Configure your firewall for administrative access via RADIUS authentication

Version 1.0

PAN-OS 5.0.1

Johan Loos

johan@accessdenied.be

Configure your Palo Alto firewall for RADIUS Authentication

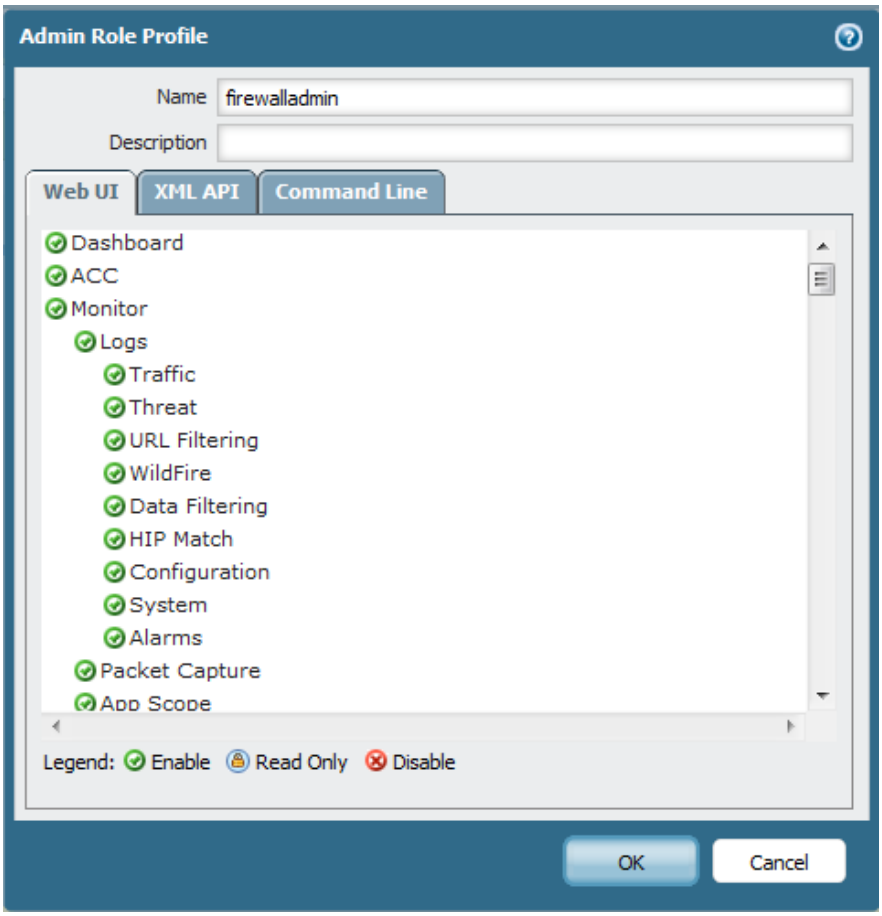
This guide describes how that you can configure your firewall for RADIUS authentication when you need to manage the device. The RADIUS server used is a Windows Server 2012 installed with the Network Policy Server Role.

Configure PA for RADIUS Authentication Task List

- △ Define an administration role
- △ Create a RADIUS Server Profile
- △ Create a RADIUS Authentication Profile
- △ Create a Local Authentication Profile
- △ Configure Authentication Fallback
- △ Change Management Authentication
- △ Create a Security Group in Active Directory
- △ Configure your firewall as RADIUS client on Windows Server 2012 NPS
- △ Create a Connection Request Policy on Windows Server 2012 NPS
- △ Create a Network Policy on Windows Server 2012 NPS
- △ Test

Define an administration role

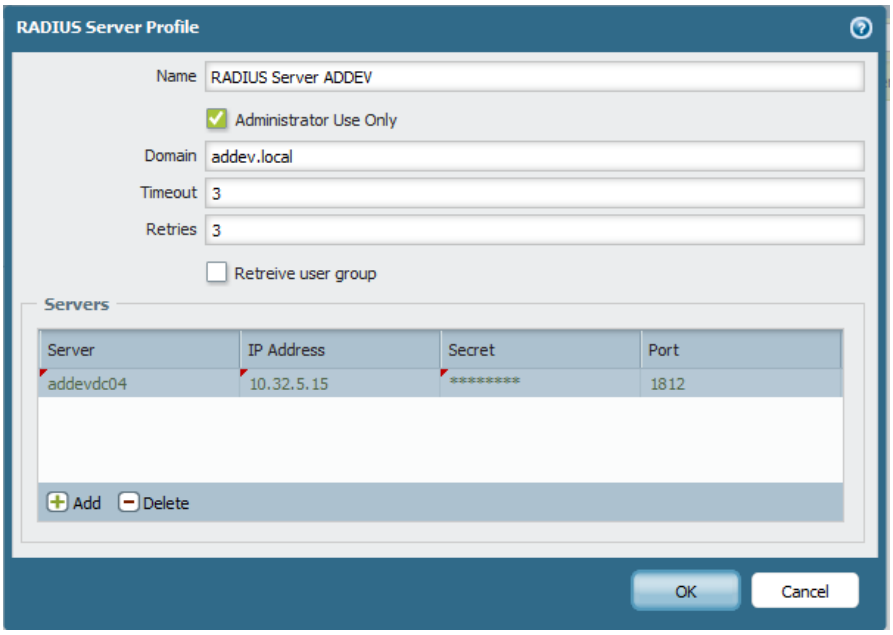
- Navigate to **Device | Admin Roles** and click **Add**
- On the **Admin Role Profile** page, Enable or Disable all the required options



- Click **Close**

Create a RADIUS Server Profile

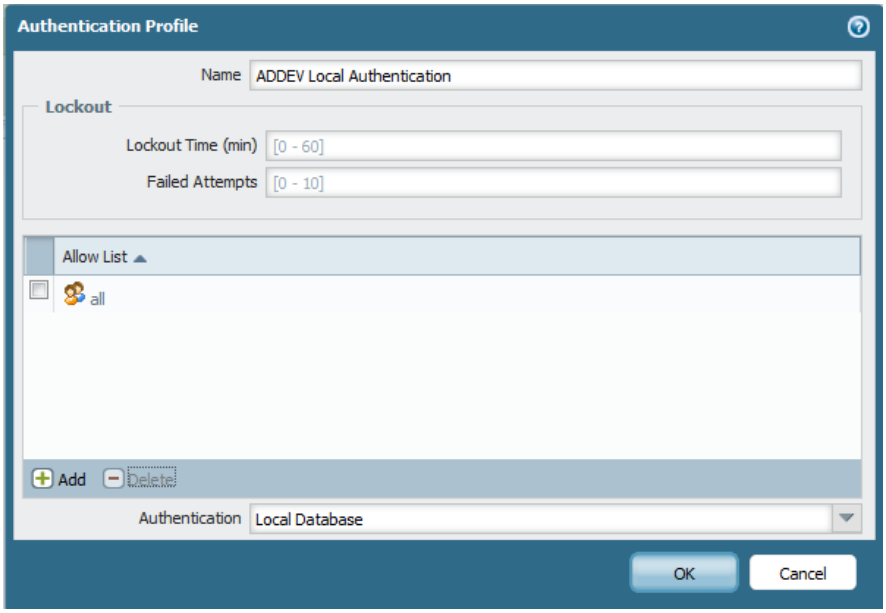
- Navigate to **Device | Server Profiles | RADIUS** and click **Add**
- On the **RADIUS Server Profile** page, type a name for your profile, select **Administrator Use Only**, specify a domain, click **Add** the add the IP Address of the RADIUS server, Secret and Port



