Deploying IPsec Server and Domain Isolation with Windows Server 2008 Group Policy - Part 2

In this part 2, we'll move on to the second step, which is the step to install and configure the Network Policy Server, the Health Registration Authority and the subordinate CA.

Picture 1 of Deploying IPsec Server and Domain Isolation with Windows Server 2008 Group Policy - Part 2

Deploying IPsec Server and Domain Isolation with Windows Server 2008 Group Policy - Part 1
Thomas Shinder

TipsMake.com - *In part 1 of this series, we introduced you to using IPsec implementation with NAP 'health' policies, which introduced an example network and pointed out the The most basic step required for NAP to work with IPsec enforcement policy.*

Below is a list of steps to implement the solution.

• Configuring Domain Controller
• Install and configure Network Policy Server, Health Registration Authority and Subordinate CA (subordinate CA)
• Configuring NAP IPsec Enforcement Policy on the Network Policy Server
• Configure VISTASP1 and VISTASP1-2 for testing
• Test Health Certificate and Auto-remediation Configuration
• Verify NAP Policy Enforcement on VISTASP1
• Configure and test IPsec policies

In the first part of this series, we introduced the steps needed to configure domain controllers in NAP with the IPsec execution environment. In this part 2, we'll move on to the second step, which is the step to install and configure the Network Policy Server, the Health Registration Authority and the subordinate CA.

Install and configure Network Policy Server, Health Registration Authority and subordinate CAs.

Let's first consider the Network Policy Server section. Network Policy Server or NPS takes care of the RADIUS server role. NPS is the new name given to Microsoft's previous Internet Access Server (IAS) name. There are two main components to the new NPS server: the RADIUS component (this is a component that includes new support for NAP) and the RRAS component. We will not mention the RRAS component in this scenario, so we will not install and configure RRAS. We need to do the following steps to create an NPS server with the Health Registration Authority and the CA Under the bow is installed and configured on this machine:

• Add a network policy server to the NAP Exempt Group

• Restart the Network Policy Server
• Request a computer certificate for the Network Policy Server
• See the computer certificate and health certificate installed on the Network Policy Server.
• Install Network Policy Server, the Health Registration Authority and the Subordinate CA (lower level CA).
• Configure Subordinate CA on the Network Policy Server
• Activate the permissions for the Health Registration Authority to request, issue, and manage certificates.
• Configure the Health Registration Authority to use a subordinate CA to issue 'health' certificates.

Let's take a closer look at each of these steps.

Add the Network Policy Server to the NAP Exempt Group group

We need to set the **WIN2008SRV1** computer to become a member of the NAP Exempt Group so that it can automatically enroll the created health certificate. This will allow this computer to act as a NAP policy server and the Health Registration Authority in communicating with other computers on a secure network, even if this computer does not meet NAP requirements. .

Perform the following steps on the domain controller of WIN2008DC computer:

1. On **WIN2008DC** , click **Start** , point to **Administrative Tools** , and then click **Active Directory Users and Computers** .
2. In the left pane of the **Active Directory Users and Computers** console, expand the **msfirewall.org** section, then click the **Users** button.
3. Double-click the **NAP Exempt** group in the right pane of the console.
4. Click the **Members** tab, click **Add** , click **Object Types** , select the **Computers** check box, and then click **OK** .

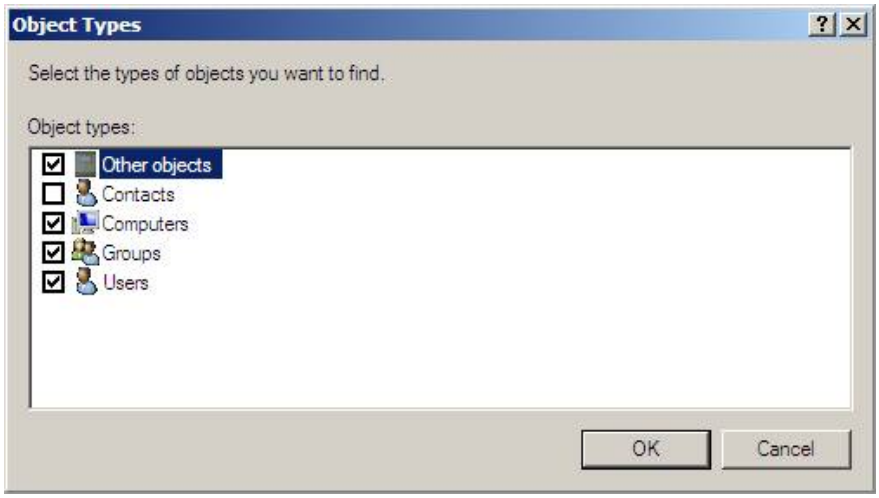

Figure 1

5. In **Enter the object names to select (examples)** , type **WIN2008SRV1** , then click **Check Names** . Click **OK** , and then click **OK** in the **NAP Exempt Properties** dialog box.

