

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

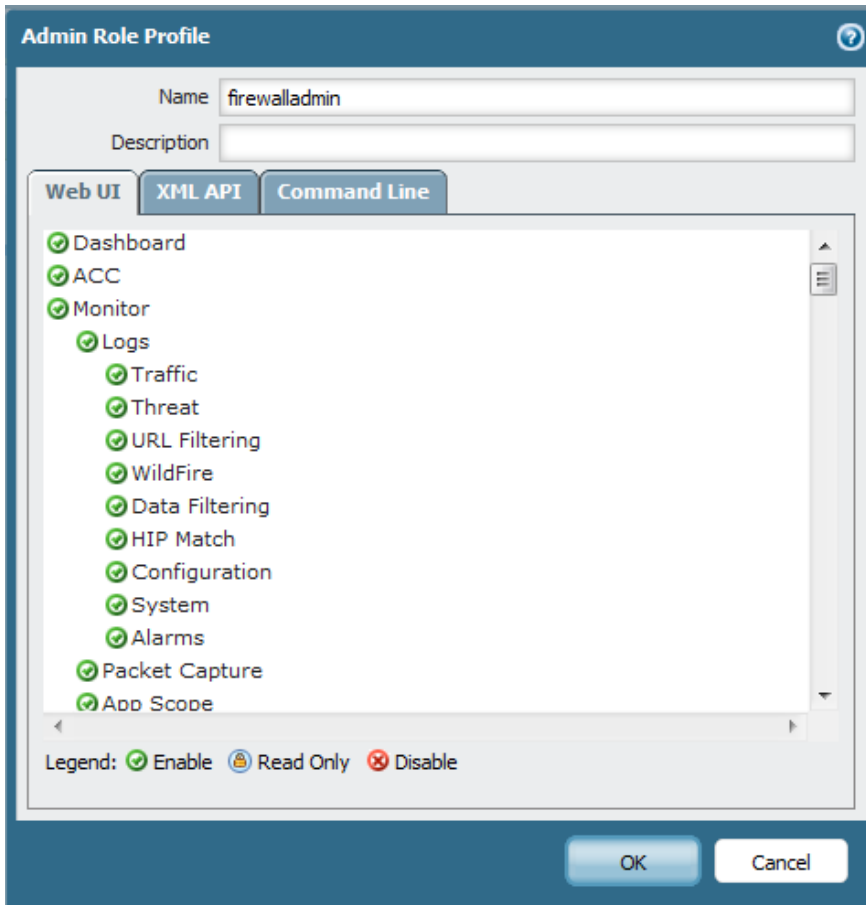
This guide describes how that you can configure your firewall for RADIUS authentication when you need to manage the device. The RADIUS server used is a Windows Server 2012 installed with the Network Policy Server Role.

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** then add the IP Address of the RADIUS server, Secret and Port

RADIUS Server Profile

Name: RADIUS Server ADDEV

Administrator Use Only

Domain: addev.local

Timeout: 3

Retries: 3

Retrieve user group

Server	IP Address	Secret	Port
addevdc04	10.32.5.15	*****	1812

+ Add - Delete

OK Cancel

- 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**

Authentication Profile

Name: ADDEV Local Authentication

Lockout

Lockout Time (min): [0 - 60]

Failed Attempts: [0 - 10]

