Authenticating users of Cisco NCS or Cisco Prime Infrastructure against Microsoft NPS (RADIUS)

Date: January 15, 2013

My hope with this guide is to help others take advantage of a centralized user database with their Cisco gear; in this case, Cisco NCS or Cisco Prime Infrastructure (PI). I will walk you through, step-by-step, on how to configure both sides of the puzzle and get users authenticated against a Microsoft Network Policy Server (NPS) using their Active Directory credentials.

Assumptions and Prerequisites:

- Cisco NCS or Cisco Prime Infrastructure has already been installed
- You know how to install Windows Server 2008 and add a role

Contents

Adding your RADIUS server to NCS or PI

Required:

- IP address of NPS Server
- Ports (only if changed from defaults)
- Shared secret*

I like to start on the Cisco side of this puzzle first. Why? Mainly because most of the troubleshooting and trial and error I did while making this guide was on the Microsoft side. So it's easier to start with the easy stuff and then start working on the harder parts at the end.

Step 1

There are a couple of requirements before you start this section. You will, obviously, need the IP address of your RADIUS / NPS server. If you changed the ports for Authentication, then you will need that as well. * The shared secret is if you already have a password in mind that you want to use. You could generate a shared secret from NPS, but that can be difficult to manage later down the line; although, it could be more secure with being random.

Step 2

Once you have this information, proceed to logging into your NCS or PI server using your current login credentials. You will need to navigate to the Administration tab and click on, "AAA". See figures 1 and 2.

Cisco NCS

Figure 1

Cisco Prime Infrastructure

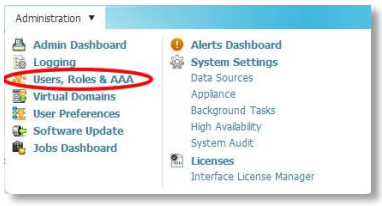

Figure 2

The sections on the left are sub-menus of where we need to be working to get authentication working against NPS. There are three sections that we will be working with:

- RADIUS Servers
- AAA Mode
- User Groups

We will be working with those and in that order.

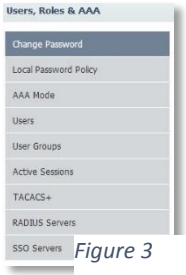

Figure 3

Step 3

We will add our RADIUS server to NCS or PI. Click on the link to the left of the screen labeled, "RADIUS Servers." You will be presented with a screen such as Figure-4.

Fill out these fields that you collected previously:

- Server Address is your NPS
- Authentication Port (if changed from default)
- Shared Secret
- Authentication type: ***PAP***[1]

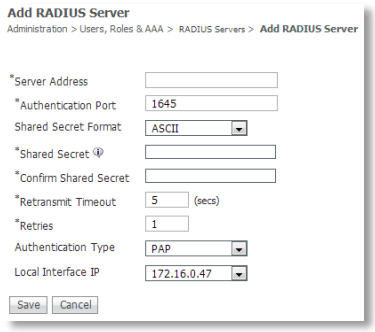

Figure 4

The **Local Interface IP** is what you are going to put into the RADIUS server as a RADIUS client. Keep this information for the NPS section.

Step 4

Once you finished configuring the RADIUS settings, click on "Save" and then on the left, click on "AAA Mode"

Your screen should now look like Figure-5

Select the "RADIUS" radio button.

I also like to check the box next to, "Enable fallback to Local". And from the drop down, "on auth failure or no server response".

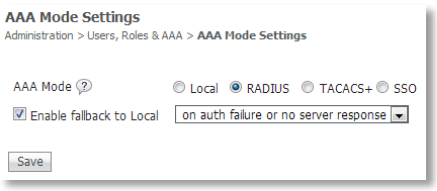

Figure 5

[1] I haven't done extensive testing on CHAP. But from my brief testing of it it didn't work with NPS. I have not gone down the path of using certificates just yet. That will be my next step and guide.

Just in case my NPS server is having issues or someone without AD credentials needs to connect (a consultant, maybe?)

Almost done with the Cisco part…

Gathering the RADIUS Attributes from NCS or PI

Step 5

This next part is where we gather some more important information before we head off to the NPS side of things.

On the left, click on “User Groups.” Your screen should look similar to Figure-6

For configuration purposes, I’m going to use the group name, “Admin”

The level of access you give staff your staff is up to you.

Click on the “Task List” link that is on the same row as the “Admin” group name.