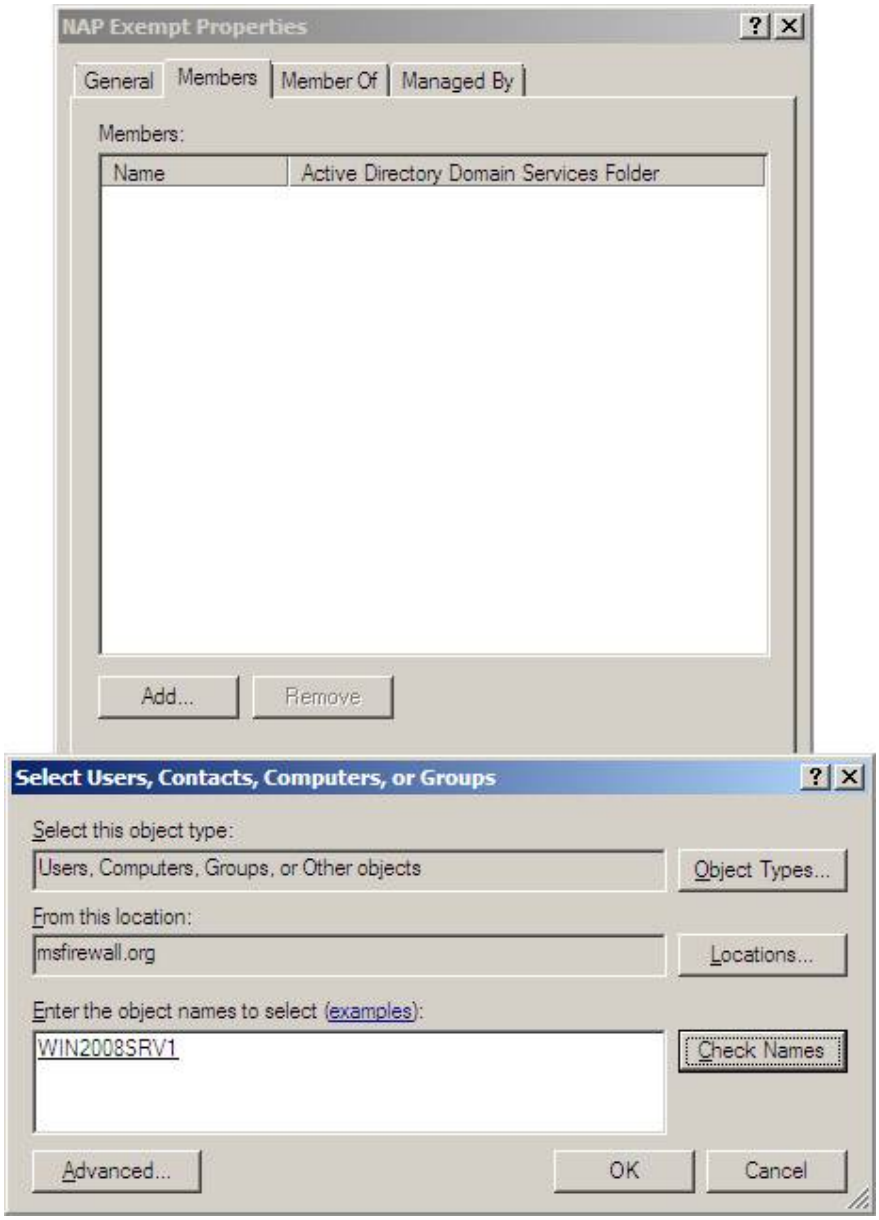
NAP Exempt Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Add...
Remove
Select Users, Contacts, Computers, or Groups
Select this object type:
Users, Computers, Groups, or Other objects
Object Types...
From this location:
msfirewall.org
Locations...
Enter the object names to select (examples):
WIN2008SRV1
Check Names
Advanced...
OK
Cancel

Figure 2

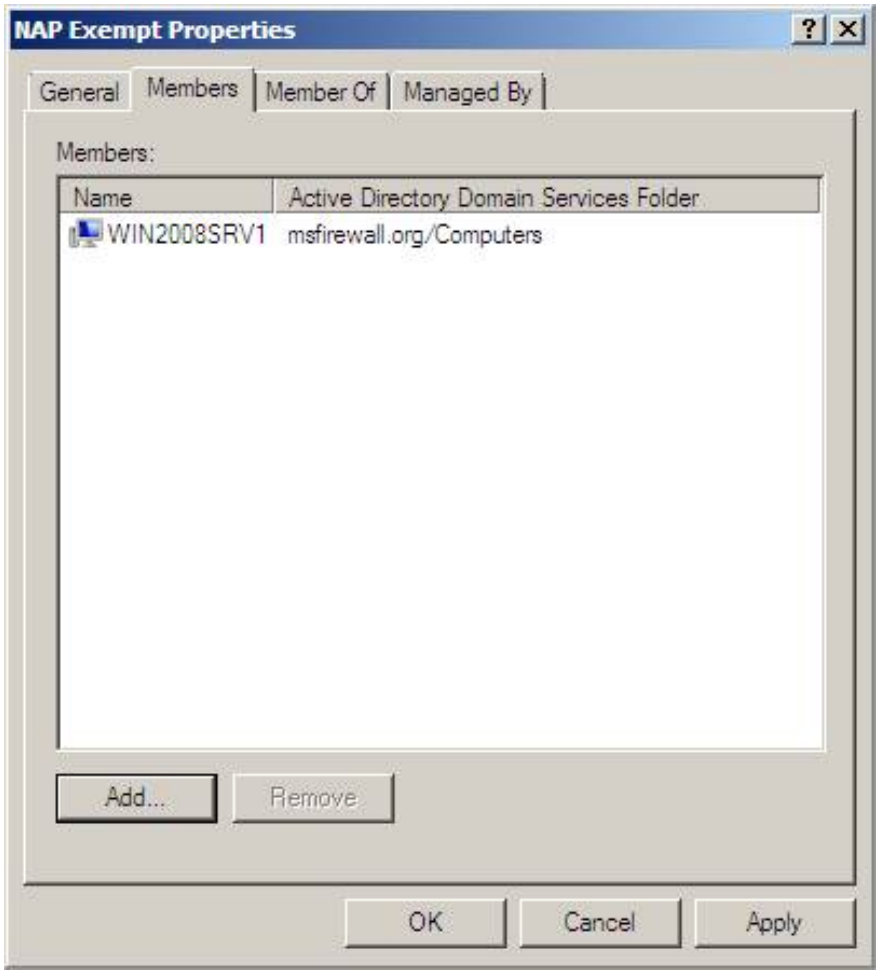

Figure 3

6. Close the **Active Directory Users and Computers** console

Restart the Network Policy Server

To enable new domain member settings and security group members, restart **WIN2008SRV1** .

1. Restart **WIN2008SRV1** .
2. After your computer restarts, log on to the computer under the administrator account.

Request a computer certificate for the network policy server

The **WIN2008SRV1** machine needs a certificate to support SSL connections for the server. SSL connections will come from NAP clients when they connect to the Health Registration Authority Web server on the NPS server. Note that in this example, the NPS server and the Health Registration Authority are on the same machine. However, it is not required to do so - you can put the Health Registration Authority and NPS server on different machines. In that scenario, you need to install the NPS service on the HRA computer and configure that computer to be a RADIUS proxy, since the HRA is a network access server in this scenario and the NAS needs to declare the NPS service. client state.

Perform the following steps on **WIN2008SRV1** NPS machine:

1. On the **WINS2008SRV1** machine, click **Start** , click **Run** , type **mmc** , and then press ENTER.
2. Click **File** , and then click **Add / Remove Snap-in** .
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates** and then click **Add** . In the **Certificates snap-in** dialog box, select the **Computer account** option and click **Next** .