Allow List ▲

all

+ Add - Delete

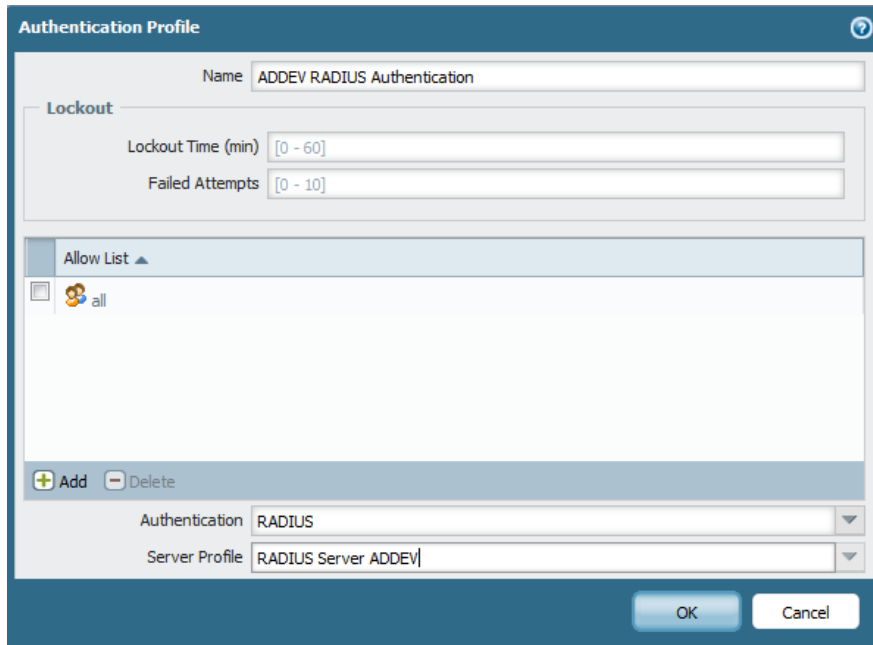
Authentication: Local Database

OK Cancel

- 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

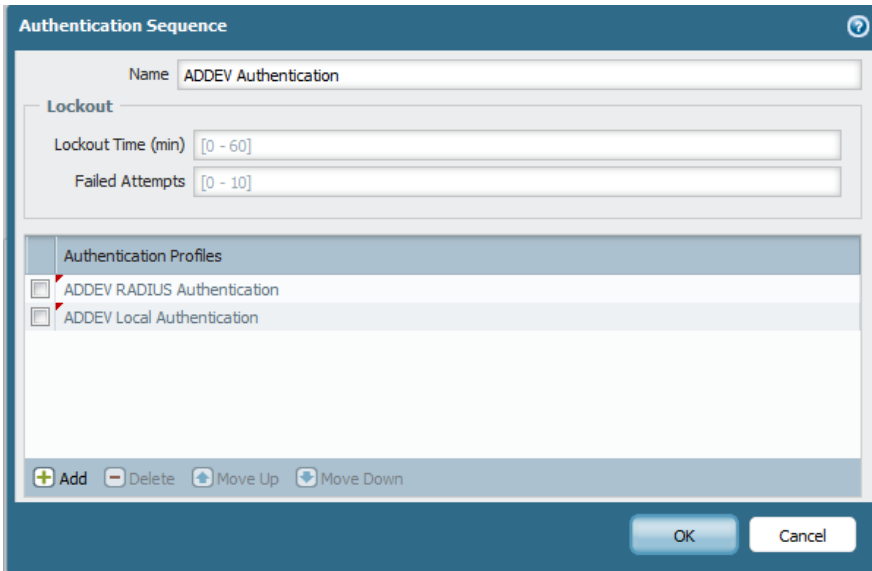


The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field is set to 'ADDEV RADIUS Authentication'. Under the 'Lockout' section, 'Lockout Time (min)' is set to '[0 - 60]' and 'Failed Attempts' is set to '[0 - 10]'. The 'Allow List' section shows a single entry 'all'. At the bottom, the 'Authentication' dropdown is set to 'RADIUS' and the 'Server Profile' dropdown is set to 'RADIUS Server ADDEV'. There are 'Add' and 'Delete' buttons above the dropdowns, and 'OK' and 'Cancel' buttons at the bottom right.

- Click **OK**

Configure Authentication Fallback

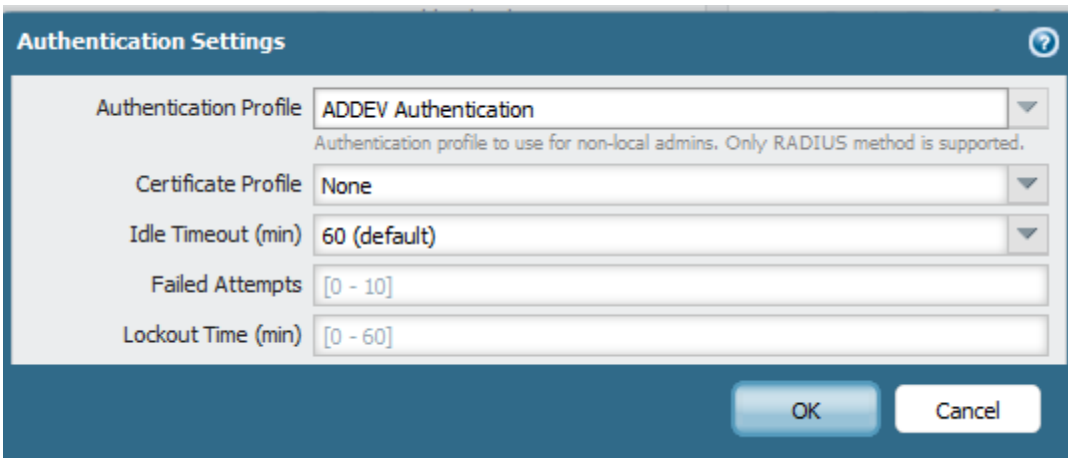
- Navigate to **Device | Authentication Sequence**, and click **Add**
- On the **Authentication Sequence** page, type a name for the authentication sequence
- Click **Add**, select all the required Authentication Profiles, move the listed Authentication Profiles in the correct order