- Click **OK**

Create a Local Authentication Profile

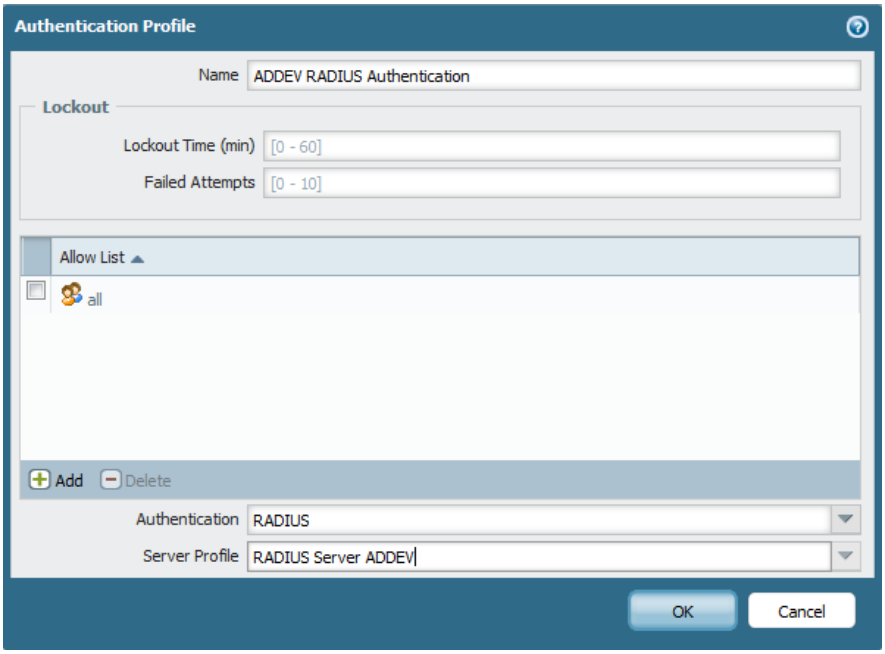
- Navigate to **Device | Authentication Profile**, and click **Add**
- On the **Authentication Profile** page, type a name for your profile
- Select the users which are allowed to logon to your firewall, from the Authentication list box select **Local Database**



- Click **OK**

Create a RADIUS Authentication Profile

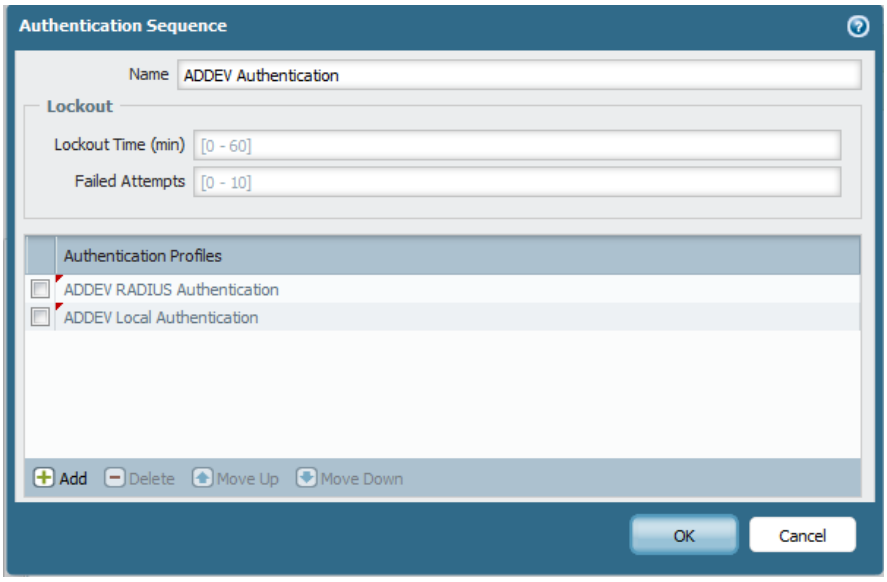
- Navigate to **Device | Authentication Profile** and click **Add**
- On the **Authentication Profile** page, type a name, from the **Authentication** list box select your RADIUS server profile



- Click **OK**

Configure Authentication Fallback

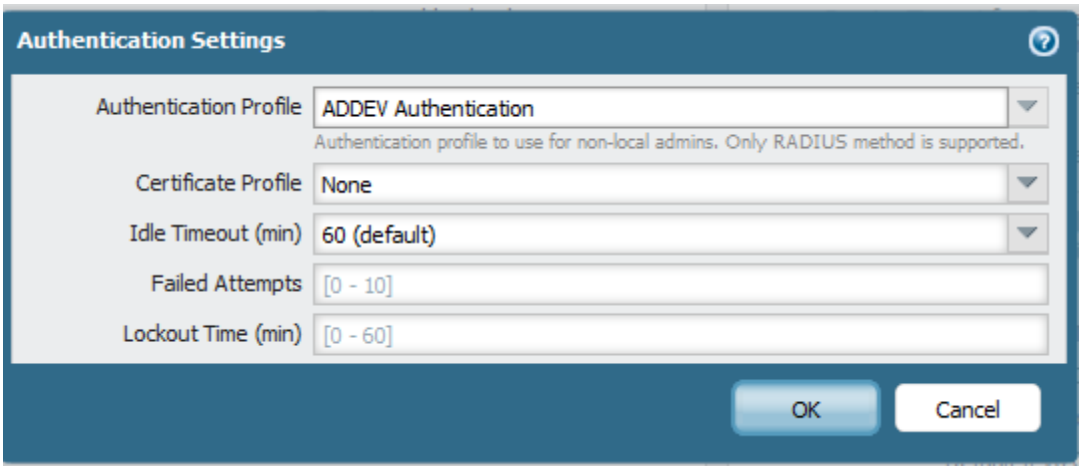
- Navigate to **Device | Authentication Sequence**, and click **Add**
- On the **Authentication Sequence** page, type a name for the authentication sequence
- Click **Add**, select all the required Authentication Profiles, move the listed Authentication Profiles in the correct order



- Click **OK**

Change Management Authentication

- Navigate to **Device | Setup | Management | Authentication Settings** and click on **Edit**
- On the **Authentication Settings** page, change the required Authentication Profile to your RADIUS Profile