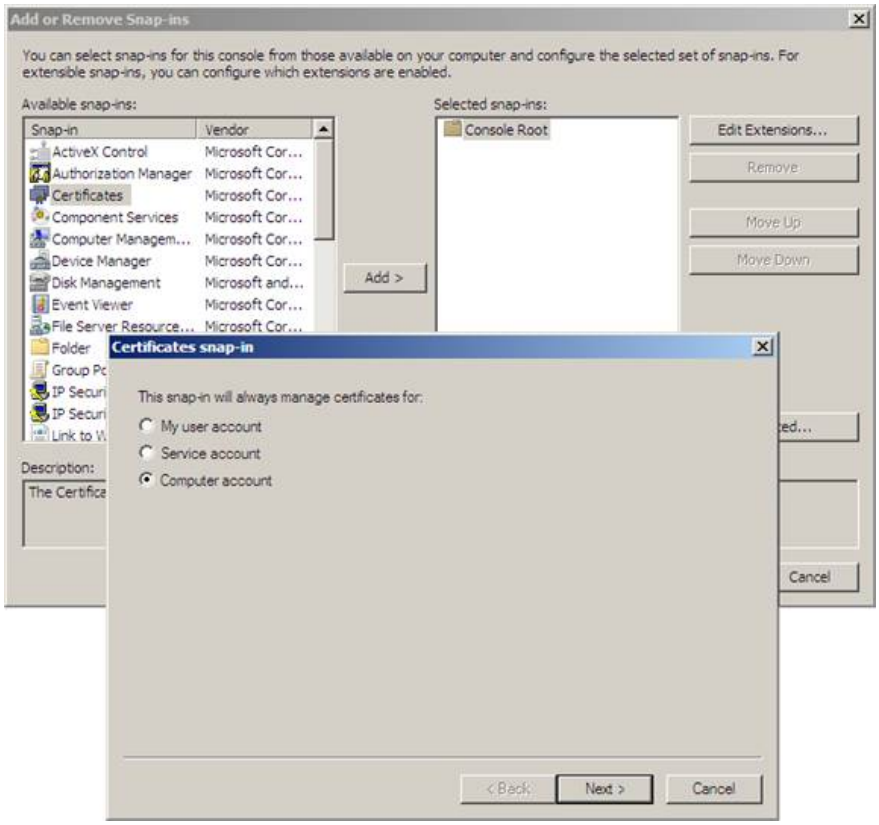

Figure 4

4. In the **Select Computer** check box, select the **Local Computer** option and click **Finish** .

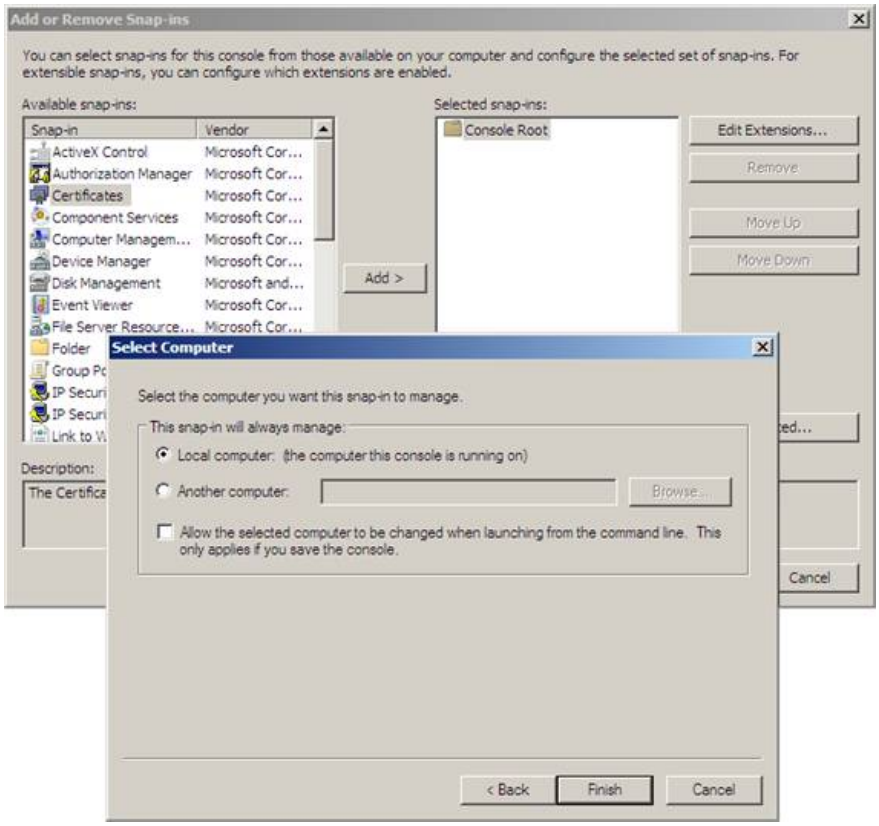

Figure 5

5. Click **OK** in the **Add or Remove Snap-ins** check box.

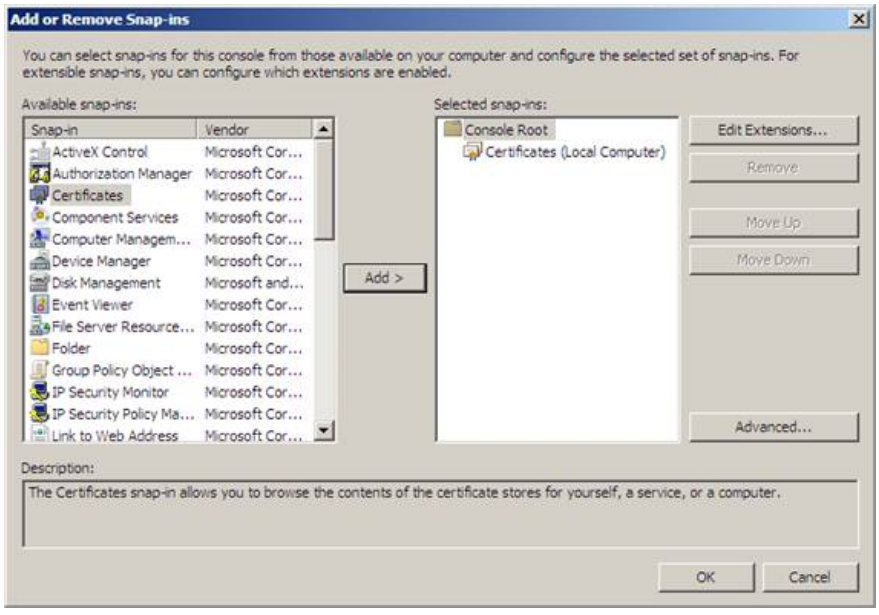

Figure 6

6. In the **Certificates** console, open the **Certificates (Local Computer) button** , then open **Personal** . Click the **Certificates** button, right-click it and point to **All Tasks** then click **Request New Certificate** .