- 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

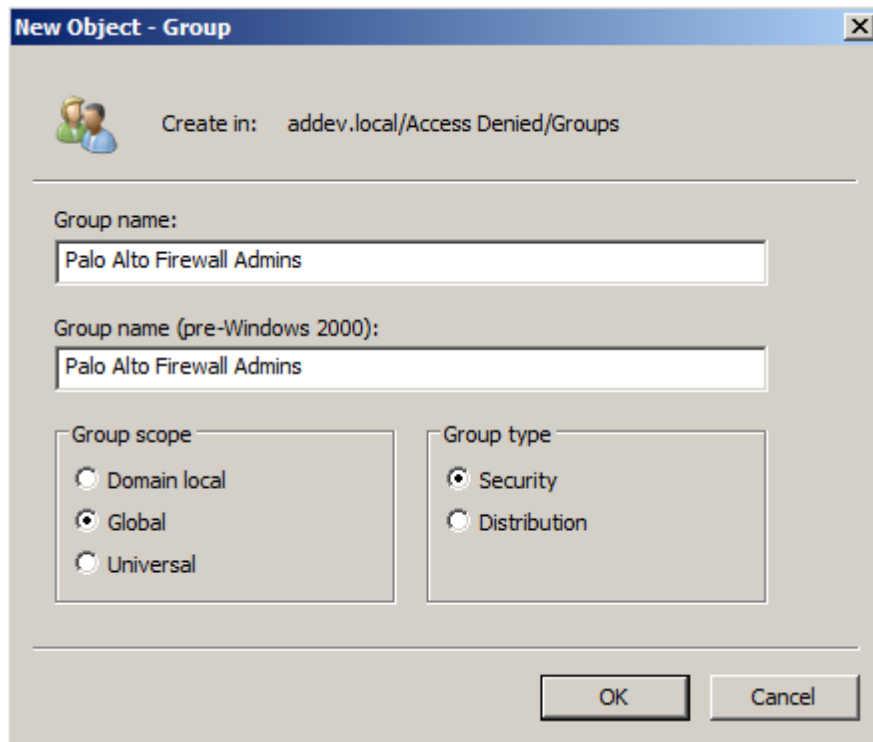


- Click **OK**

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



New Object - Group

Create in: addev.local/Access Denied/Groups

Group name:
Palo Alto Firewall Admins

Group name (pre-Windows 2000):
Palo Alto Firewall Admins

Group scope

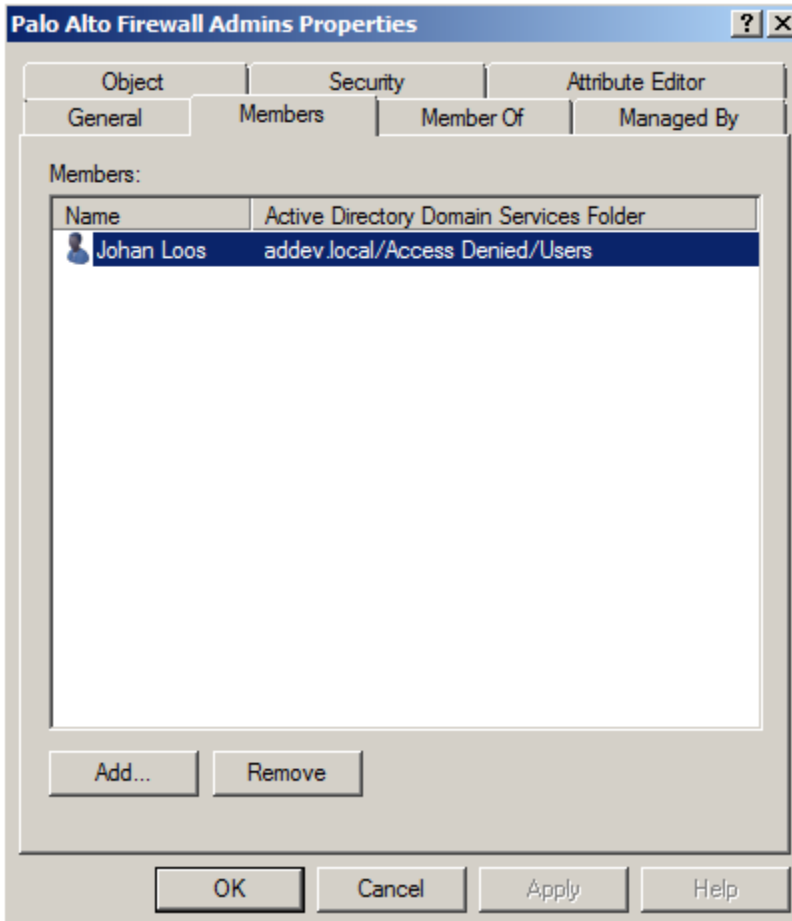
- Domain local
- Global
- Universal

Group type

- Security
- Distribution

OK Cancel

- 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

New RADIUS Client

Settings Advanced

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
Palo Alto Firewall

Address (IP or DNS):
10.32.5.5 Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

