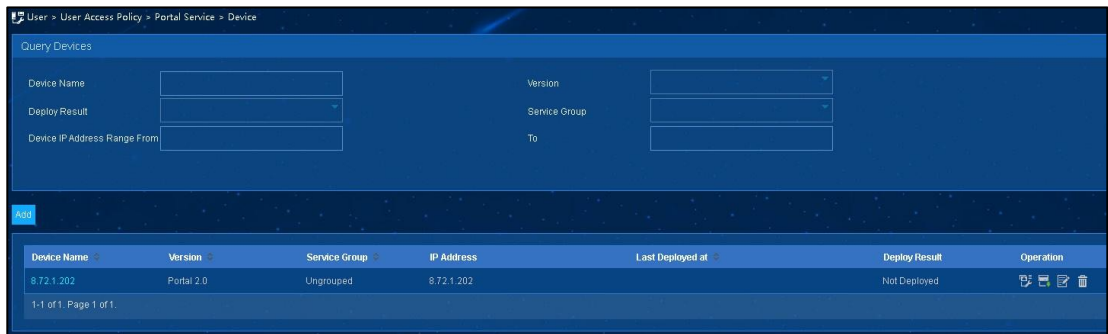
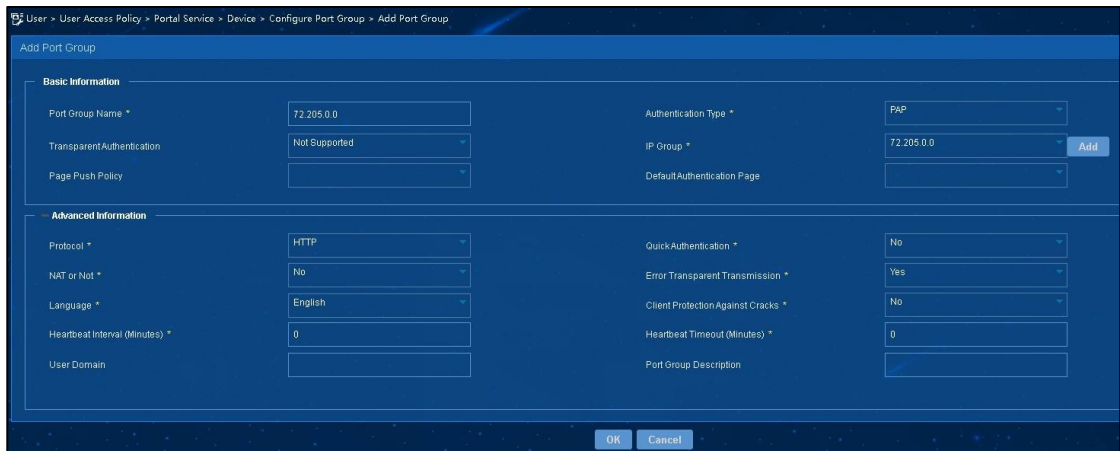


図6 ポートグループの追加



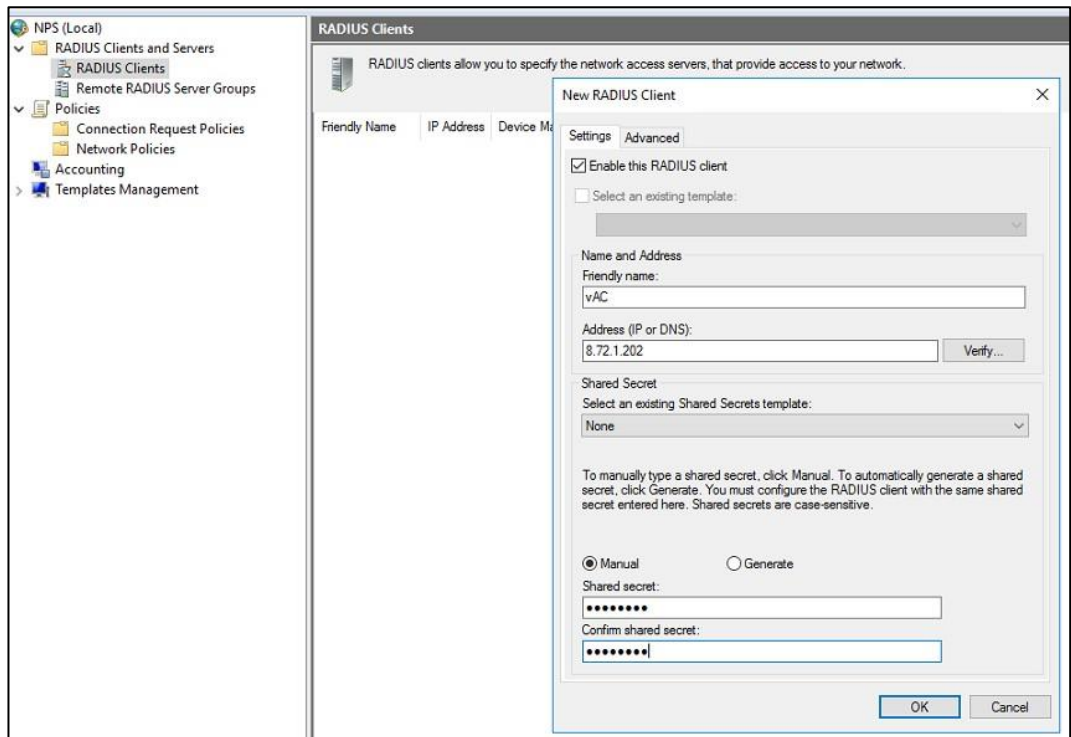
NPSサーバー(RADIUSサーバー)を構成する

1. RADIUSクライアントを設定します。

a. ネットワークポリシーサーバー(NPS)コンポーネントを開きます。左側のナビゲーションペインで **RADIUS Client and Servers > RADIUS Clients** を選択します。