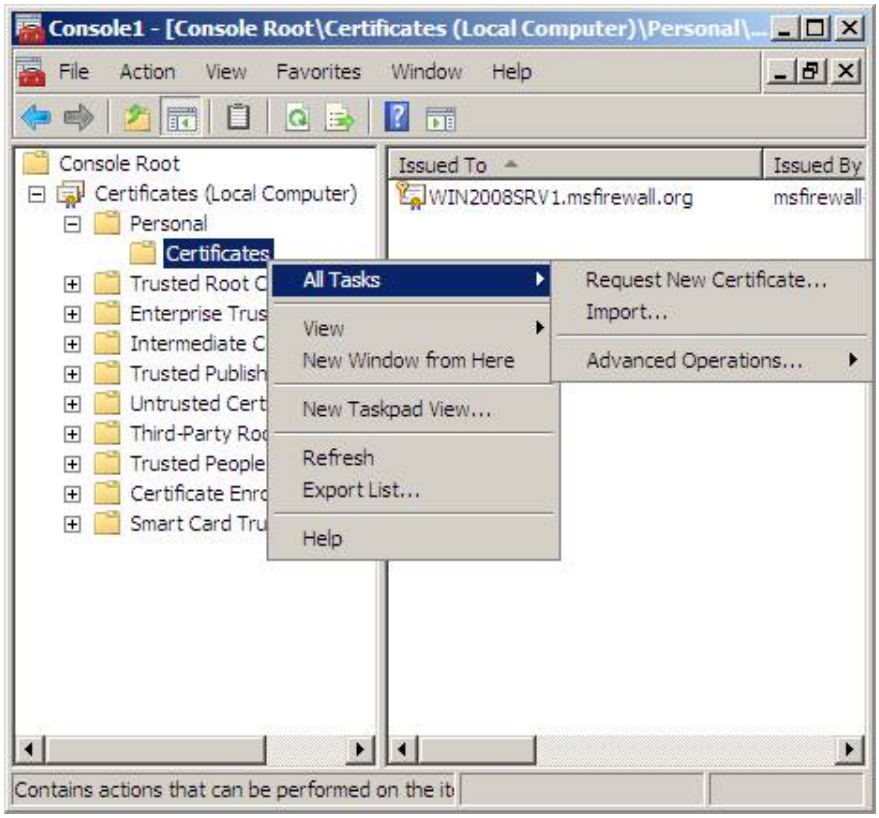

Figure 7

7. Click **Next** on the **Certificate Enrollment** page.

On the **Request Certificates** page, you can see a list of certificate templates available on this computer. Note that, although there are many certificate templates available, there are only a few templates for this machine, which are based on permissions configured for certificate templates. Check the **Computer** check box and click **Enroll** . Note that you can perform the details of this certificate by clicking the **Properties** button.

Figure 8

8. Click **Finish** in the **Certificate Installation Result** dialog box.

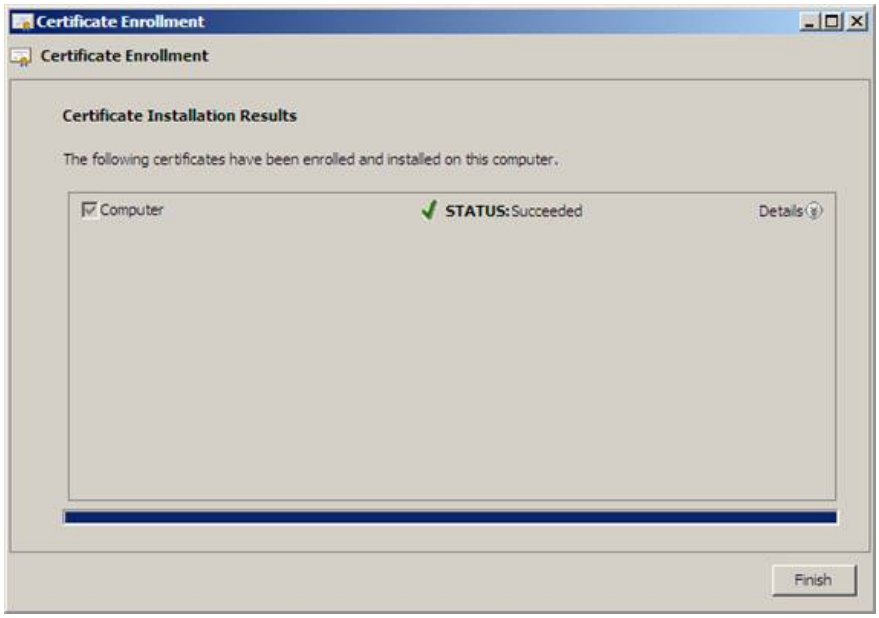

Figure 9

9. Leave this window for the next procedure below.

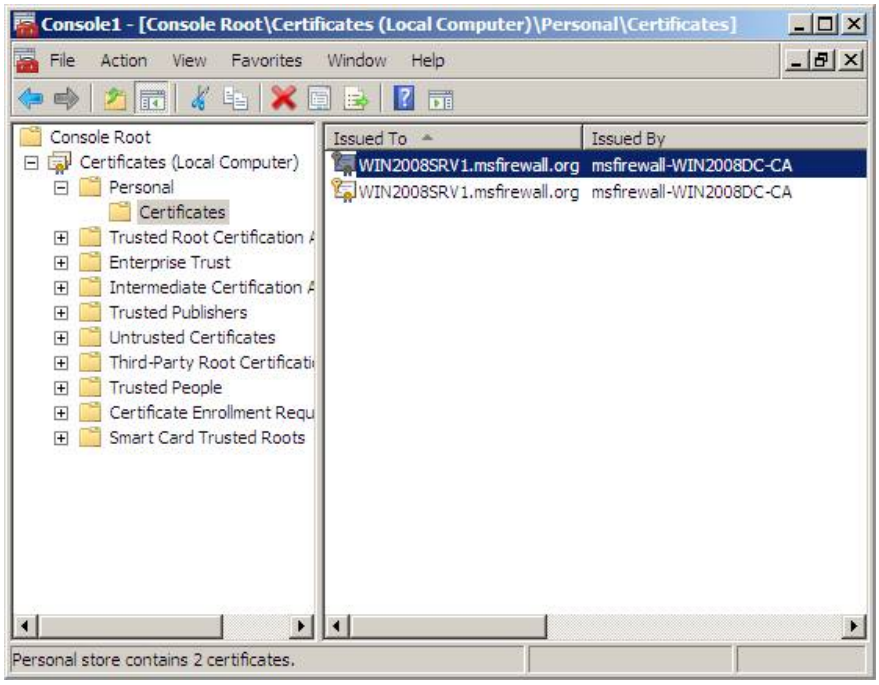

Figure 10

See the computer and health certificate installed on the Network Policy Server

Next, verify that **WIN2008SRV1** has an SSL certificate and an NAP exemption certificate.

1. In the left pane of Console **Certificates** , open **Certificates (Local Computer) PersonalCertificates.** In the right pane, verify that the certificate has been automatically enrolled by **WIN2008SRV1** with **Intended Purposes** of **System Health Authentication** and **Client Authentication** . This certificate will be used for NAP client IPsec exemption.