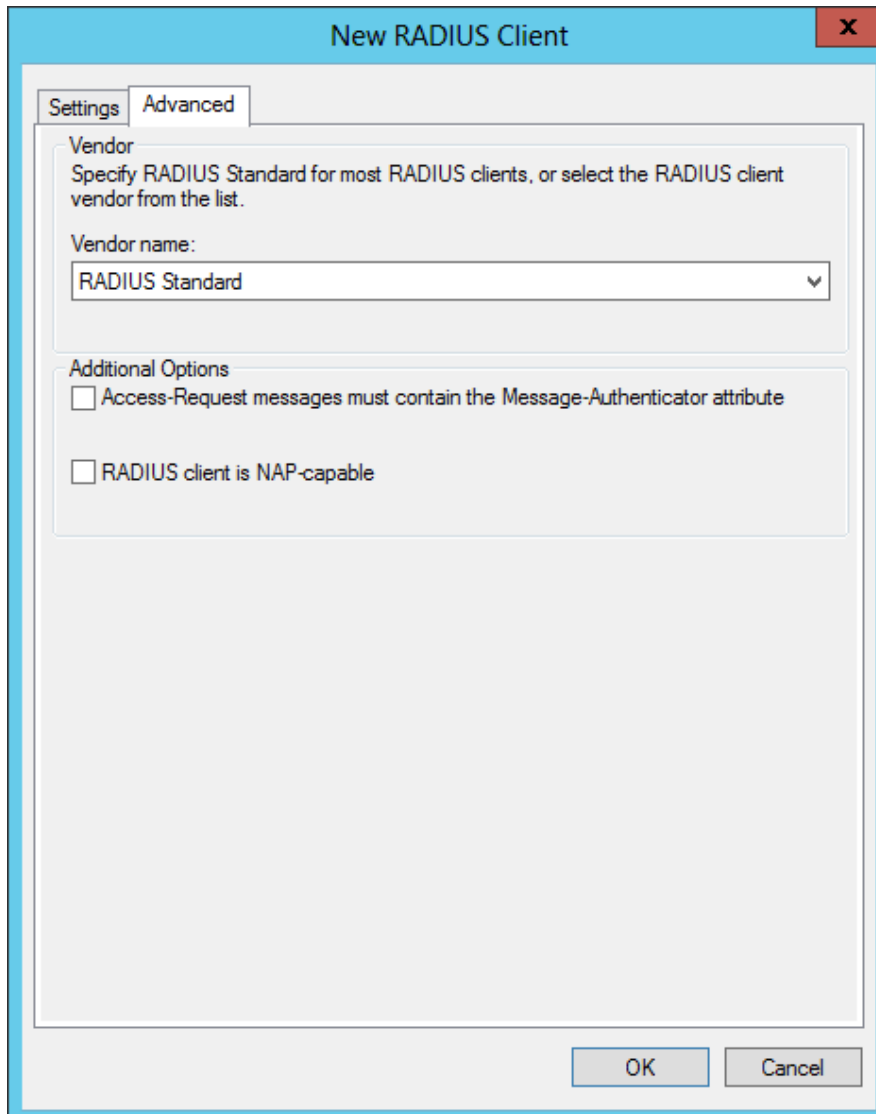
Manual Generate

Shared secret:
.....

Confirm shared secret:
.....

OK Cancel

- 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**

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name:
Palo Alto Connection Request Policy

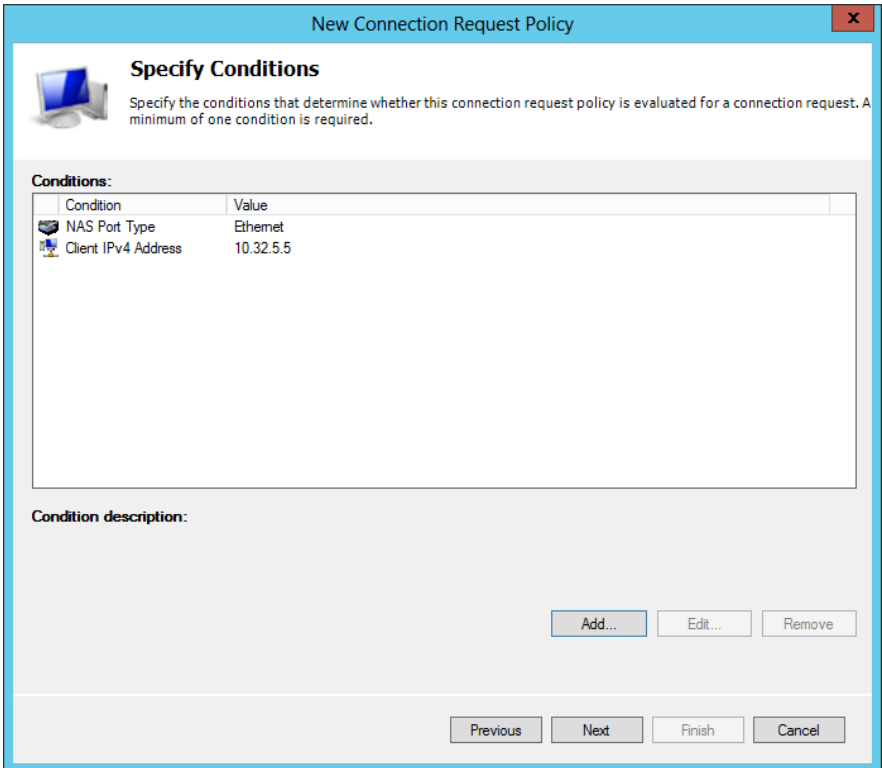
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Unspecified