b. 新しいRADIUSクライアントの追加: **Address(IP or DNS)**フィールドにACのIPアドレスを入力します。共有秘密を入力します。共有秘密は、プライマリ認証およびアカウントングサーバーに設定されている共有キーと同じである必要があります。この例では、共有秘密は**12345678**です。

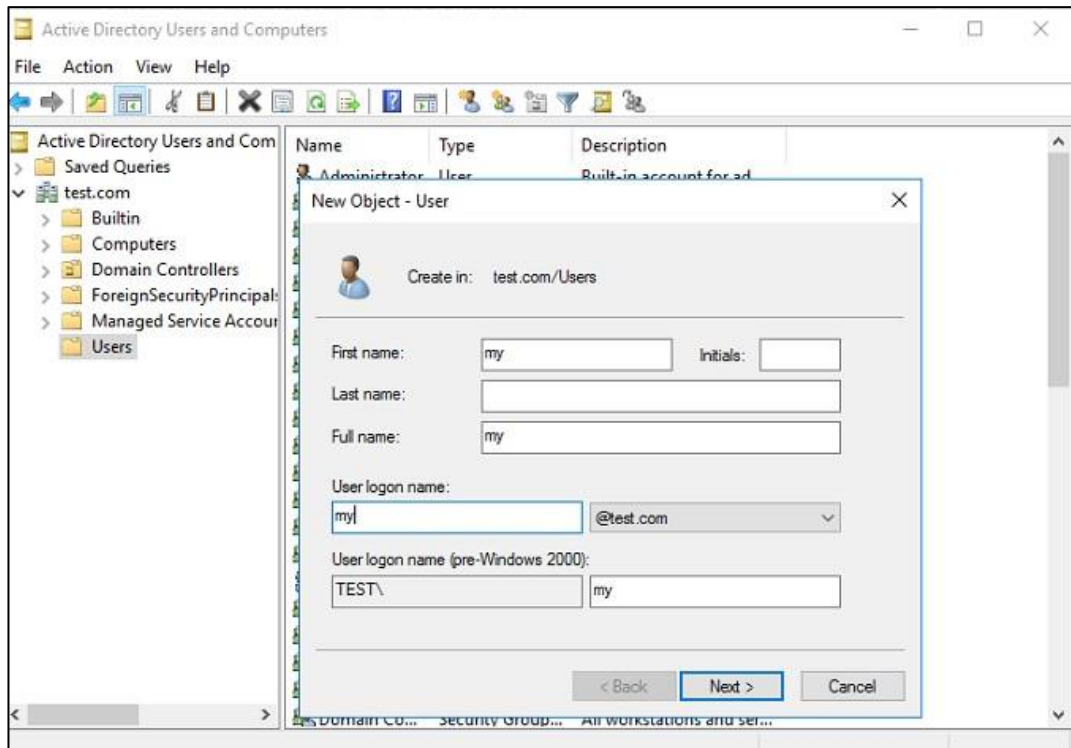
図7 RADIUSクライアントの作成



2. ユーザーの作成:

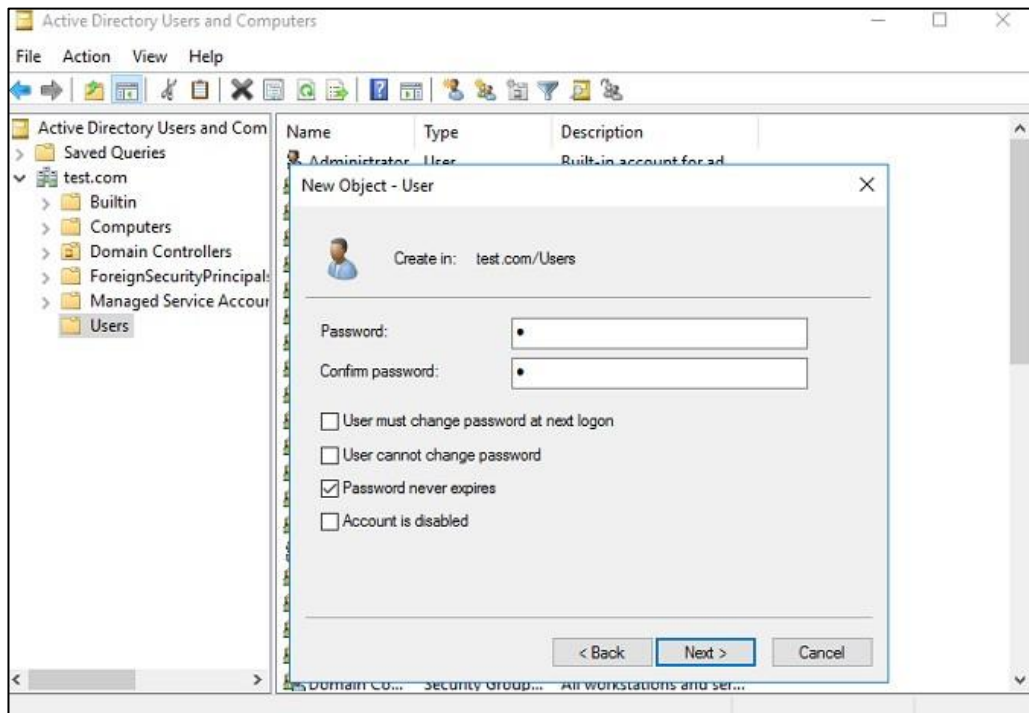
- a. Active Directory Users and Computersコンポーネントを開きます。Usersディレクトリを選択して右クリックし、新しいユーザーを追加します。
- b. ユーザー名をmyに設定し、Nextをクリックします。