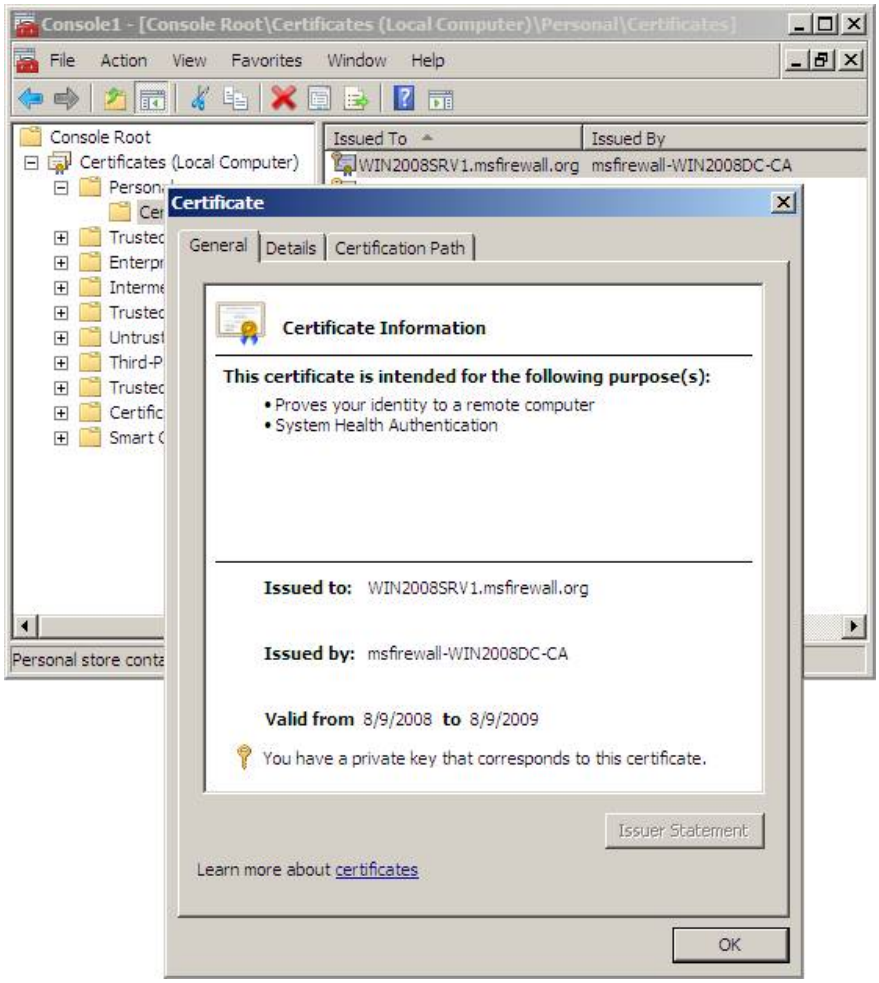

Figure 11

2. In the right pane, verify that the certificate has been enrolled with the **Intended Purposes** of **Client Authentication** and **Server Authentication** . This certificate will be used for SSL authentication on the server side.

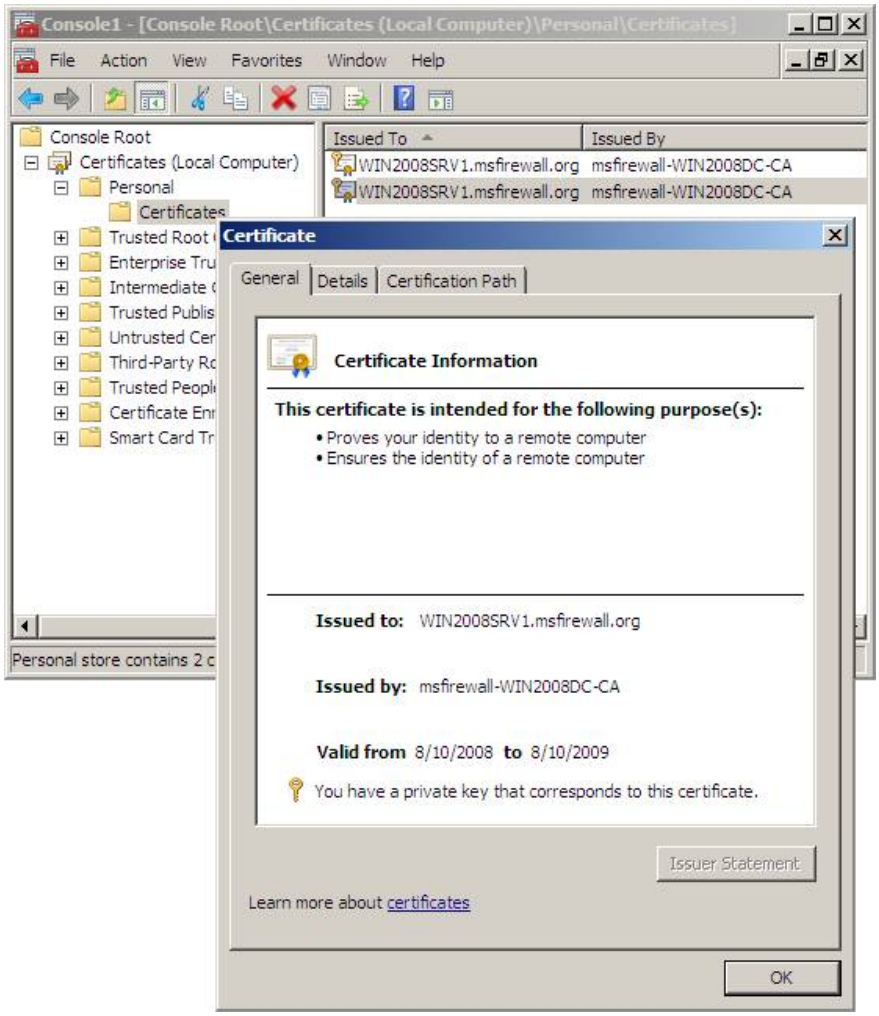

Figure 12

3. Close Console **Certificates** . If you are prompted to save the settings, click **No.**

Install the Network Policy Server roles, the Health Registration Authority, and the Subordinate Certificate Server.

Next, install role services to set **WIN2008SRV1** to a NAP health policy server, NAP server and NAP CA server.