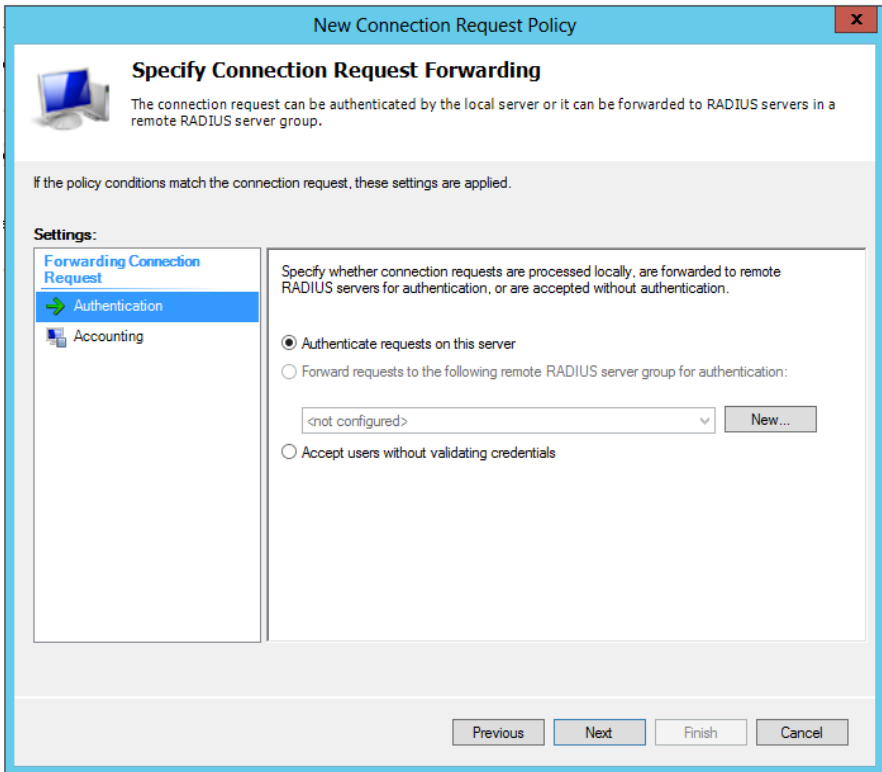
Vendor specific:
10

Previous Next Finish Cancel

- 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**

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. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

Override network policy authentication settings
 These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

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

EAP Types:

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

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

New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
 If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

Vendor Specific

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: Called-Station-Id

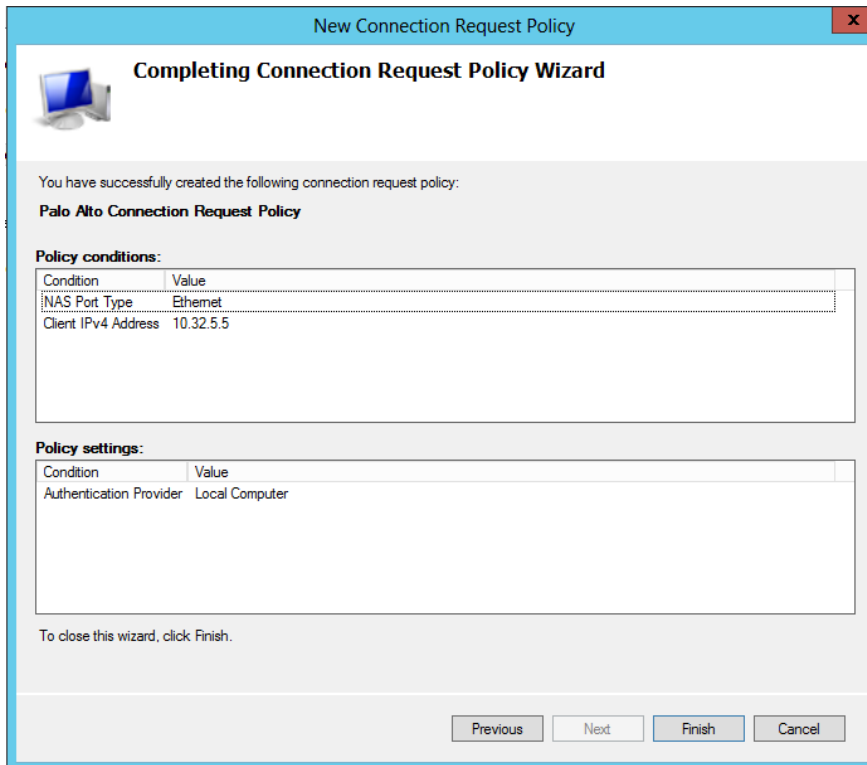
Rules:

Find	Replace With

Add
Edit
Remove
Move Up
Move Down

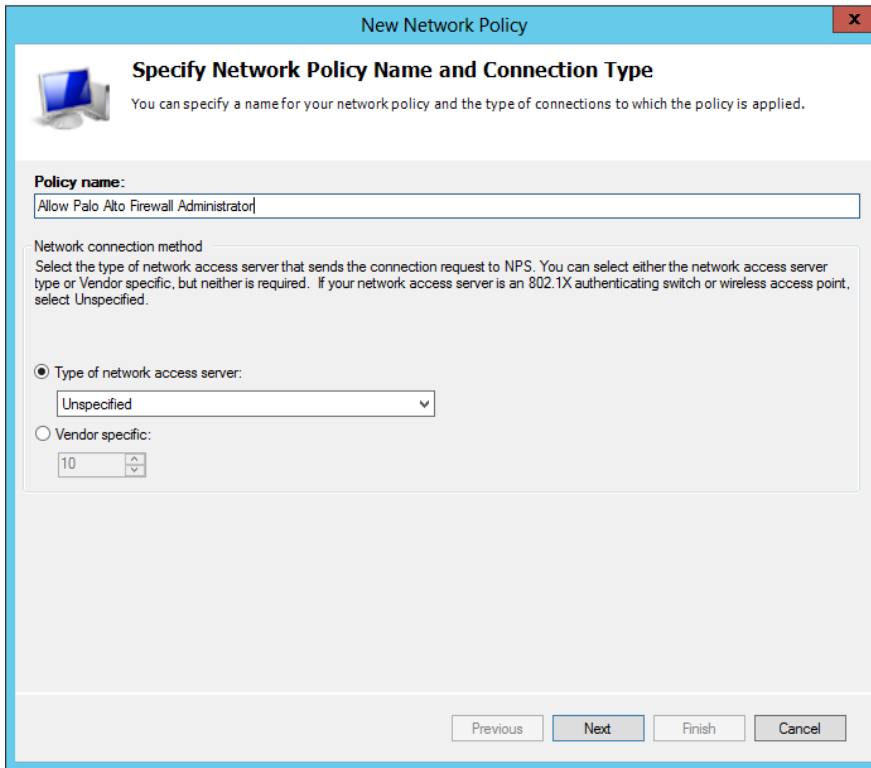
Previous Next Finish Cancel

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

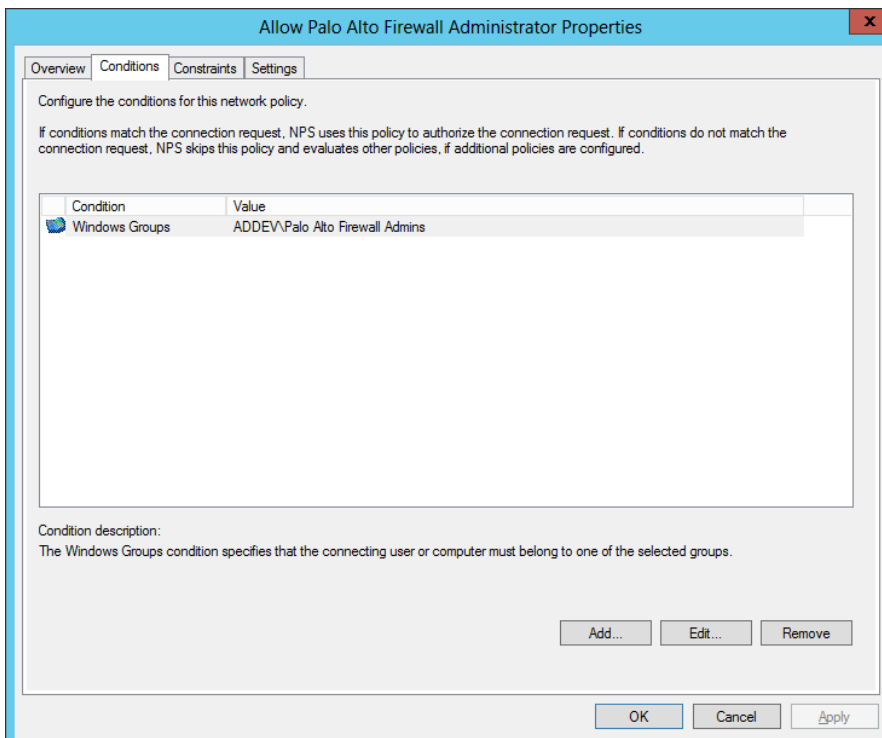


Create a Network Policy on Windows Server 2012 NPS

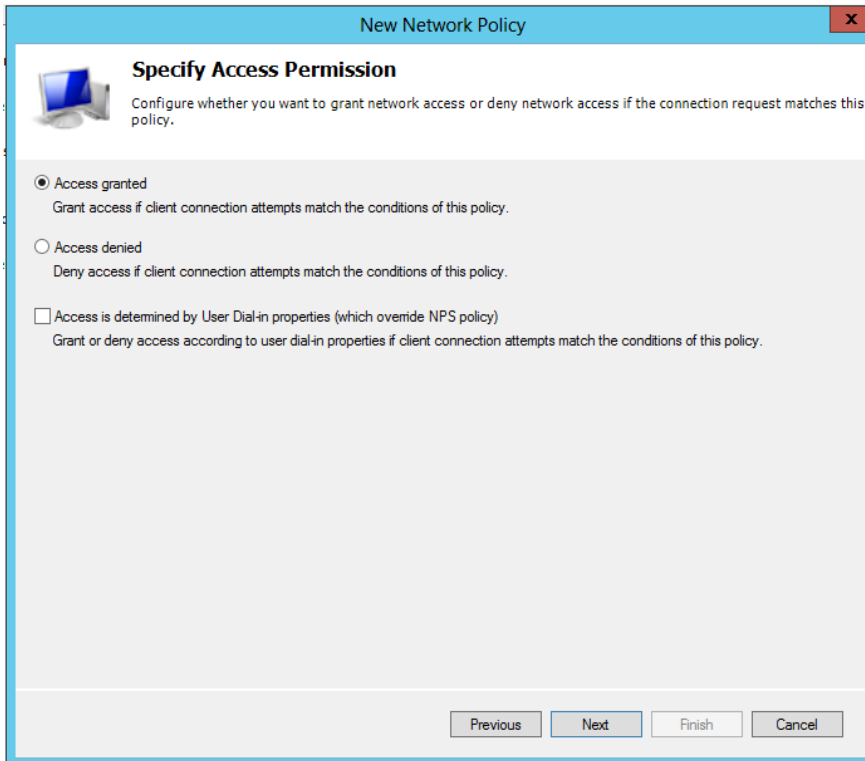
- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**