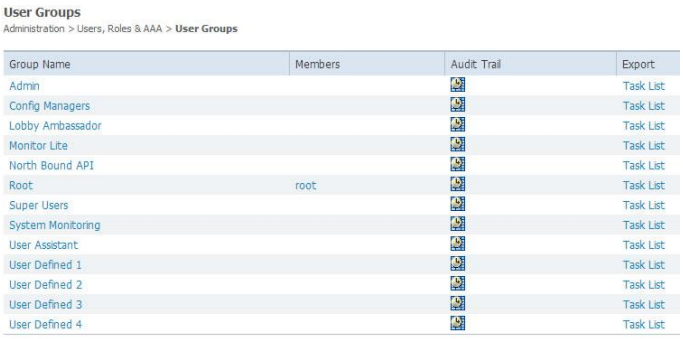

Figure 6

You should see a similar screen as in Figure 7.

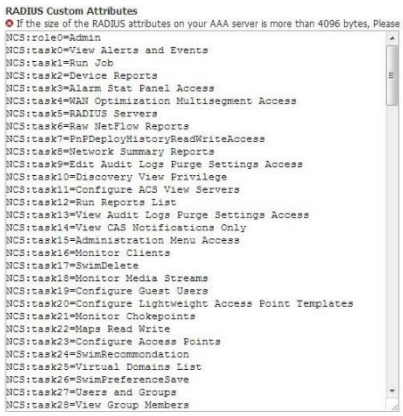

Figure 7

** IMPORTANT **

This is where the differences in NCS or PI come into effect.

For NCS, you need to copy every single role and task in the Task List as seen on the left in Figure 7. For the “Admin” and “Root” group names, this could be over 100 tasks that you need to import into NPS. You will also need the “virtual domain,” which I will discuss shortly.

However! With Prime Infrastructure, you only need to copy two things: The role, in this example it would be, “***NCS:role0=Admin***”

And the second would be the virtual domain.

You can find the link to what Virtual Domains you have on your NCS or PI installation by scrolling or looking at the bottom of your task lists screen. Find the link at the bottom.

Figure 8

Click on the link and you will see the RADIUS attributes for the virtual domain.

Figure 9

Gather all these RADIUS attributes up and put them in notepad for the next section of configuring Microsoft NPS.

Configuring Microsoft NPS – adding RADIUS clients

I'm not going to go through the steps of adding a role to your windows server. You should already know how to do this.

However, after the NPS role has been added, some people forget to do this step. You need to register your NPS server with Active Directory.

Open up your NPS console and then right-click on the NPS logo, see figure 10.

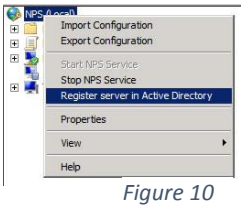

Figure 10

Once you do that we can now add your RADIUS clients. That is, the devices on your network at will be contacting the NPS server for authentication.

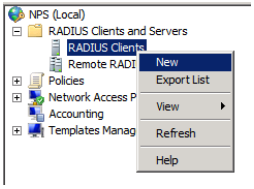

Figure 11

Expand the folder, "RADIUS Clients and Servers." Then right-click on, "RADIUS Clients" and select "new."

You will then see a screen like the one in figure 12.

Give your client a “friendly name,” something that is easy to remember or that conforms to your companies nomenclature.

Enter in the IP address. This was gathered back in Step 3 and was the “Local Interface IP” of your NCS or PI server. See Figure 4.

Then enter in the shared secret that you created.

** Please double check to make sure the shared secret is accurate.

I leave the advanced tab at their defaults.

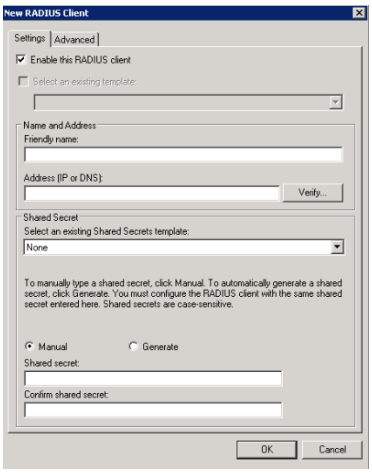

Figure 12

Configuring Microsoft NPS – creating network policy

Now comes the fun part! </sarcasm>

If you are using Cisco NCS, then it isn’t that fun.

In your NPS console, expand “Policies” and right-click on the “Network Policies” folder and select, “New”

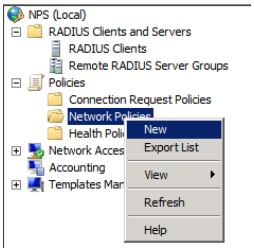

Figure 13

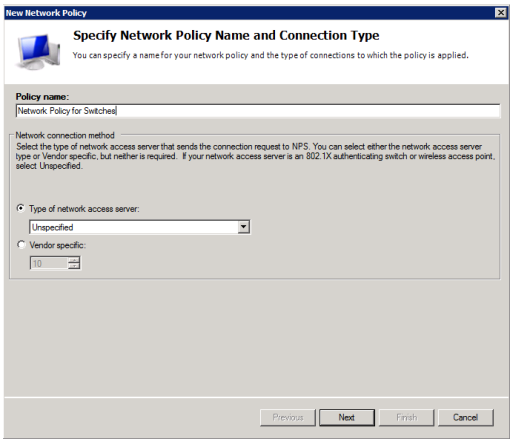

Figure 14

Give your new network policy a name.