図8ユーザーの作成



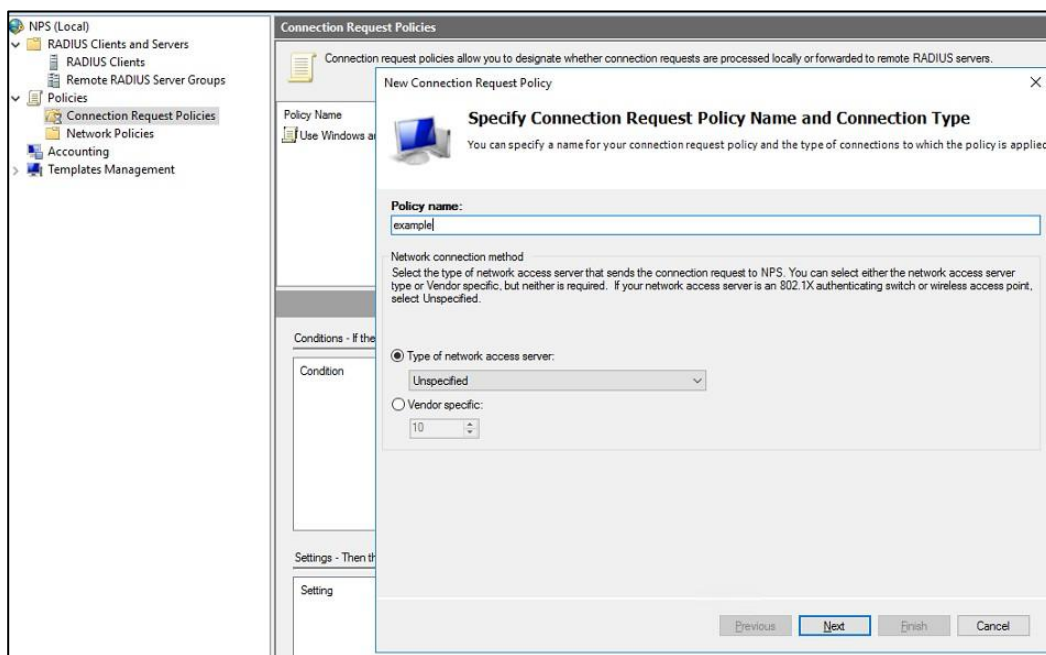
- c. ユーザーパスワードを構成し、**Password never expires**を選択します。
Nextをクリックします。