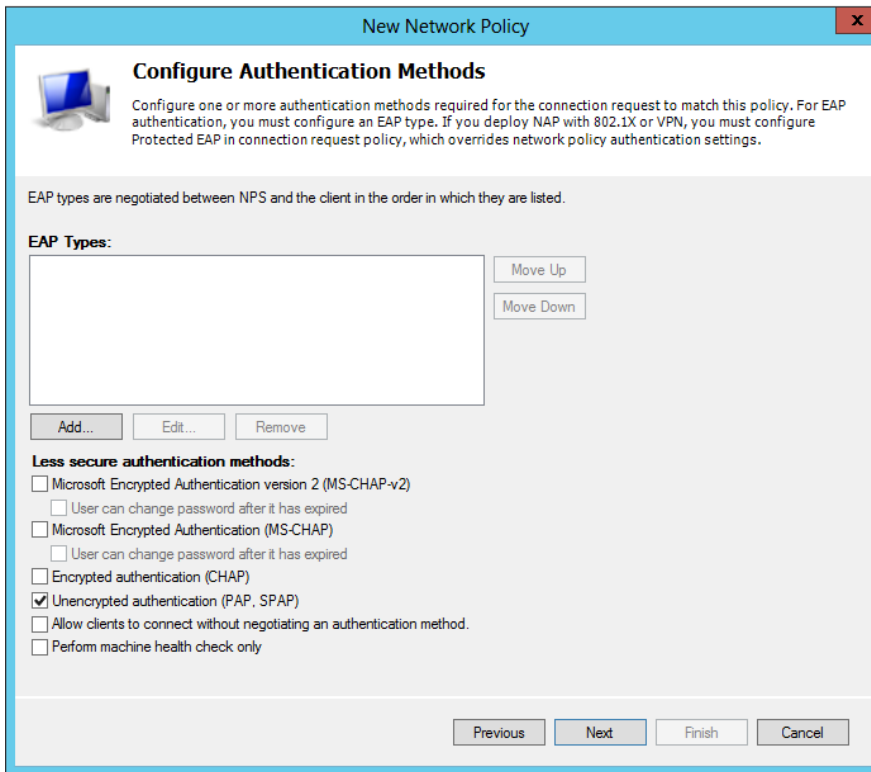
- On the **Specify Conditions** page, click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Palo Alto Firewall Admins* , and click **Next**



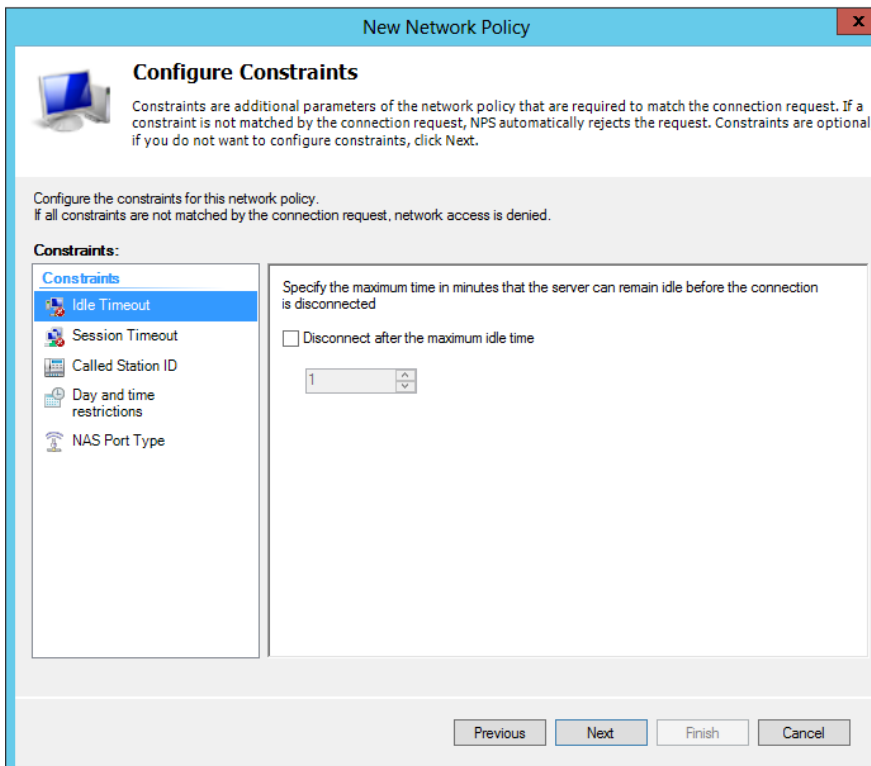
- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**