Follow the steps below on **WIN2008SRV1** :

1. In **Server Manager** , in the **Roles Summary** section, click **Add Roles** , and then click **Next** .

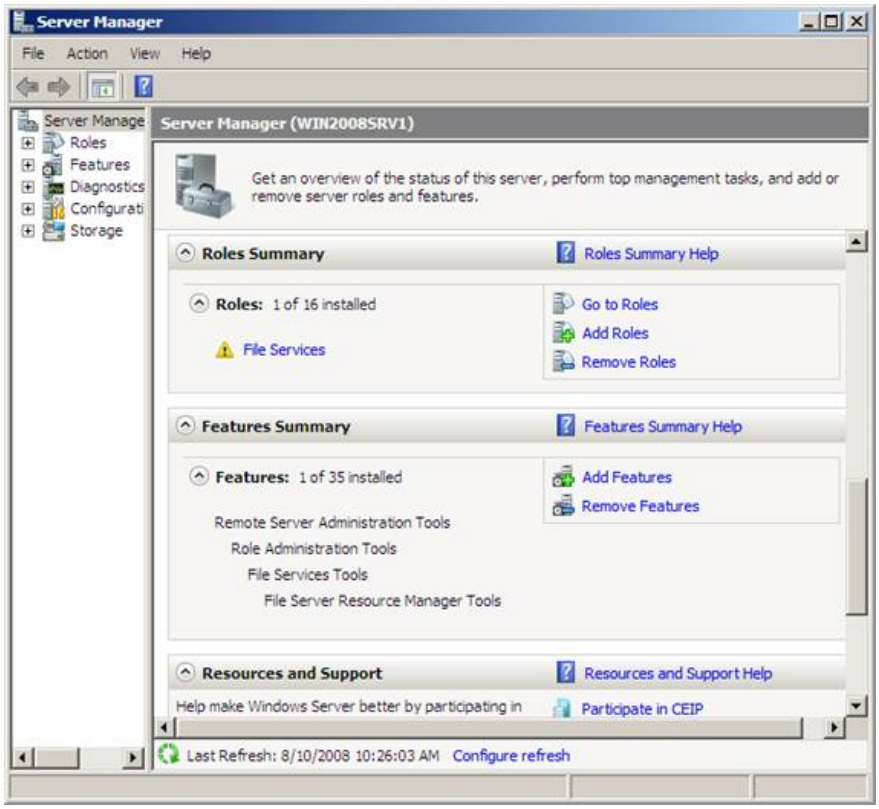

Figure 13

2. On the **Select Server Roles** page, select the **Active Directory Certificate Services** and **Network Policy and Access Services** check boxes, and then click **Next** twice.

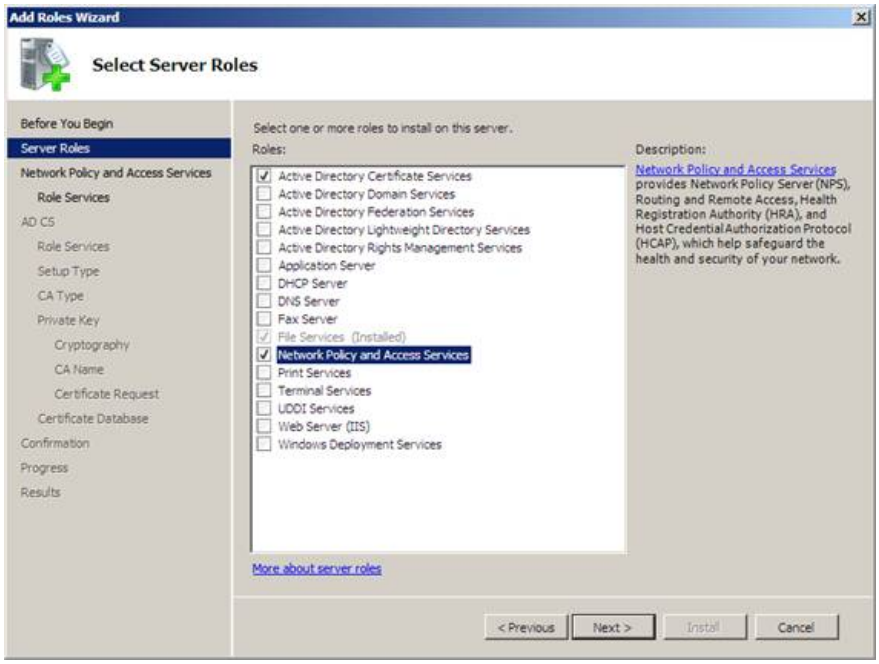

Figure 14

3. On the **Select Role Services** page, select the **Health Registration Authority** check box, click **Add Required Role Services** in the **Add Roles Wizard** window, and click **Next** .

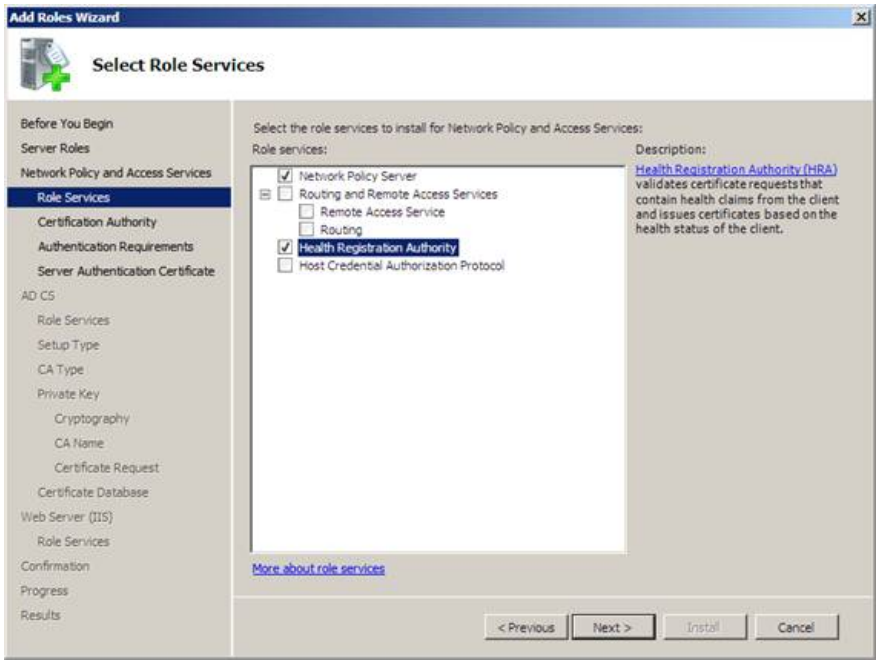

Figure 15

4. On the **Choose the Certification Authority page to use with the Health Registration Authority** , select **Install a local CA to issue health certificates for this HRA server** , then click **Next** .