図9ユーザーパスワードの構成



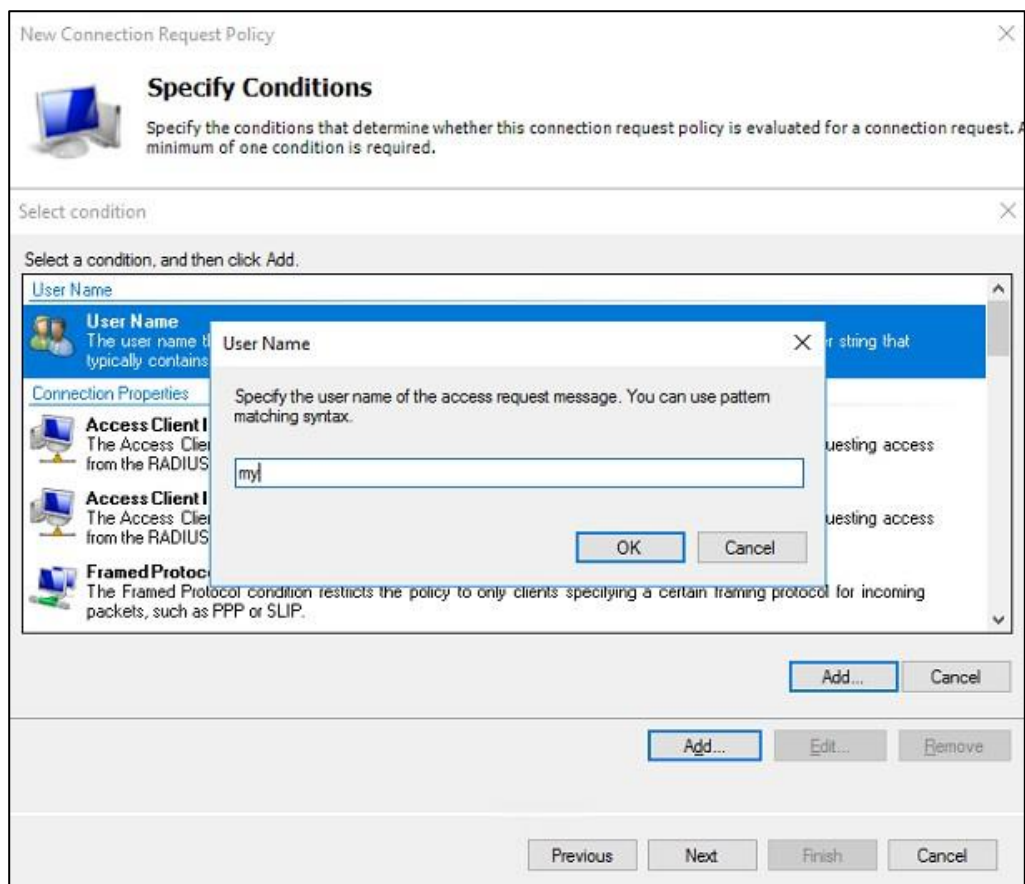
3. 接続要求ポリシーを構成します。
- a. 新しい接続要求ポリシーを追加します。
#NPSコンポーネントを開きます。ナビゲーションペインで、**Policies > Connection Request Policy**を選択します。
#request policyを追加します。ポリシー名を設定し、他のオプションにはデフォルト設定を使用して、**Next**をクリックします。

図10 接続要求ポリシーの作成



- b. **Add a user name:** Specify Conditions ページで User Name を選択し、Add をクリックして、前の手順で追加した RADIUS ユーザーを接続リクエストポリシーに追加します。OK をクリックします。

図11 ユーザー名の追加



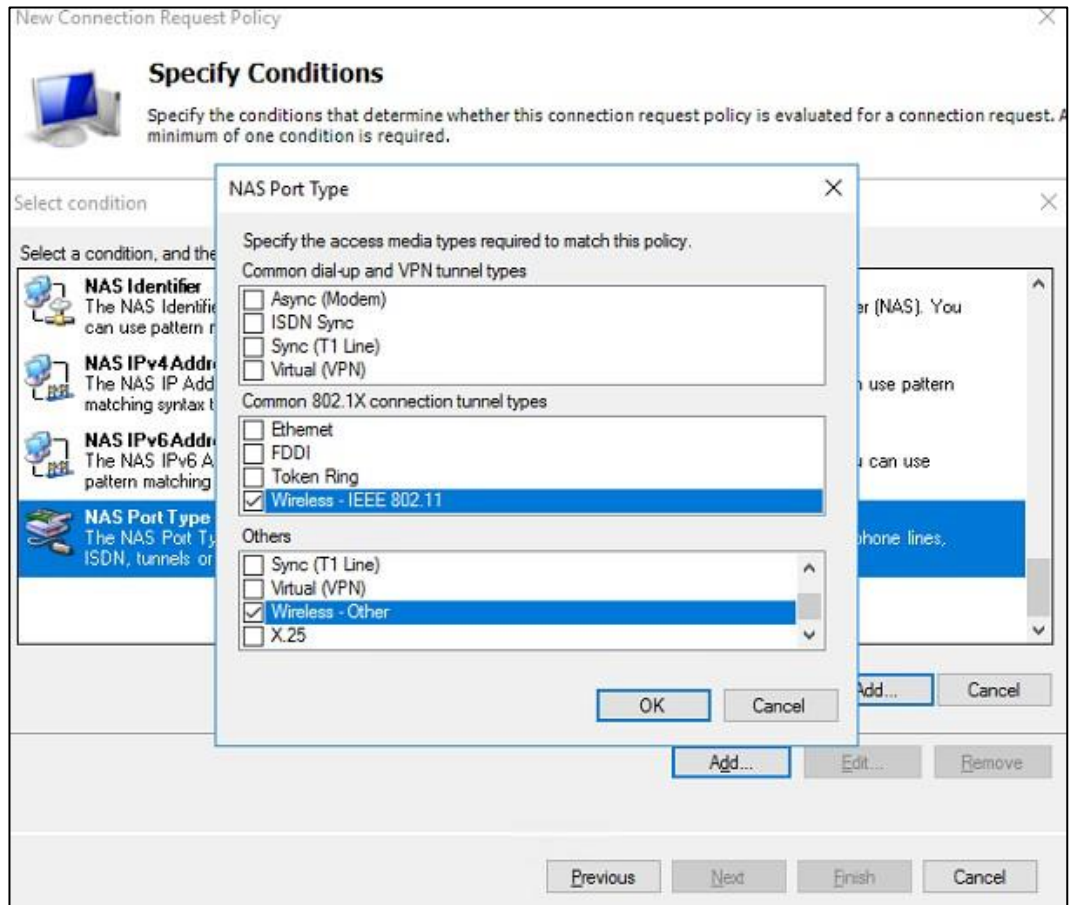
c. NASポートタイプを構成します。

Specify Conditionsページの下部で、**NAS Port Type**を選択し選択したタイプを接続要求ポリシーに追加します。

#**Common 802.1X connection tunnel types**領域で、**Wireless IEEE-802.11**を選択します。**Others**領域で、**Wireless-Other**を選択します。