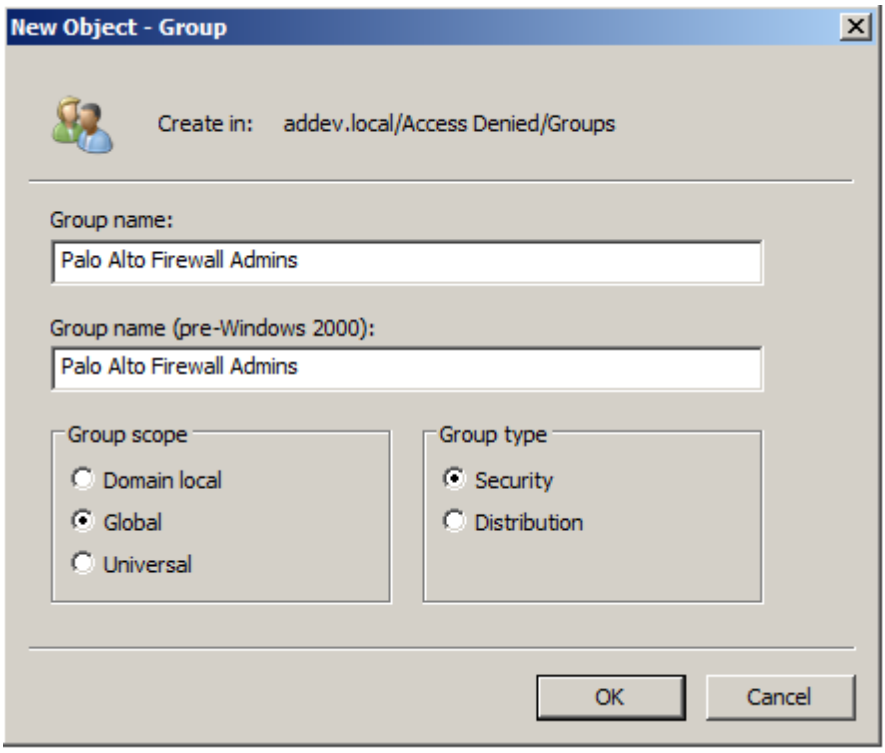


- Click **OK**

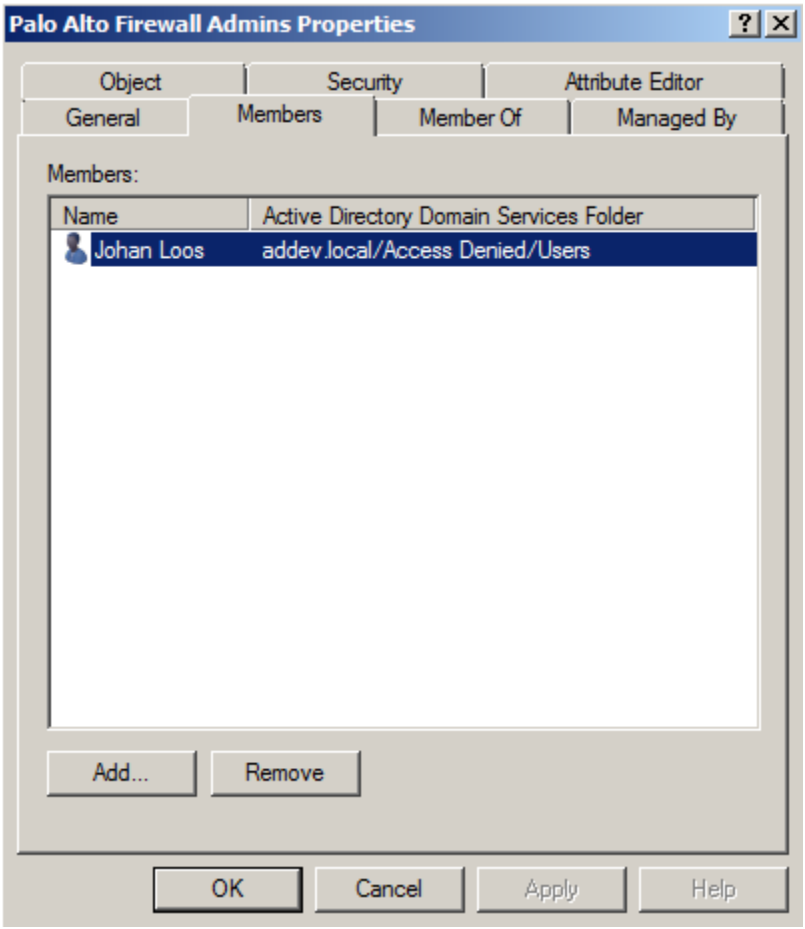
Create a Security Group in Active Directory

- Open **Active Directory Users and Computers** from **Administrative Tools**
- Navigate to an OU, right click and select **New Group**

- On the **New-Group** dialog box, type the name of your group who needs to manage the Palo Alto Firewall



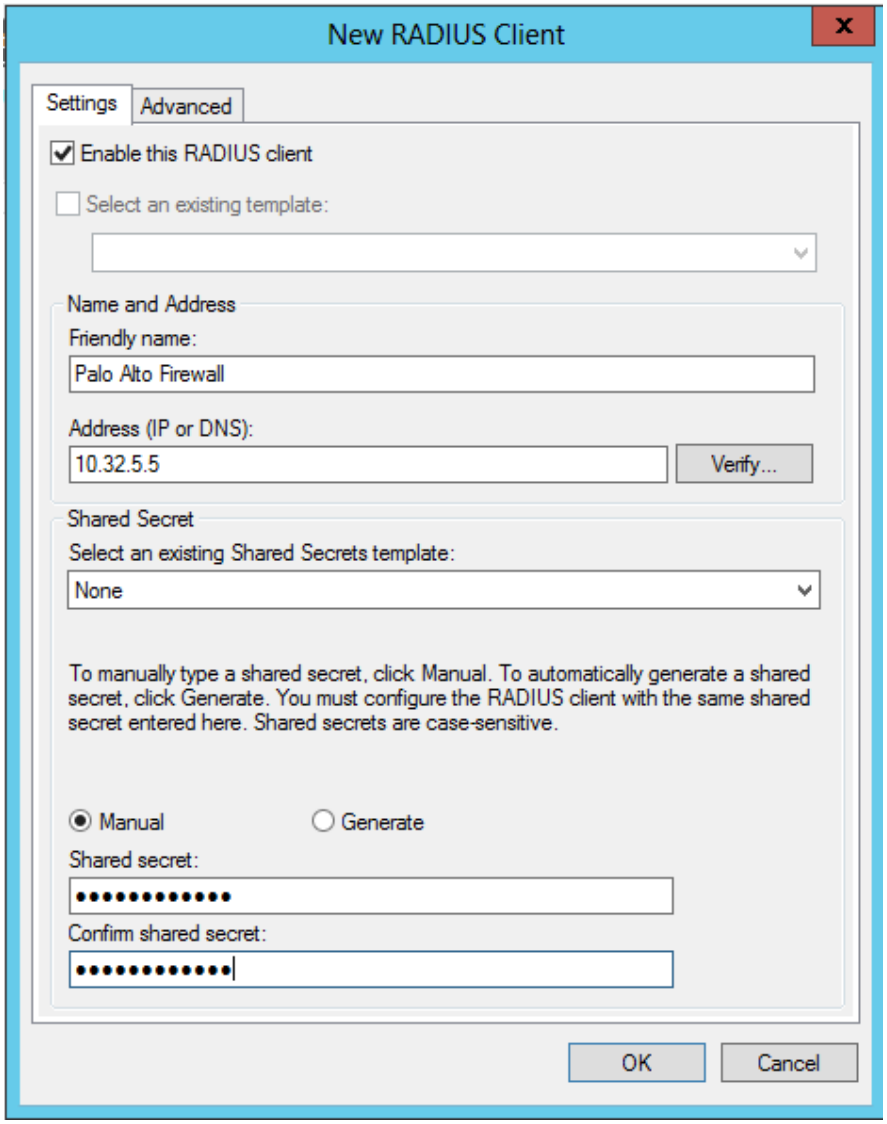
- On the **Members** tab add the required user accounts