- 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**

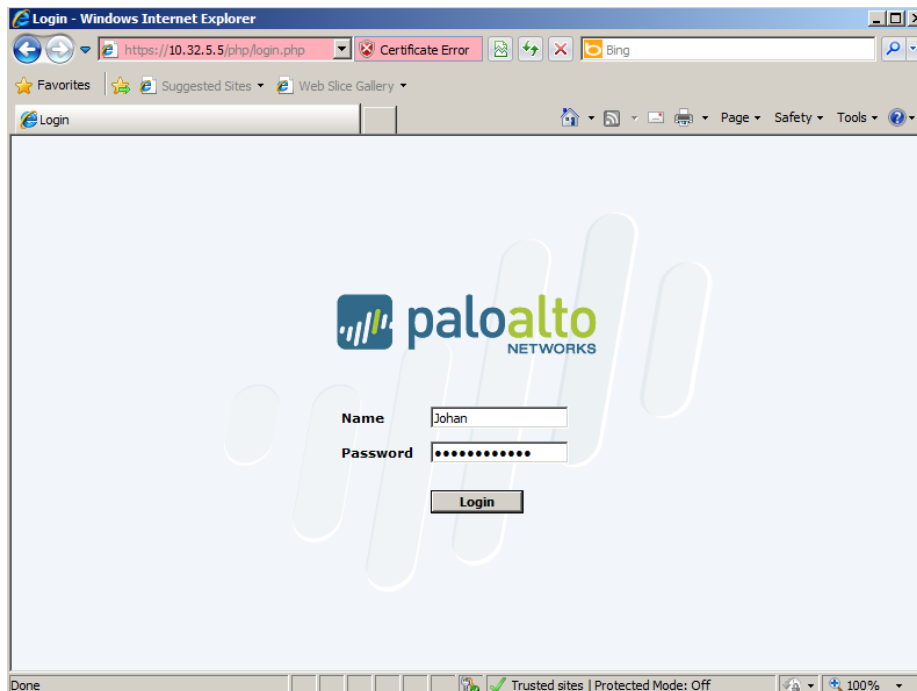
- On the **Vendor Add Specific Attribute Information** page, select **Custom**
- On the **Attribute Information** page, click **Add**
- On the **Vendor-Specific Attribute Information** page select **Enter Vendor Code**, type 25461, select **Yes, it conforms** and click **Configure Attribute**

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

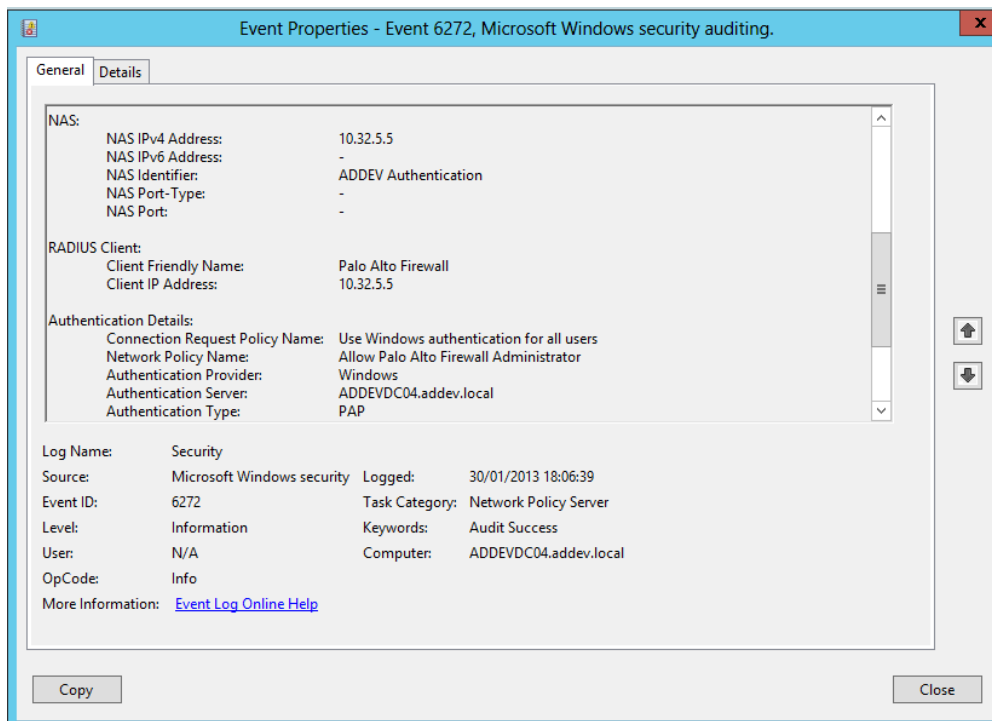
- Click multiple times **OK**, click **Next**
- On the **Completing New Network Policy** page, click **Finish**

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

Name	Value
Client Friendly Name	Palo Alto Firewall
Client IP Address	10.32.5.5
Connect Request	IAS_SUCCESS
Connect Result	Unknown
Duration	00:00:00
FQ User Name	ADDEV\Johan
NP Policy Name	Allow Palo Alto Firewall Administrator
Record Count	2
Server IP	10.32.5.5
Server Name	ADDEVDC04
Start DateTime	01/30/2013 18:06:39
Stop DateTime	01/30/2013 18:06:39
User Name	addev.local\Johan
Start Date	01/30/2013
Start Time	18:06:39
Stop Date	01/30/2013
Stop Time	18:06:39
Class	311 1 10.32.5.15 01/30/2013 17:00:53 4
SAM Account Name	ADDEV\Johan
Proxy Policy Name	Use Windows authentication for all users
SQ User Name	ADDEV\Johan
NAS Identifier	ADDEV Authentication
Debug Info	AutoClose=False; CalcDuration=0

- 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.