#**OK**をクリックします。

図12 NASポートタイプの構成



#**Next**をクリックして、**Connection Request Forwarding**ページを開きます。

d. ID認証の場所を設定します。

Connection Request Forwardingページで、**Authentication**を選択し、**Authenticate requests on this server**を選択します。

図13 ID認証ロケーションの構成

The screenshot shows a Windows wizard window titled "New Connection Request Policy". The main heading is "Specify Connection Request Forwarding". Below the heading, there is a sub-heading "Forwarding Connection Request" and a description: "The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group." Below this, a note states: "If the policy conditions match the connection request, these settings are applied." The "Settings:" section is divided into two panes. The left pane, titled "Forwarding Connection Request", has two items: "Authentication" (selected with a blue bar and a right-pointing arrow) and "Accounting". The right pane contains the following text: "Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication." There are three radio button options: 1. "Authenticate requests on this server" (selected with a filled circle). 2. "Forward requests to the following remote RADIUS server group for authentication:" (unselected). Below this option is a dropdown menu showing "<not configured>" and a "New..." button. 3. "Accept users without validating credentials" (unselected). At the bottom of the wizard, there are four buttons: "Previous", "Next" (highlighted with a blue border), "Finish", and "Cancel".

#Nextをクリックして、Authentication Methodsページを開きます。

e. 認証方式を指定します。

#EAP Typesボックスで、Protected EAP(PEAP)とSecured password(EAP-MSCHAP v2)を追加します。

#Less secure authentication methods領域で、Microsoft Encrypted Authentication version 2(MS-CHAP-v2)、Microsoft Encrypted Authentication(MS-CHAP)、Encrypted Authentication(CHAP)、Unencrypted Authentication(PAP.SPAP)、およびAllow clients to connect without negotiating an authentication methodを選択します。

図14 認証方式の指定

New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

Override network policy authentication settings
These authentication settings are used rather than the constraints and authentication settings in network policy.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method