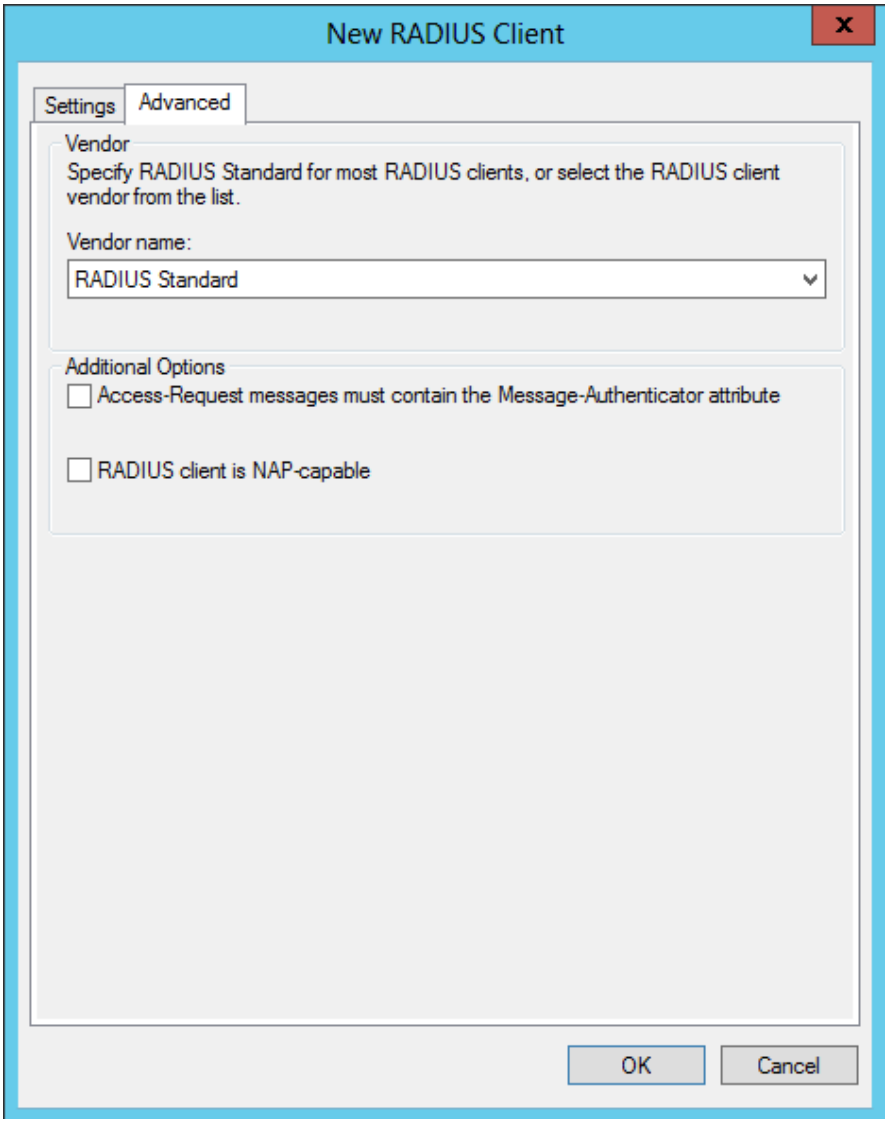
- Click **OK**

Configure your firewall as RADIUS client on Windows Server 2012 NPS

- Open **Network Policy Server** from **Administrative Tools**
- Expand RADIUS Clients and Servers, right click on **RADIUS Clients** and select **New RADIUS Client**
- On the **New RADIUS Client** dialog box, specify a friendly name and IP address



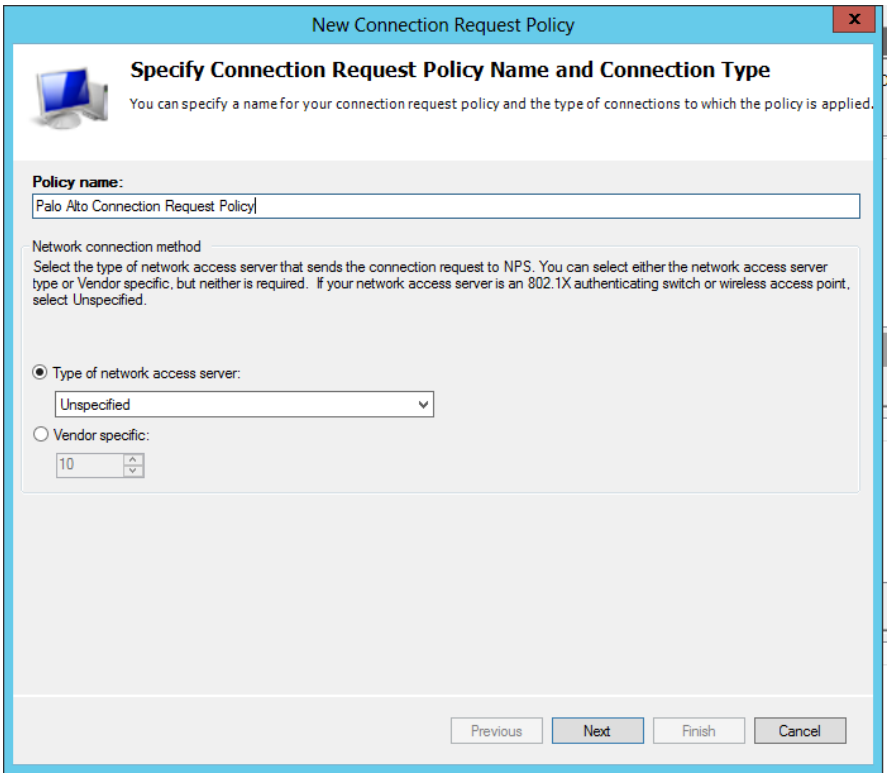
- Click on **Advanced**, uncheck or check the required options



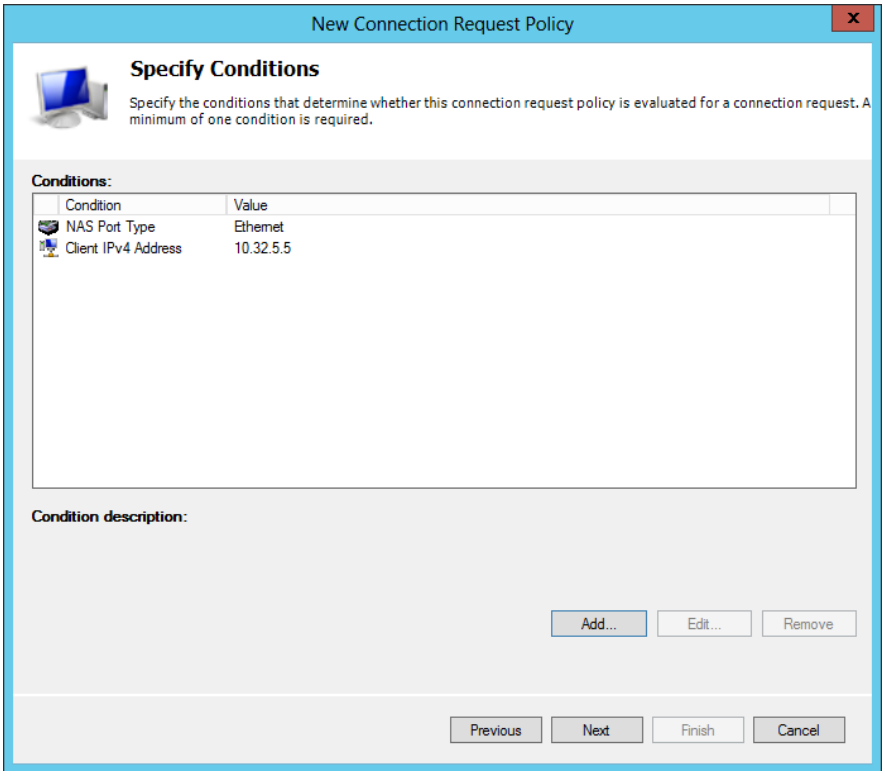
- Click **OK**

Create a Connection Request Policy on Windows Server 2012 NPS

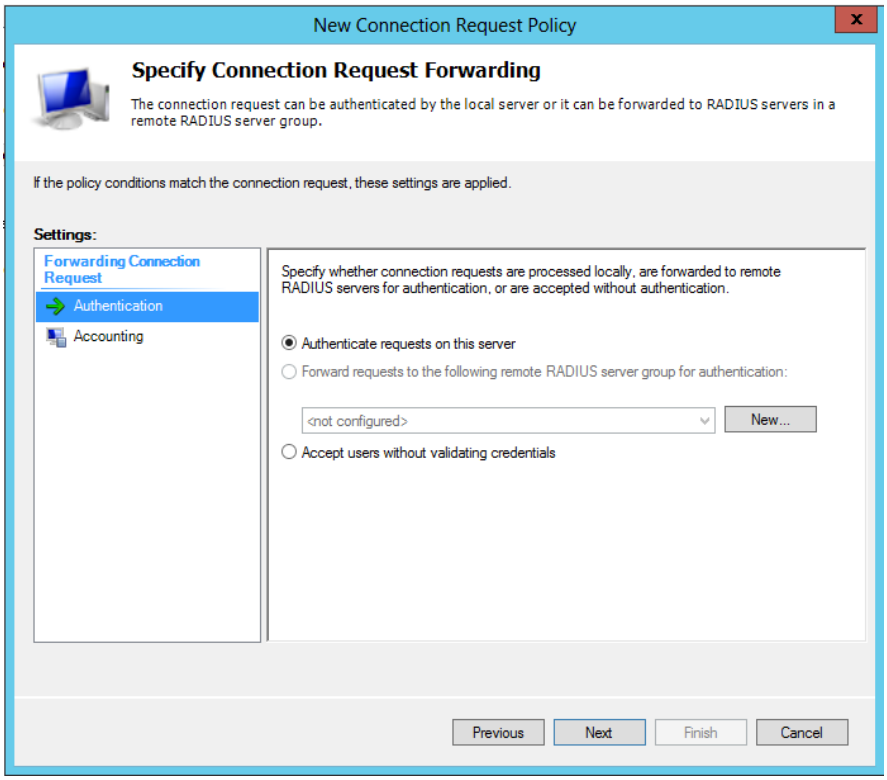
- From the **Network Policy Server** Console, right click on **Connection Request Policies** and select **New**
- On the **Specify Connection Request Policy Name and Connection Type** page, type a name for the policy and click **Next**