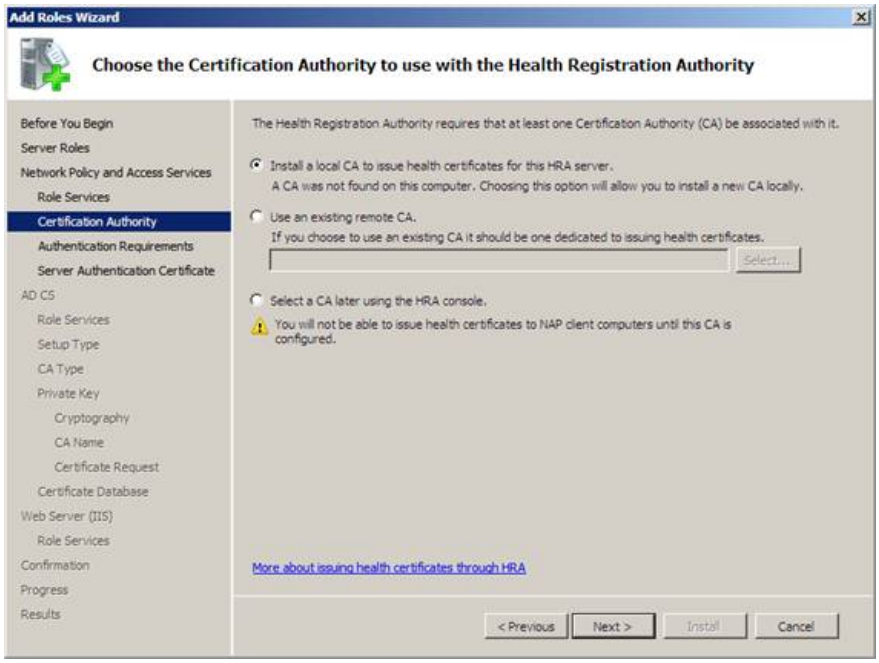

Figure 16

5. On the **Choose Authentication** page **for the Health Registration Authority** , select No, allow anonymous requests for health certificates, and then click **Next** . This option will allow computers to be enrolled in health policies in a workgroup environment. We will look at an example of a workgroup computer receiving the 'health' certificate later.

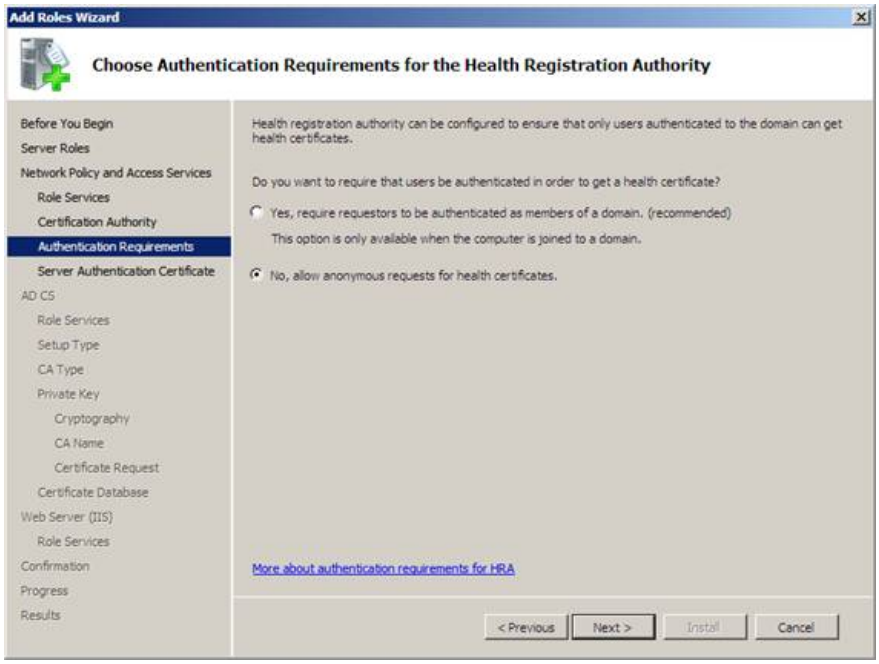

Figure 17

6. In the **Choose a Server Authentication Certificate page for SSL Encryption** , select **Choose an existing certificate for SSL encryption (recommended)** , click the certificate shown in this option, and then click **Next** .

Note:
You can view the properties of the certificates in the local computer's certificate store by clicking on a certificate, selecting **Properties** and then clicking the **Details** tab. A certificate used for SSL authentication must have a **Subject** field value that corresponds to the full domain name of the HRA server (for example, NPS1.Contoso.com) and the **Enhanced Key Usage** field value of **Server Authentication** . The certificate must also be issued from a root CA trusted by the client.

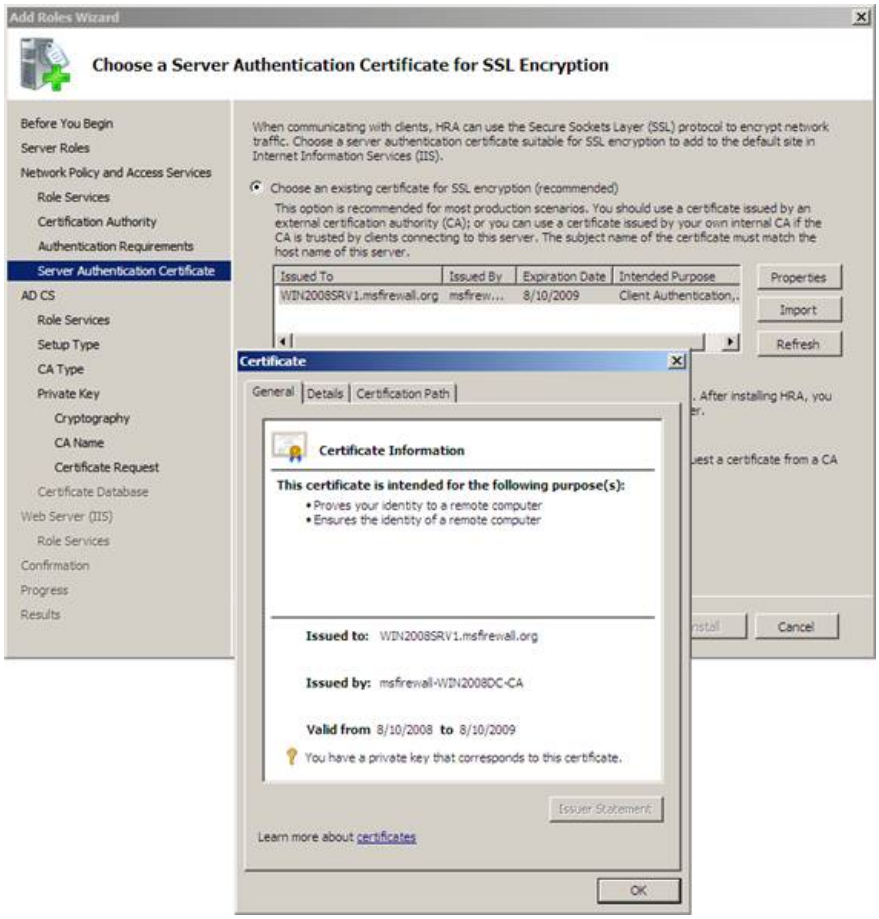

Figure 18

7. On the **Introduction to Active Directory Certificate Services page** , click **Next** .
8. On the **Select Role Services** page, verify that the **Certification Authority** check boxes are selected, and then click **Next** .