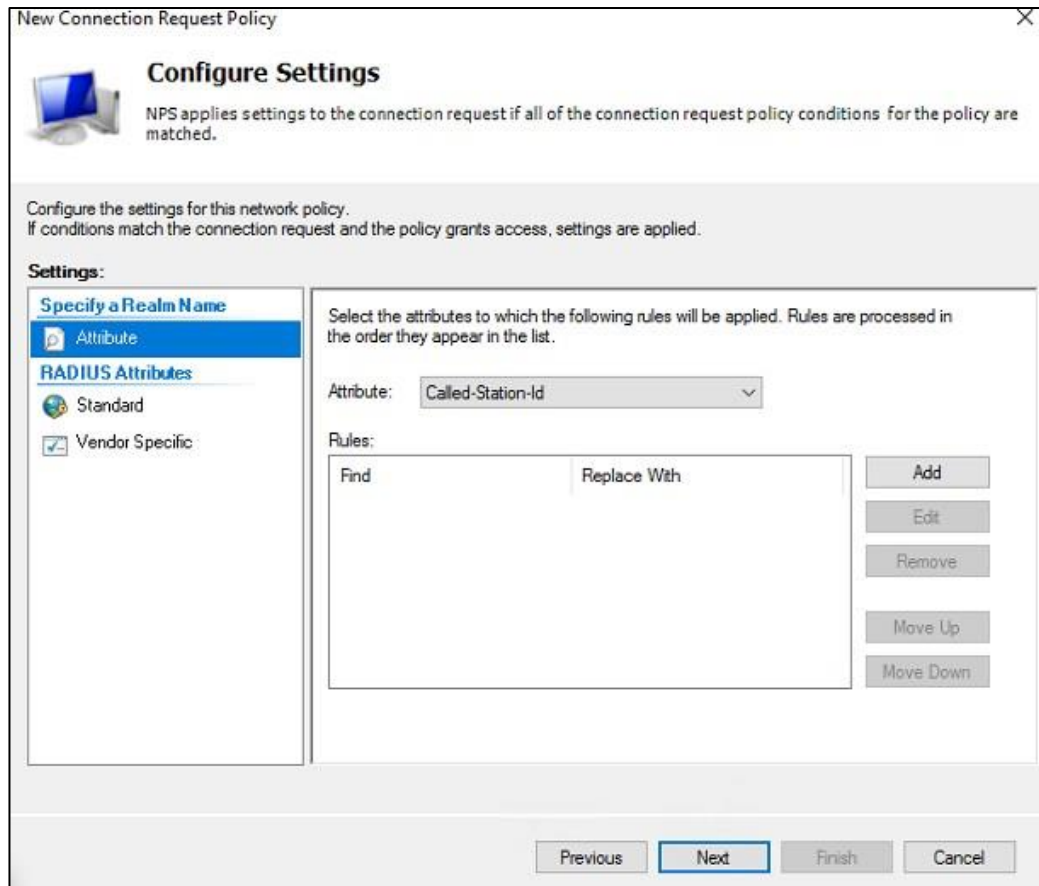
Previous Next Finish Cancel

#Nextをクリックします。

#開いたウィンドウで、NoをクリックしてConfigure Settingsページを開きます。

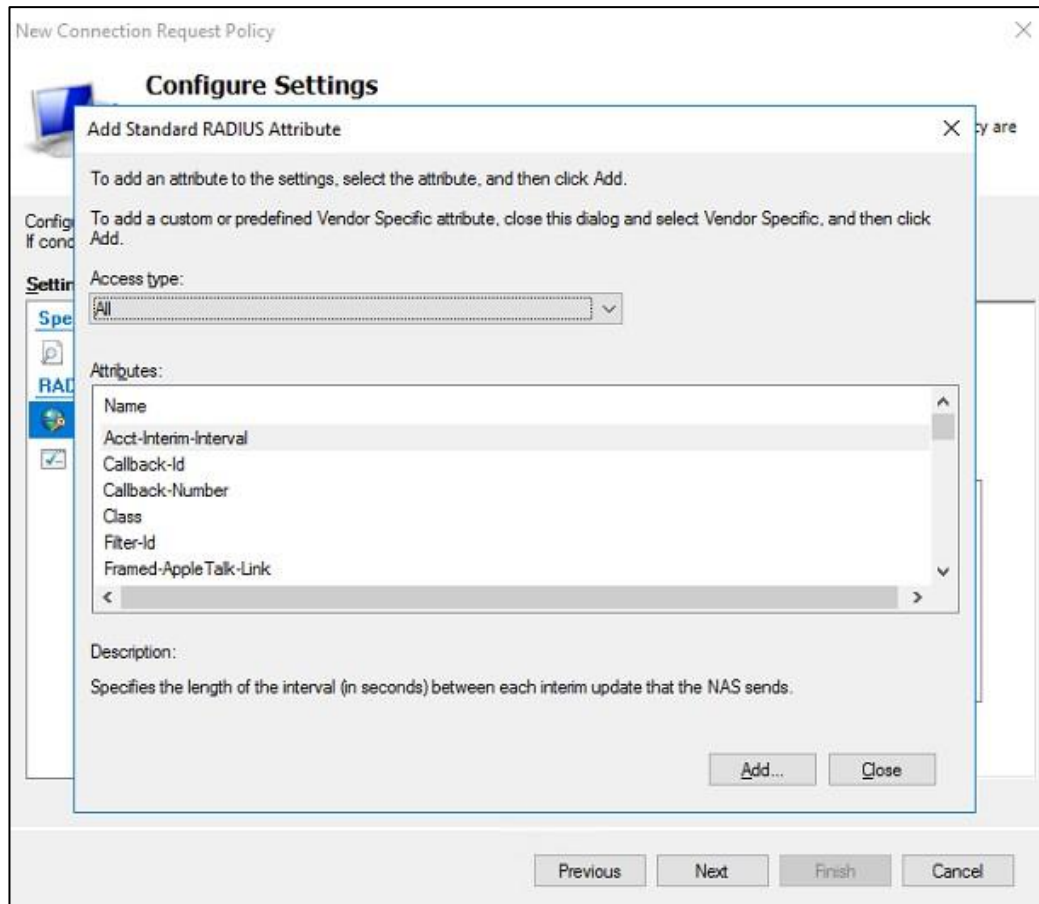
- f. ポリシーアトリビュートを設定します。AttributeリストからCalled-Station-Idを選択します。

図15 ポリシー属性の構成



- g. 標準のRADIUSアトリビュートを追加します。
#RADIUS AttributesでStandardを選択します。
#Attributes列で属性名を選択し、Addをクリックします。Attribute Informationダイアログボックスが表示されます。