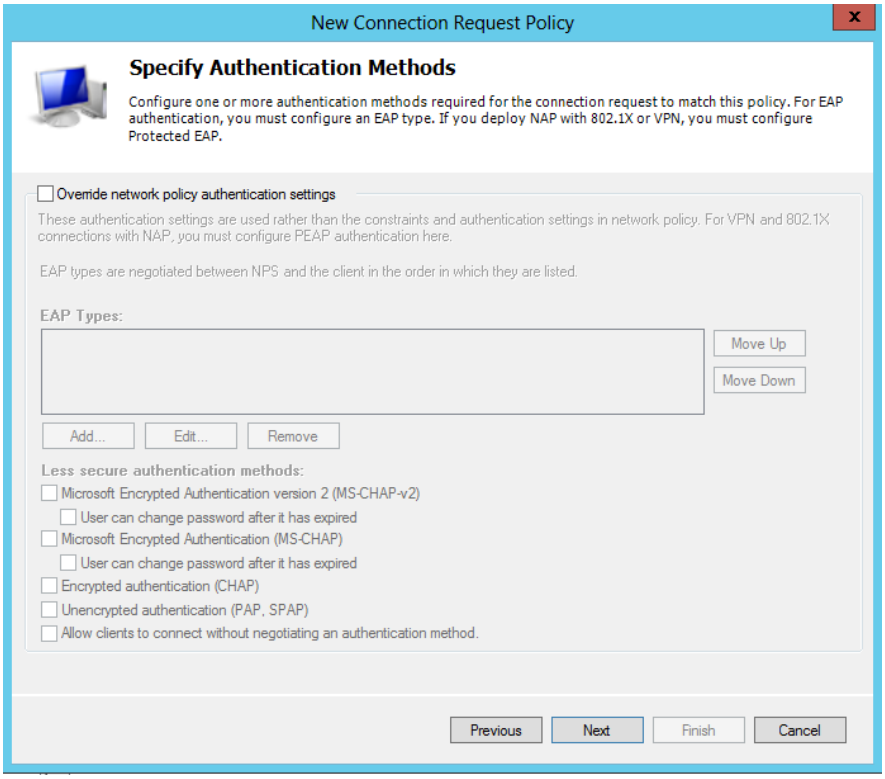
- On the **Specify Conditions** page, click **Add**. Select **NAS Port Type (Ethernet)**
- On the **Select conditions** dialog box, select **Client IPv4 Address** and click **Add**
- On the **Client IPv4 Address** dialog box, type the management IP address of the firewall
- Click **OK** and click **Next**



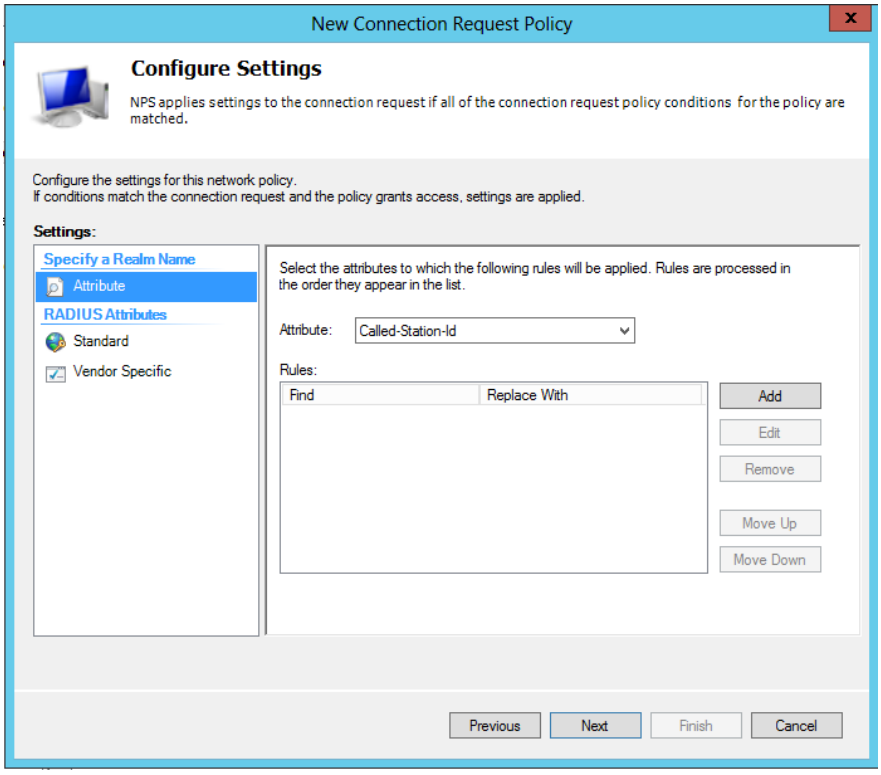
- On the **Specify Connection Request Forwarding** page, select **Authenticate requests on this server** and click **Next**



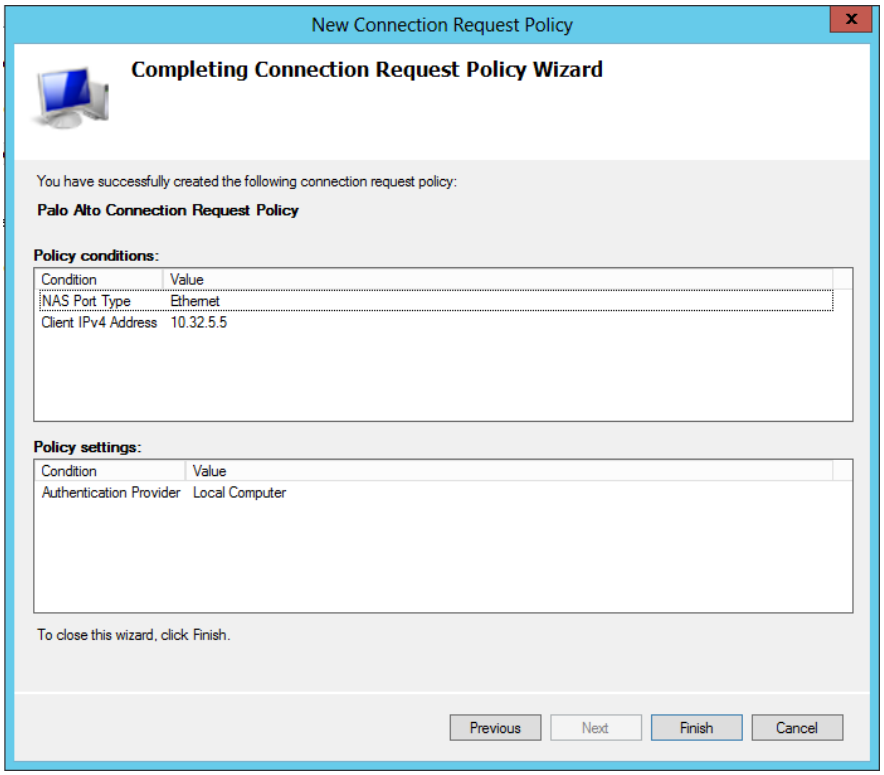
- On the **Specify Authentication Methods** page, click **Next**



