Tech Art: TA0001-Windows 2008 RADIUS for CISCO Device Authentication by John McManus

Network Device Authentication

It is not uncommon to discover infrastructures with authentication policies in place for Windows Admin Access using Active Directory accounts, only to find the network devices are being accessed using a common user name and password. It would be ideal if the Active Directory accounts that are used to administer the Windows environment could be used to administer the network devices too. (This article is specific to Cisco Network Devices)

One solution is to purchase a Cisco Secure Access Control Server, this can use accounts in the Active Directory. The product is quite extensive and has many more feature than just logon authentication.

- Device administration: Authenticates administrators, authorizes commands, and provides an audit trail
- Remote Access: Works with VPN and other remote network access devices to enforce access policies
- Wireless: Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control: Communicates with posture and audit servers to enforce admission control policies

An alternative would be to use the Network Policy Access Server from Windows 2008, this was previously known as the Internet Authentication Service (IAS) from Windows 2003. Here is a list of features:

- Device administration: Authenticates administrators, authorizes commands levels
- Remote Access: Works with VPN and other remote network access devices to enforce access policies
- Wireless: Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network access protection: client health policy creation, enforcement, and remediation technology

Actually the previous IAS version could achieve the first three functions, so what we are doing here with Windows 2008 NPS we can also do with Windows 2003 IAS. The Cisco ACS does have much deeper features when using TACACS+ for authorising specific command, detailed audit trails and access lists, but the Microsoft Solution still has enough features that make the Microsoft solution ideal for smaller businesses.

I would also predict that Network Policy Server(NPS) will see more adoption in infrastructures to take advantage of Network Access Protection (NAP) which although in its early days, has a lot of potential, and will definitely be the subject of Future Tech Arts.

One frustrating part of the previous IAS and now with NAP is that there is **NO** built in feature to replicate the policy to another NPS server. So if we define multiple RADIUS Servers in our network device configurations we need to ensure that the same policy is presented on each NPS. This could be achieved by manually creating identical policies on each server or performing an export/import process to copy the configuration from one NPS to another; this will ensure policy consistency across NPSs. Therefore when designing and placing NPS servers it is a good idea to logically highlight one as being the Master where you do all the administration.

Command to export the configuration

```
Netsh nps export filename=”backup.xml” exportPSK=YES
```

Command to import the configuration

```
Netsh nps import filename=”backup.xml”
```

One solution I have implemented in the past is to run a scheduled task that exports the policy from the “master” server and copies the output to each of the “slave” servers, the slave server then has a scheduled task which imports the policy.

TIP : For Working with multiple NPS servers with common policies

- ***Logically identify a “Master” NPS server and make all policy updates here.***

Rationale

- ***By making changes in the same place these change can be knowingly exported from the “Master” server and imported to other NPS server ensuring consistent policies across NPS server.***

That enough background lets configure NPS for Cisco Device authentication.

Overview

The RADIUS server can be installed on an Active Directory Domain controller or on a Windows Server in the domain. Windows 2003 Enterprise Edition was required to support more that 50 radius clients, I have been unable to find if there are any such limitations with the Windows 2008 SKUs.

Each device must be configured as a RADIUS client in the NPS, the RADIUS Key must match the key specified on the remote access device. In NPS you have the option of automatically generating the key. To transfer the key to the Cisco device I recommend copying it into notepad, then whenyou are doing the Cisco part; copy and paste into the configuration, using this method you can create multiple clients in NPS and paste all their keys into notepad without having to jump between NPS and the Cisco Terminal Session. Always destroy the notepad file once the Cisco configuration has been completed.

A remote access policy should then be created to allow specified users

TIP: To provide added security between the Cisco devices and the RADIUS server:

- ***The shared secret key should be at least 22 characters long and consist of a random sequence of upper and lower case letters, numbers, and punctuation. This will ensure maximum protection of the key. Luckly now the NPS will generate a secret key longer than 22 characters.***
- ***Each client should be configured with a different key.***

Note: The authentication mechanism is limited to PAP for Cisco device which is unencrypted; however RADIUS will encrypt the password over the network to the RADIUS server. This is why a strong key is required.