Click ‘Next’

On the ‘Specify Conditions’ page, click on “Add”.

I use Active Directory groups for easier management of users who can access our network equipment.

Double click on “Windows Groups”

- Click on “Add groups” button
    - Find and add your Active Directory groups to the list.
- Select, OK.
- Select, OK
- Next

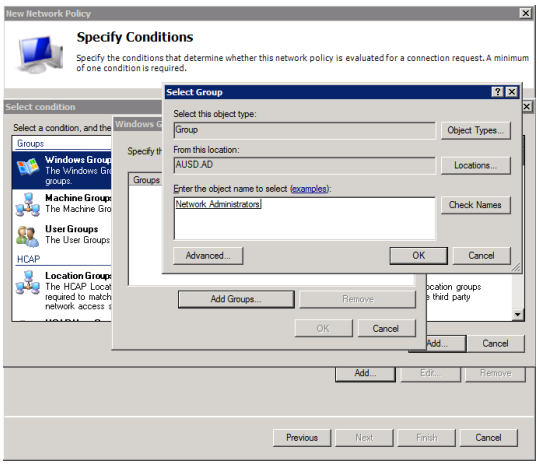

Figure 15

On the next screen. Make sure the “Access granted” radio button is selected and select “Next”

On this screen, “Configure Authentication Methods” I enable, “Encrypted authentication (CHAP)” and also, “Unencrypted authentication (PAP, SPAP)”

*** Note – I have not configured SSL certificates with NCS or PI. I will try that later and update this guide. If you have installed an SSL certified for your NCS or PI server. You will probably need to do two additional steps.*

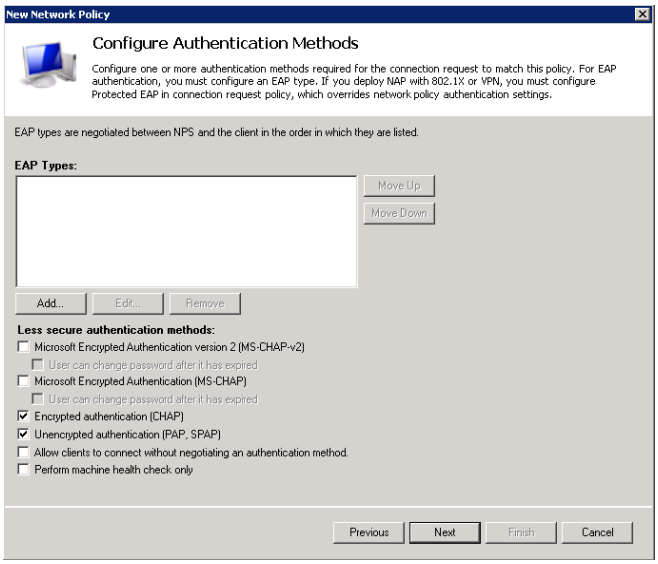

Figure 16

1) *That is create a certificate template in your Microsoft CA server and auto-enroll your NPS servers*
2) *Instead of selecting CHAP or PAP in this section, you will hit the “Add” button and select “PEAP”*
    a. *This option is only available when you do step one of adding the certificate to your NPS server.*
3) *Enable PEAP in your NCS or PI server. See Step 3 from above or Figure 4 from above*

Once you select the correct methods, hit “Next”

You can skip the section, “Configure Constraints” if you want. This is where you configure timeouts for idle or sessions. Hit, “Next”

Now here comes the hard part for you NCS customers.

This is where we configure all those task lists that we gathered from NCS or PI.

The first step is under the section, “RADIUS Attributes” and select “standard”.

You will need to remove the two Attributes already configured: “Framed-Protocol” and “Service-Type”

Then select “Vendor Specific” on the left-side of the menu.