- On the **Configure Settings** page, click **Next**

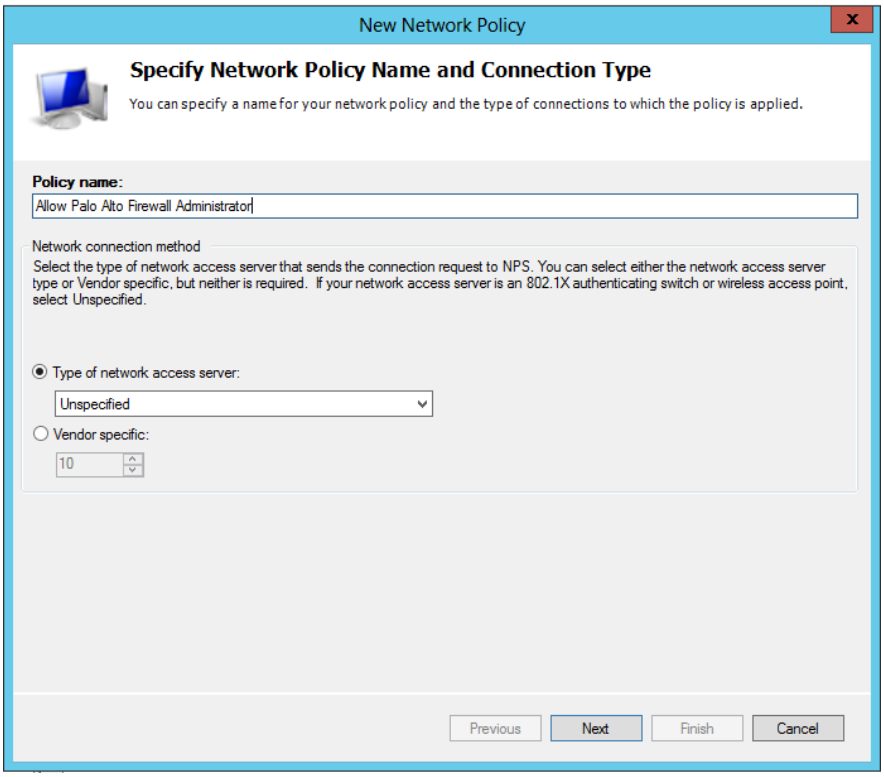


- On the **Completing Connection Request Policy Wizard** page, click **Finish**

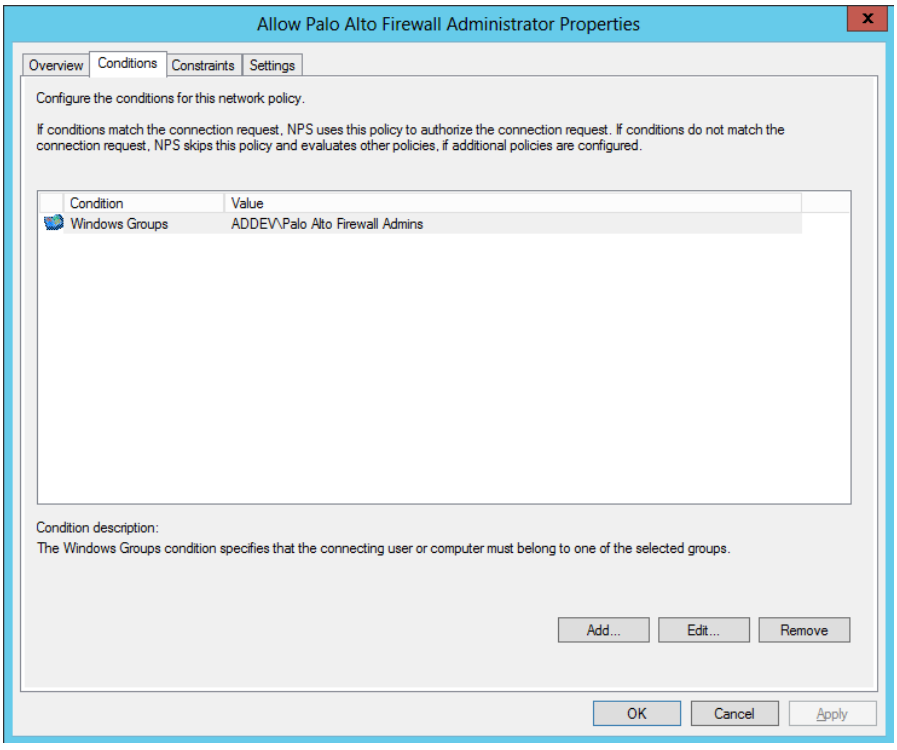


Create a Network Policy on Windows Server 2012 NPS

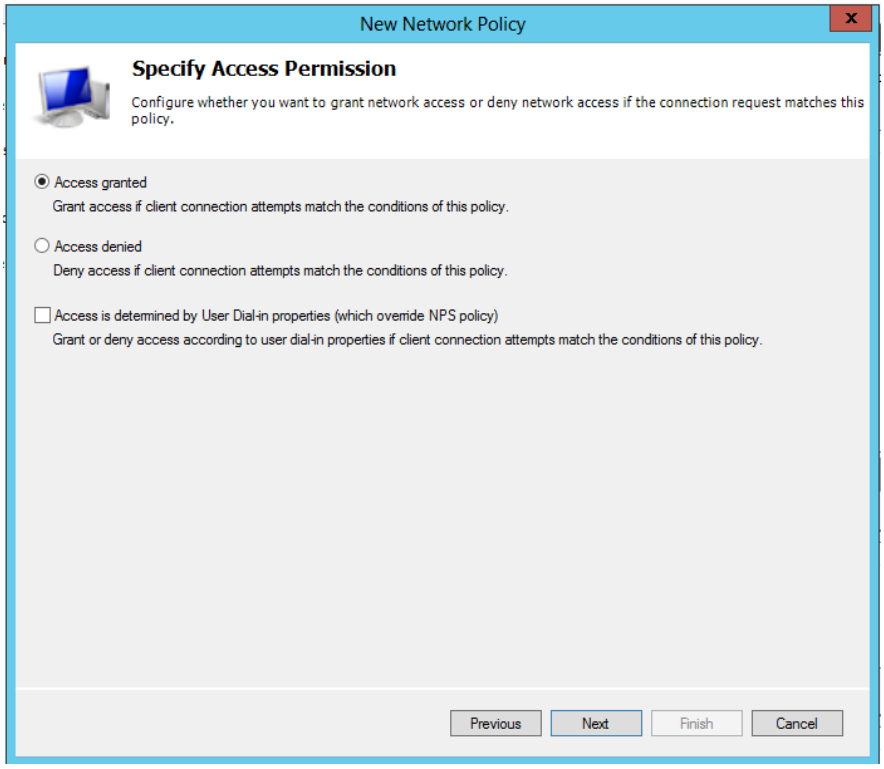
- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**