Steps Required

So what needs to be done to get the NPS to provide logon authentication and access control for Cisco Devices.

The basic steps

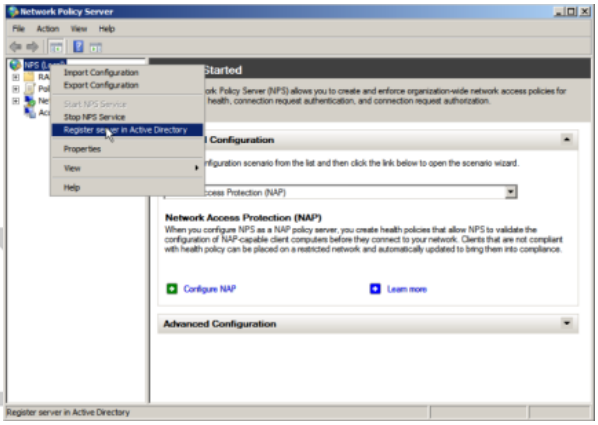
- Install the Network Policy and Access Service **Role**
- Register in Active Directory
- Configure the RADIUS Client Settings
- Configure the Access policy
- Configure the Cisco Device

Install the Network Policy and Access Service Role

- From the Initial Configuration Task Windows ->Click Add a Role
- Select the “Network Policy and Access Server Role”
- Select the Role Service “Network Policy Server” – This is all that is require to provide RADIUS authentication for our Cisco devices

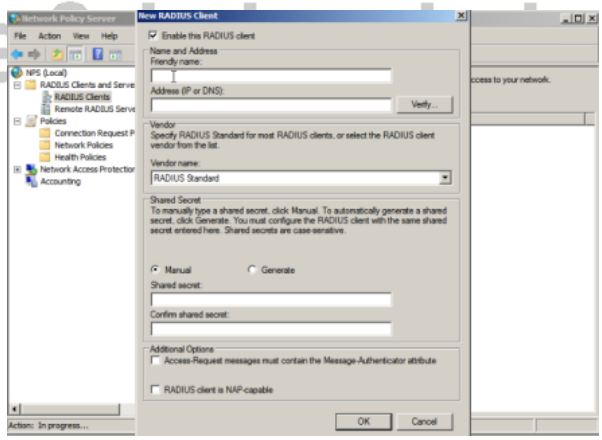
Register in Active Directory

- Once the Role has been configured then we can continue with the NPS configuration. You can find the NPS console under administrative tools
- Right Click NPS (local) and Select Register in Active Directory



Configure the RADIUS Client Settings

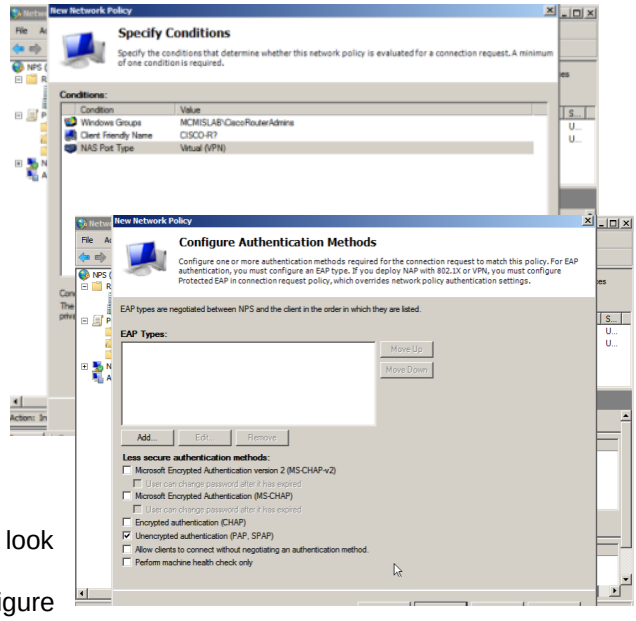
- In the RADIUS Client and Server Folder Right Click RADIUS Client and Select New RADIUS Client
- Enter Friendly Name and IP address of the Cisco Device
- Select Cisco as the RADIUS Vendor
- Click Generate to make a unique RADIUS key (make sure you copy this somewhere you can access it later to paste into the Cisco Device)



Note:
There is no message authenticator available on Cisco Routers at the time of writing.
The Cisco network devices are not NAP Capable at the time of writing.