図16 標準RADIUSアトリビュートの追加

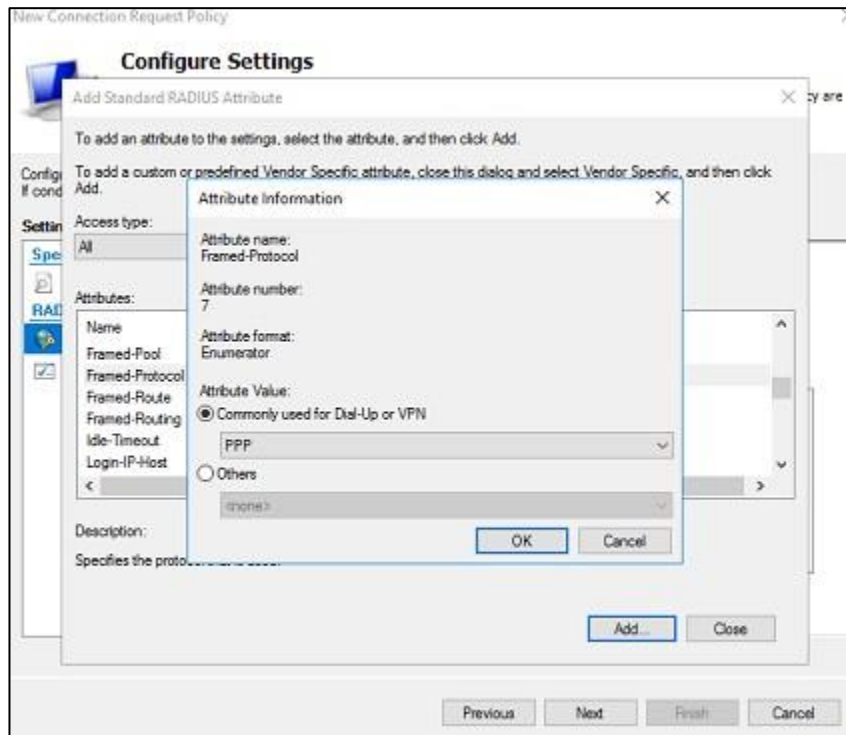


#表示されるAttribute Informationダイアログボックスで、属性値を設定します。

#属性の既定の選択を保持し、ドロップダウンリストから属性値を選択して、OKをクリックします。

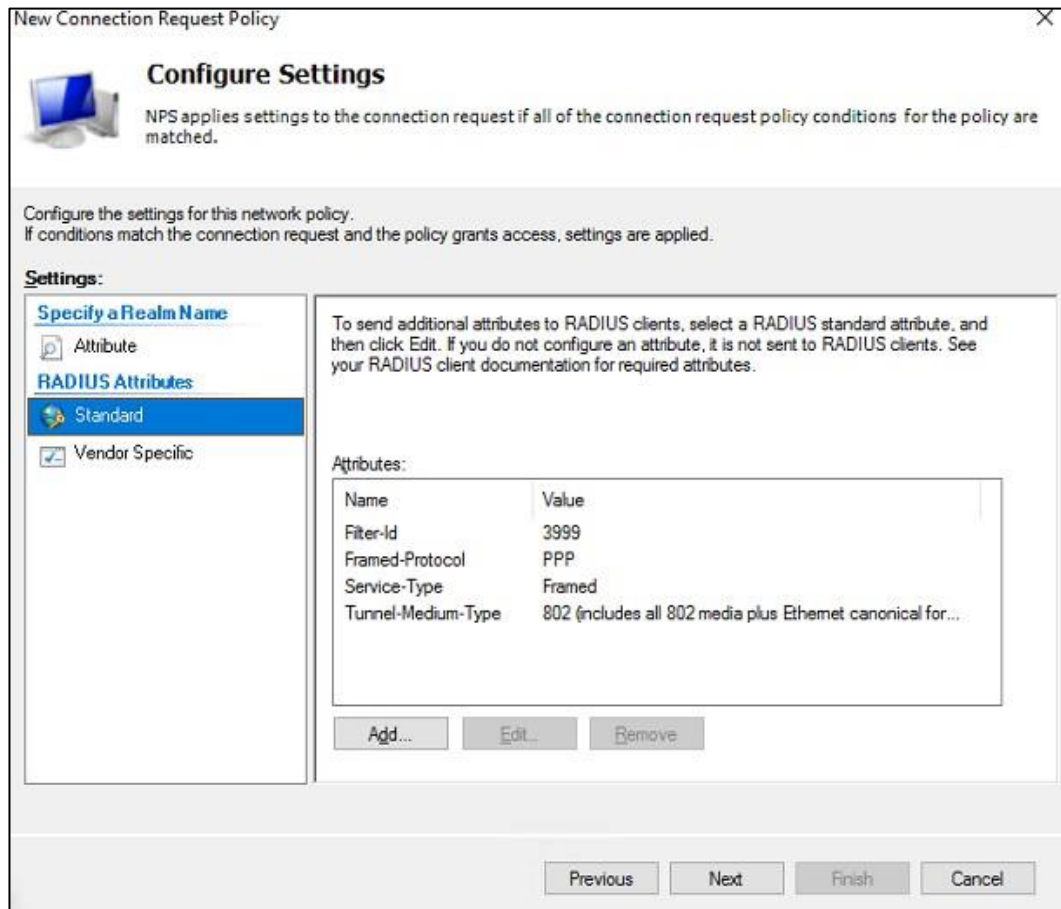
たとえば、Framed-Protocol属性では、デフォルトでDial-UpまたはVPNに一般的に使用されるオプションが選択されています。このデフォルトの選択をそのまま使用して、ドロップダウンリストからPPPを選択し、OKをクリックします。属性値PPPはFramed-Protocol属性で設定されています。