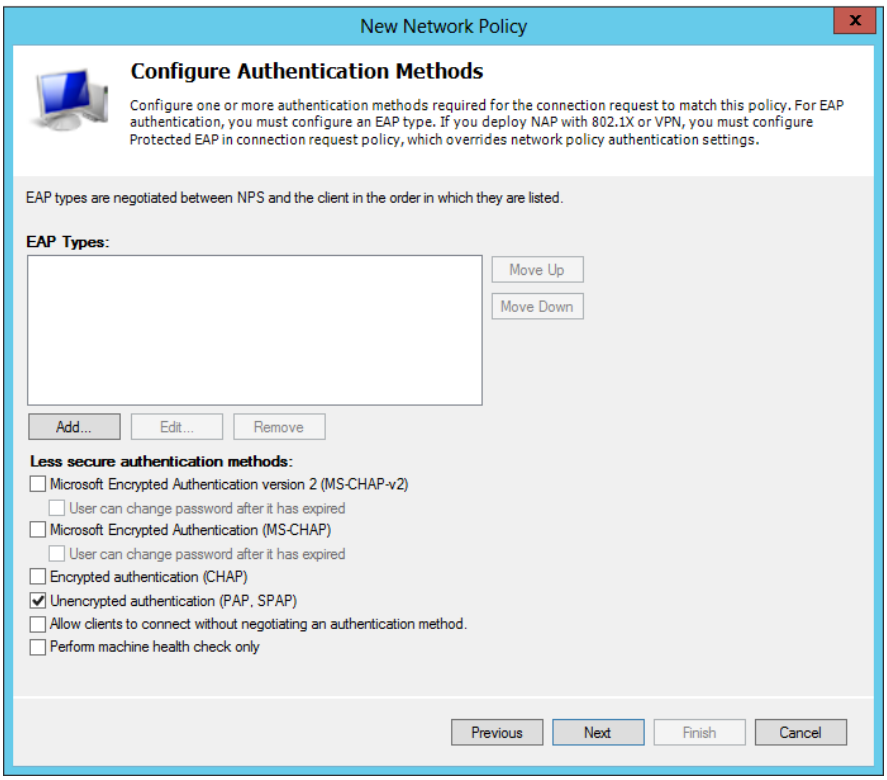
- On the **Specify Conditions** page, click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Palo Alto Firewall Admins* , and click **Next**



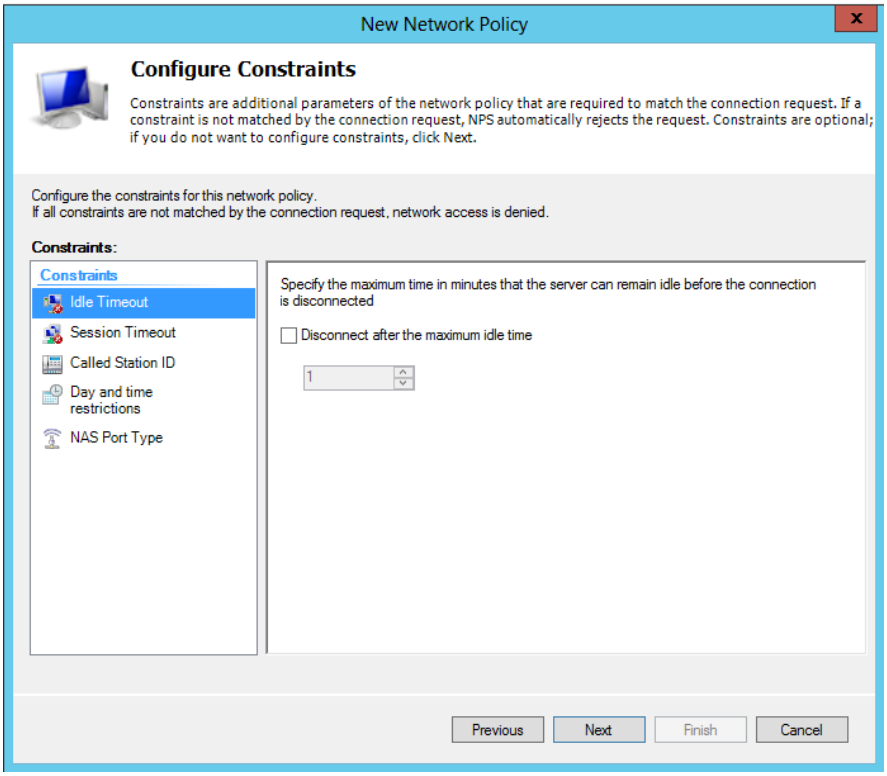
- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**



- On the **Configure Authentication Methods** page, clear all authentications methods and select only **Unencrypted Authentication (PAP,SPAP)** and click **Add**

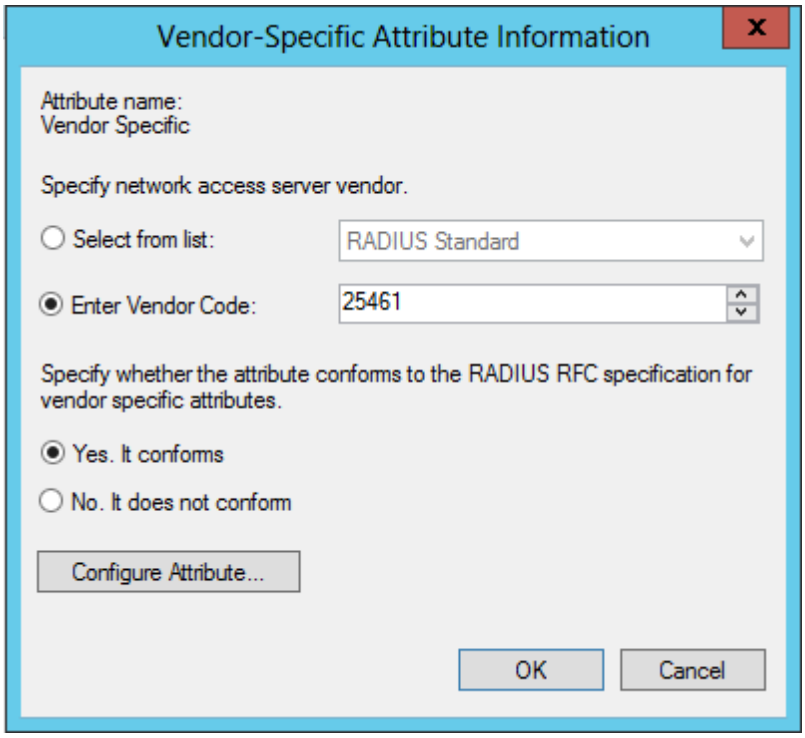


- On the **Configure Constraints** page, click **Next**

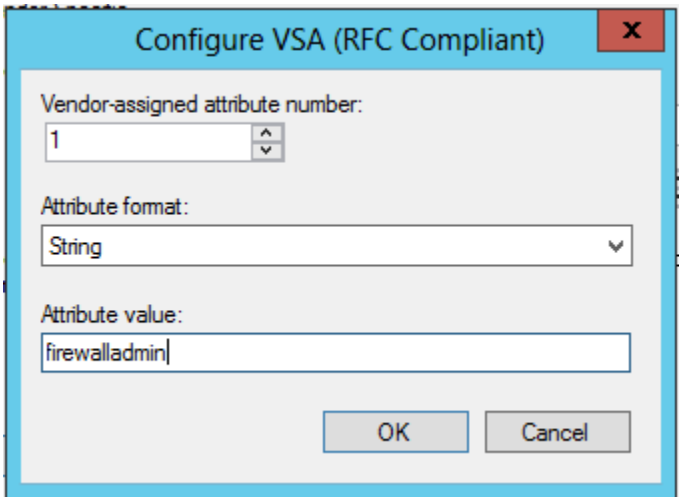


- On the **Configure Settings** page, Select **Vendor Specific** and click **Add**

- On the **Vendor Add Specific Attribute Information** page, select **Custom**
- On the **Attribute Information** page, click **Add**
- On the **Vendor-Specific Attribute Information** page select **Enter Vendor Code**, type 25461, select **Yes, it conforms** and click **Configure Attribute**