TIP: Using a standard name format for the device will allow you to use wildcard matching in the policy to identify the device.

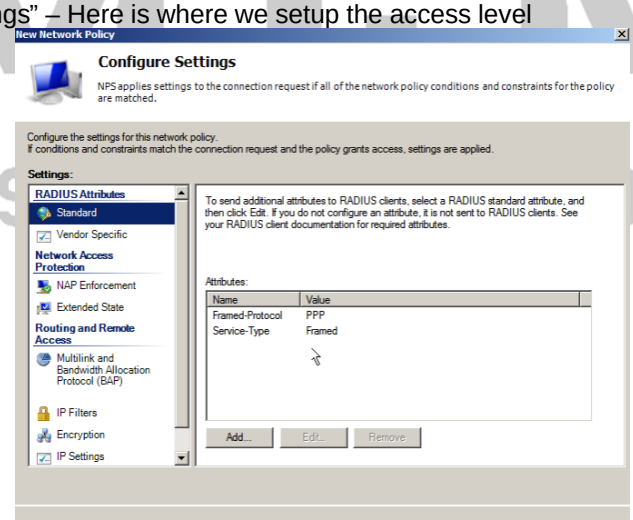
Configure the Access policy



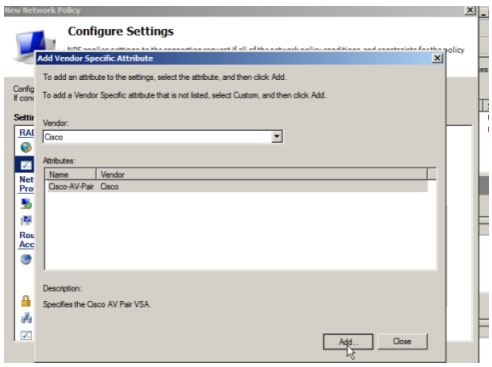
- Right Click the Network policy and Select New
- Enter a Policy Name (Leave as unspecified)
- Enter a Windows Group Condition – Enter the name of the group from AD who should have access
- Enter a Client Friendly Name as a Condition – Enter the name of the RADIUS Client (we can use wild cards here so "CISCO–R?" would match multiple RADUIS Clients
- Enter a NAS-Port-Type as a condition – Select Virtual (VPN)
- Specify Access Granted in Specify Access Permissions
- Configure Authentication Method as PAP
- You can select No when asked if you want to look up the help file.
- There are no setting necessary in the "Configure Constraint"

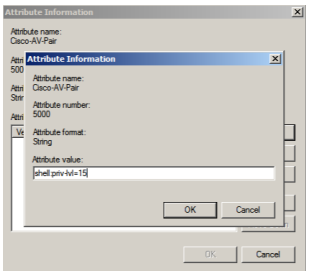
TIP-To see which policy has been match you can check out the log file, located in c:\windows\system32\log. Information is also logged in Security Event Log: Source=Microsoft Security Auditing, Task Category=Network Policy Server