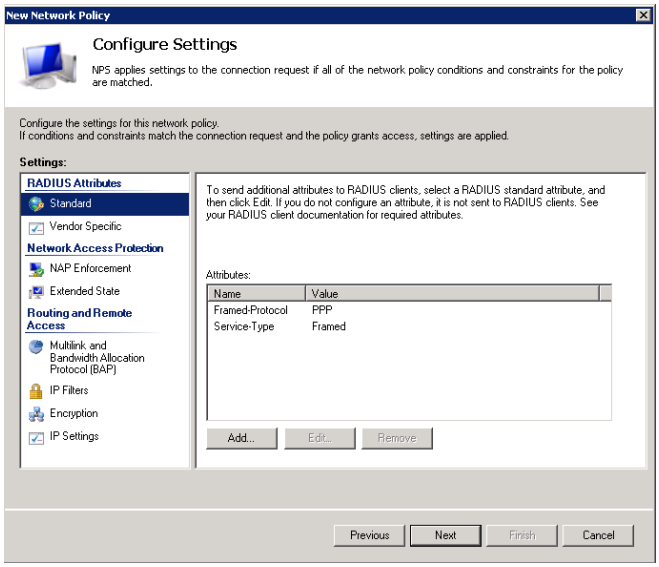

Figure 17

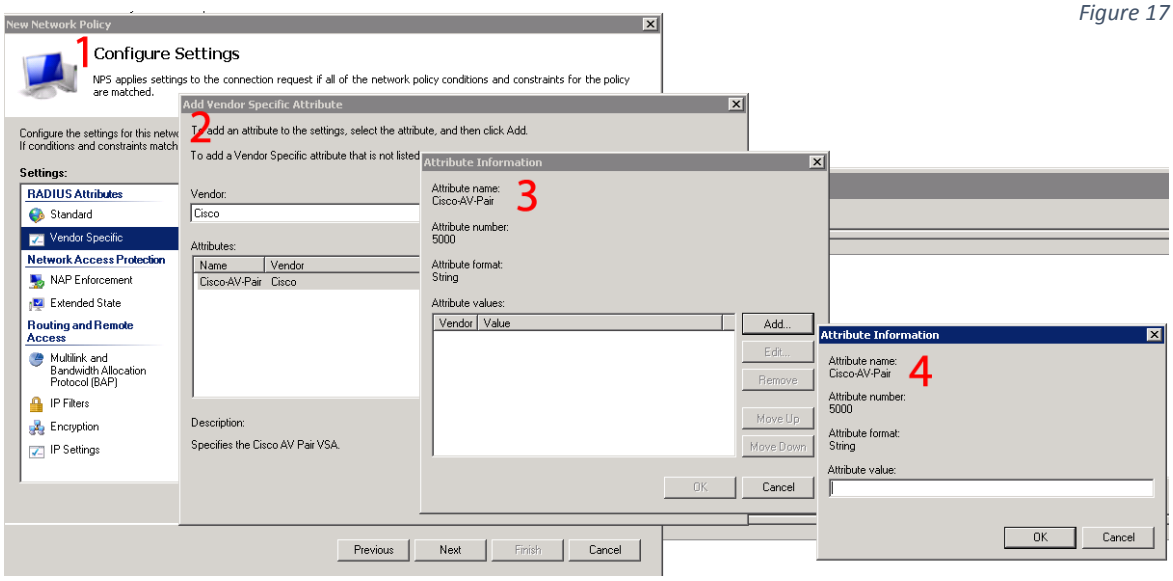

Figure 18

1) Select “Vendor Specific” from the left-side menu.
    a. Then hit the “Add” button
2) From the “Vendor” drop-down menu, select “Cisco”
    a. Double click on “Cisco-AV Pair”
3) On the Attribute Information page, select “Add”
4) Another window will pop up. This is where you are going to add all your Task list items from NCS and the roles and virtual domains.

Here is a screenshot of all the NCS roles added for the group, “Admin”:

Cisco NCS	Cisco Prime Infrastructure
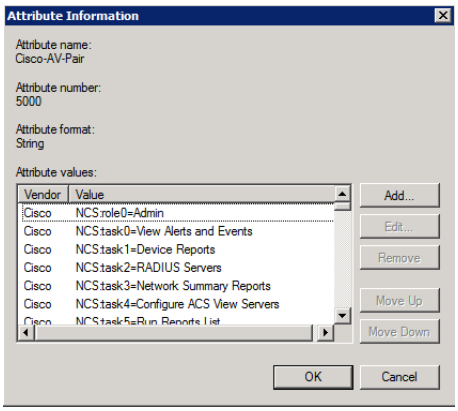	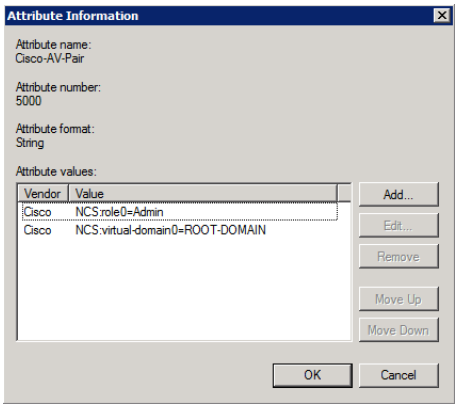
Figure 19	*Figure 20*

Once all the tasks have been entered. Press OK a few times to exit back out to the main “Configure Settings” screen. In Figure 18, it is labeled #1

Click, “Next”

The last screen is an overview of the settings you have configured. Click, “Finish”

If all goes well, you should be able to authenticate using your Active Directory user credentials.