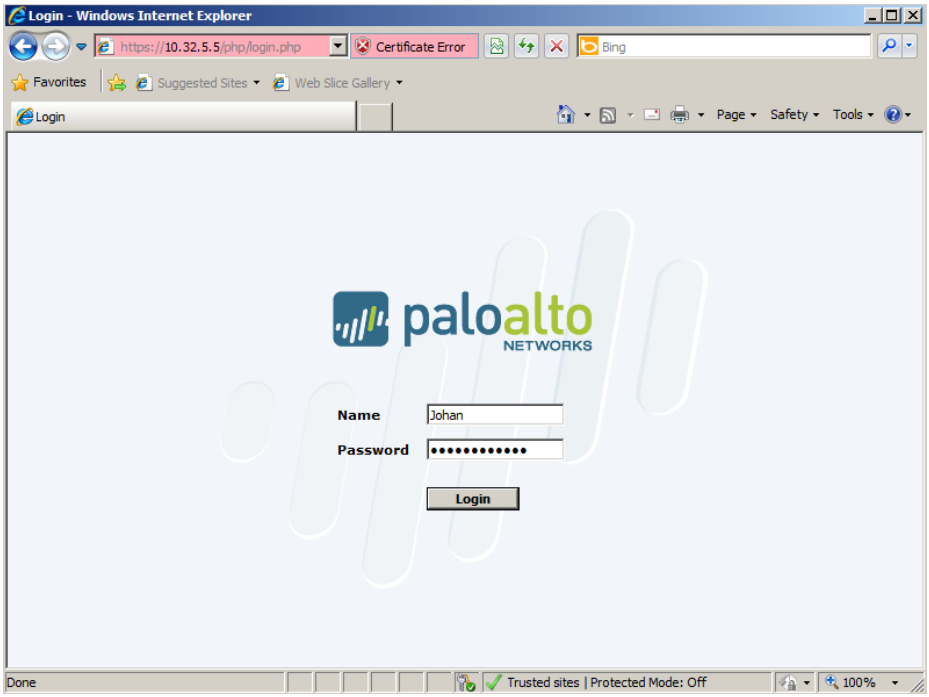
- On the **Configure VSA** page, select attribute number 1, type the Attribute value and click **OK**



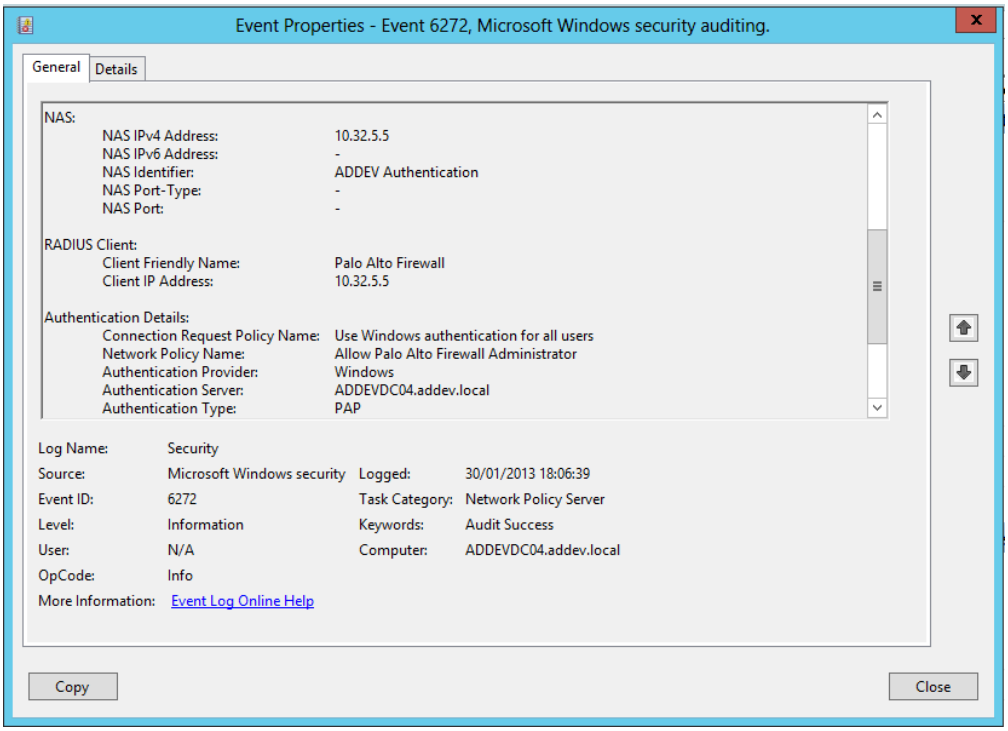
- Click multiple times **OK, click Next**
- On the **Completing New Network Policy** page, click **Finish**

Test

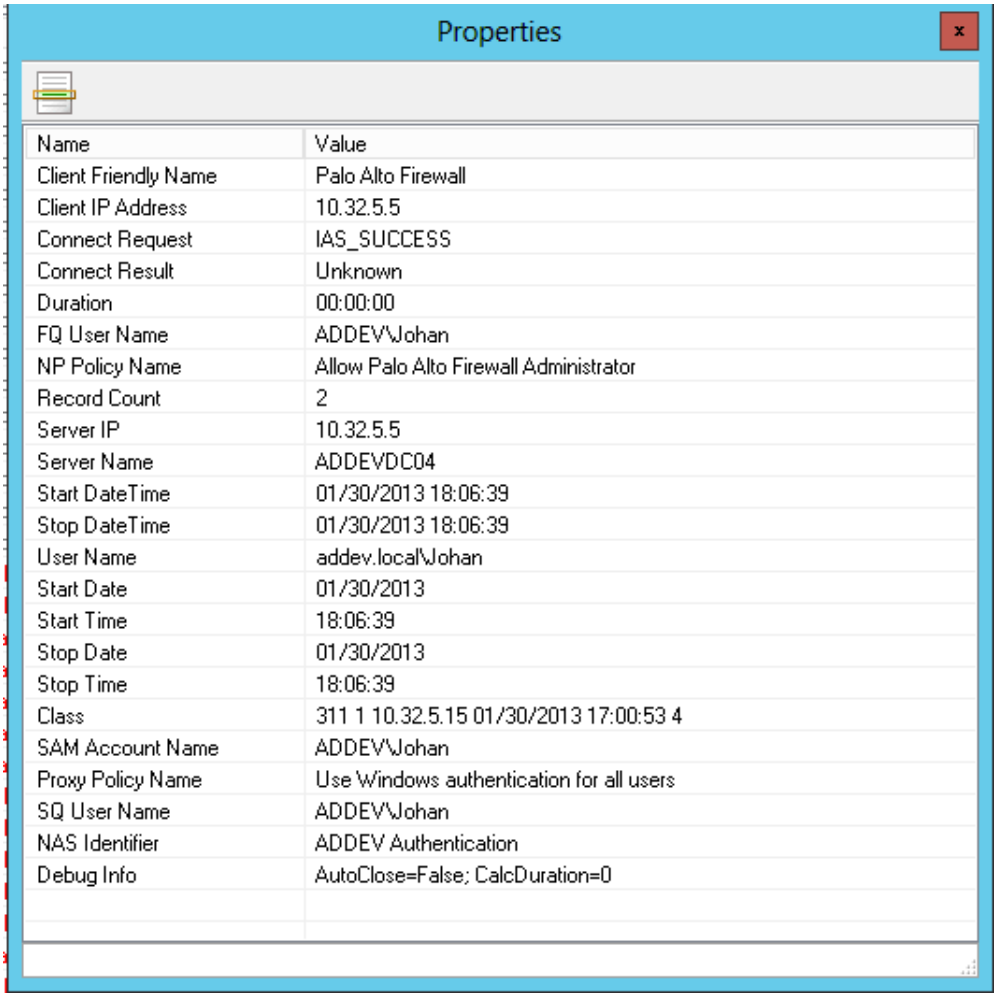
- Logon into your firewall with your user domain credentials



- After successful authentication, the following event is generated on the Network Policy Server



- Same event, but from a different tool



- Event generated on your Palo Alto Firewall

Receive Time	Type	Severity	Event	Object	Description
01/30 19:13:38	general	informat...	general		User admin accessed Monitor tab
01/30 18:11:46	general	informat...	general		User Johan logged out via Web from 10.32.5.3
01/30 18:10:17	general	informat...	general		User Johan logged in via Web from 10.32.5.3 using https
01/30 18:10:17	general	informat...	auth-success		User 'addev.local\Johan' authenticated. Profile ADDEV RADIUS Authentication in an authentication sequence ADDEV Authentication succeeded. From: 10.32.5.3.