- "Configure Settings" – Here is where we setup the access level



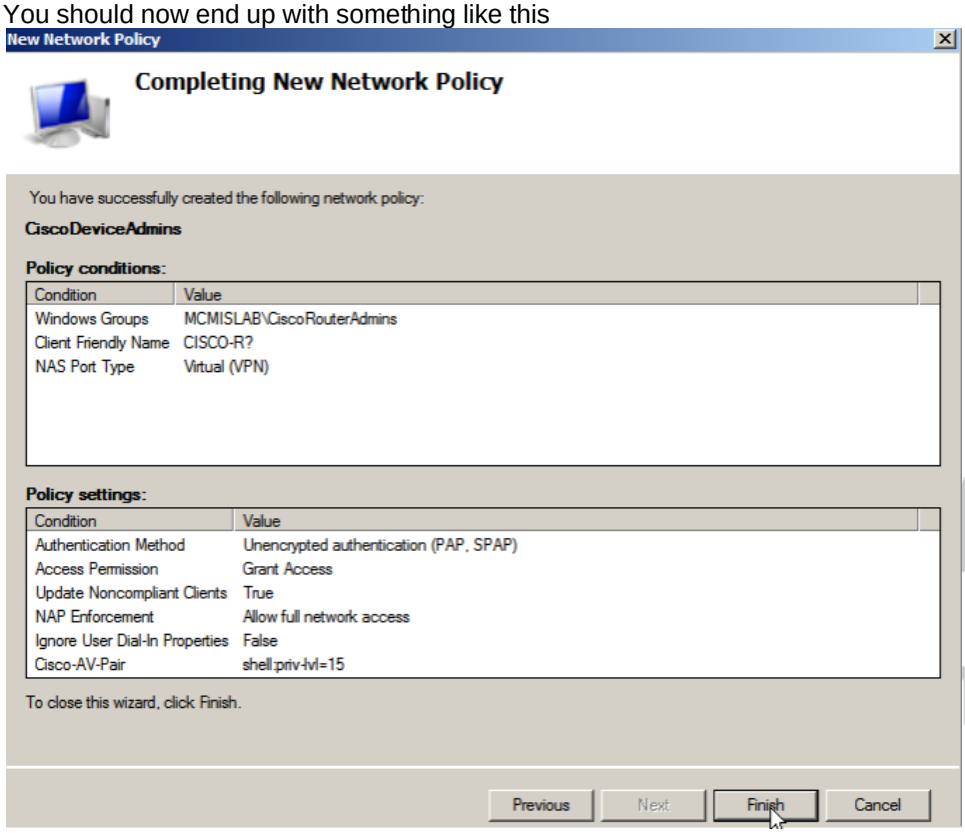
- Remove Frame-Protocol PPP
- Remove Service-Type Framed
- Select Vendor Specific





- Now Add Cisco Vendor Attribute AV=Pair
- Add Attribute Shell:priv-lvl=15

You should now end up with something like this



Tip – Which commands can be accessed
You could create another group and grant them access to level1 show command, so you have read-only type access to devices. This is achieved by changing shell:priv-lvl=?? To the appropriate level.

Configure the Cisco Device

The device in the following example is a Cisco router, and only the key lines are shown

```
01:aaa new-model

02:aaa group server radius RADIUS_AUTH

03:server x.x.x.x auth-port 1812 acct-port 1813
```

```
04:server x.x.x.x auth-port 1812 acct-port 1813

05:aaa authentication login networkaccess group RADIUS_AUTH enable

06:aaa authorization exec default group RADIUS_AUTH if-authenticated

07:ip radius source-interface FastEthernet 0/1

08:radius-server host x.x.x.x auth-port 1812 acct-port 1813 key min22charkey

09:radius-server host x.x.x.x auth-port 1812 acct-port 1813 key min22charkey

10:line vty 0 15

11:exec-timeout 0 0

12:login authentication networkaccess
```

01: Switch to Access Authentication, Authorisation and Accounting new command set
02: configure a radius group "RADIUS_AUTH" to logical group RADIUS Servers
03: specify primary RADIUS server as part of "RADIUS_AUTH"
04: specify backup RADIUS server as part of "RADIUS_AUTH"
05: define "networkaccess" as a logical name to apply logon and enable access to
06: allow RADIUS_AUTH users access to exec mode
07:specifies the interface RADIUS uses as the source.
08: specify secret key for primary RADIUS server
09: specify secret key for backup RADIUS server
10: modify the telnet access
11: set the time out for the login session
12:assign networkaccess from 05: for Login access

Now we can logon to the Cisco Device via telnet using your Active Directory account name.

Summary

Configuring RADIUS authentication for Cisco Devices against Active Directory does not require a large investment in new infrastructure. There are some very simple steps that can be performed to allow Active Directory accounts to be used for accessing the network infrastructure components. The article also provides a first look at the Windows 2008 NPS which no doubt has some interesting potential for the future with Windows 2008.

There are additional video clips showing how to configure NPS for RADIUS authentication with Cisco Devices MCM Infrastructure Solutions Technical Articles - http://www.mcmis.co.uk/TechArt/Technical%20Articles.htm