図17 属性値の構成



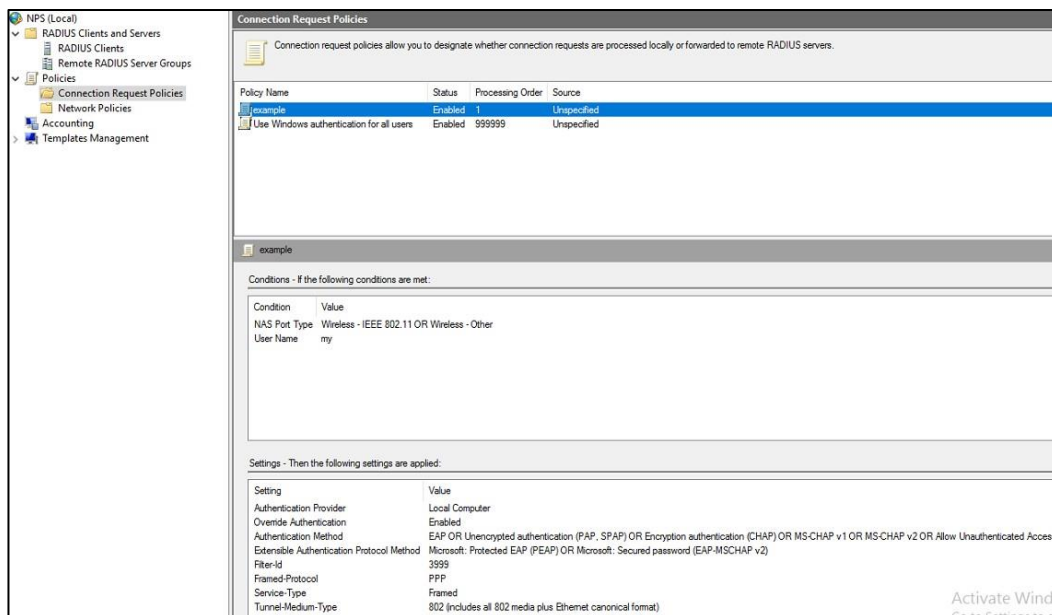
#前の手順を繰り返して、値FramedのService-Typeアトリビュート、値802のTunnel-Media-Typeアトリビュート(すべての802メディアとEthernet...を含む)、および値3999のFilter-Id(ACL)を追加します。設定されたアトリビュートは次のとおりです。

図18 標準のRADIUS属性



- h. 接続要求ポリシーを表示または編集します。
- #NPSの左側のナビゲーションペインで、**Policies > Connection Request Policies**の順に選択します。
- # **Policy Name**列で、接続要求ポリシーを表示できます。
- #ポリシーの構成を編集するには、ポリシー名を右クリックして**Properties**を選択します。

図19 接続要求ポリシー



設定の確認

1. クライアントで、ワイヤレスネットワークに接続します。ブラウザを使用してWebサイトにアクセスします。ポータル認証ページが開きます。構成されたユーザー名myとパスワードを入力します。ユーザーは認証を正常に通過できます。
2. ACで、次のコマンドを使用して、ユーザーがオンラインになり、サーバーが認可ACLをユーザーに割り当てたことを確認します。

[AC] display portal user all verbose Total portal users: 1

Basic:

AP name: ap1

Radio ID: 1

SSID: portal_nps

Current IP address: 72.205.0.1

Original IP address: 72.205.0.1

Username: my

User ID: 0x1000002b

Access interface: WLAN-BSS0/4

Service-VLAN/Customer-VLAN: 80/-

MAC address: d4bb-c8a1-8a55

Authentication type: Normal

Domain name: portal

VPN instance: N/A

Status: Online

Portal server: imc

Vendor: VIVO

Portal authentication method: Direct

AAA:

Realtime accounting interval: 720s, retry times: 5

Idle cut: N/A

Session duration: 0 sec, remaining: 0 sec

Remaining traffic: N/A

Login time: 2021-12-3 18:57:44 UTC

Online time(hh:mm:ss): 00:00:05

DHCP IP pool: N/A

Web URL: N/A

ACL&QoS&Multicast:

Inbound CAR: N/A

Outbound CAR: N/A

ACL number: 3999 (active, AAA)

User profile: N/A

Session group profile: N/A

Max multicast addresses: 4

Flow statistic:

Uplinkpackets/bytes: 7/540

Downlink packets/bytes: 0/0

構成ファイル

#

radius scheme nps

primary authentication 8.72.1.7 key simple 12345678

primary accounting 8.72.1.7 key simple12345678

user-name-format without-domain

#

domain portal

authentication portal radius-scheme nps

authorization portal radius-scheme nps

accounting portal radius-scheme nps

#

portal server imc

ip 8.1.1.231 key simple portal

#

portal web-server imc

url http://8.1.1.231:8080/portal/

```
#
wlan service-template portal
  ssid portal_nps
  portal enable method direct
  portal domain portal
  portal apply web-server imc
  service-template enable
#
wlan ap ap1 model WA6638-JP
serial-id 219801A24F8198E0001G
  radio 1
    radio enable
    service-template portal vlan 80
#
Acl advanced 3999
  rule 0 permit ip
#
vlan 80
#
interface Vlan-interface 80
  ip address 72.205.1.1 255.255.0.0
#
dhcp server ip-pool 80
  gateway-list 72.205.1.1
  network 72.205.0.0 mask 255.255.0.0
  dns-list 72.205.1.1
#
return
```