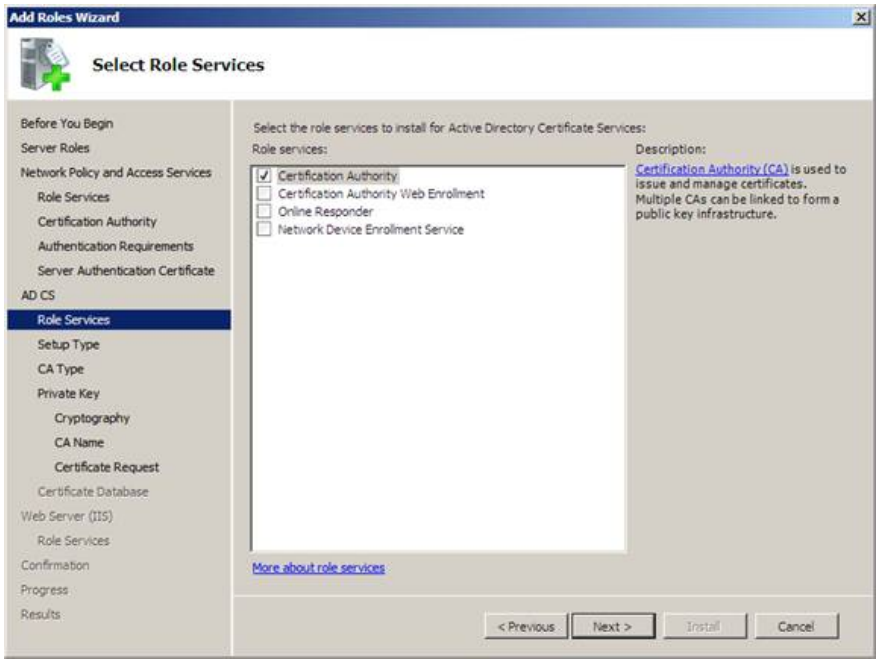

Figure 19

9. On the **Specify Setup Type page** , click **Standalone** and then click **Next** .

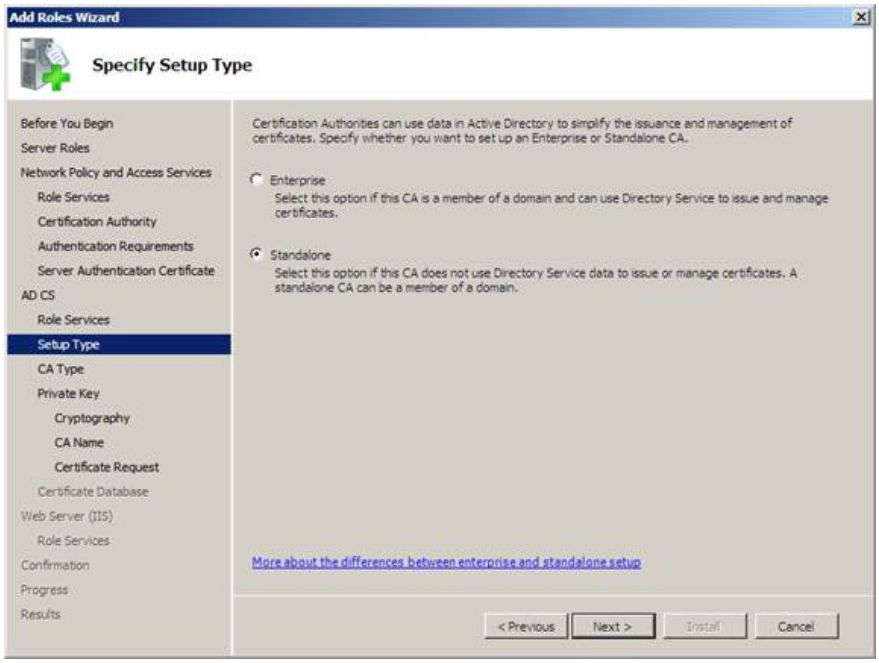

Figure 20

10. On the **Specify CA Type page** , click **Subordinate CA** , and then click **Next** . We choose to use lower level CA for safer purposes. The lower CA is responsible for issuing certificates, while the root CA's main job is to sign certificates of subordinate CAs being issued. This allows you to have multiple subordinate CAs and a root

CA. In a production environment, you can put the CA in the state ofline and only activate it online when signing certificates for subordinate CAs.

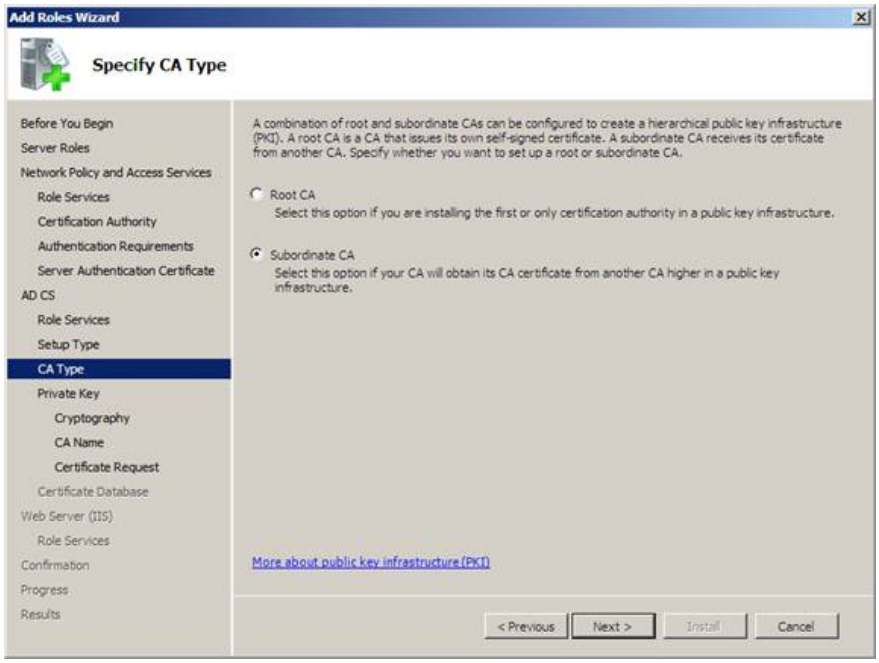

Figure 21

11. In the **Set Up Private Key page** , click **Create a new private key** , and then click **Next** .

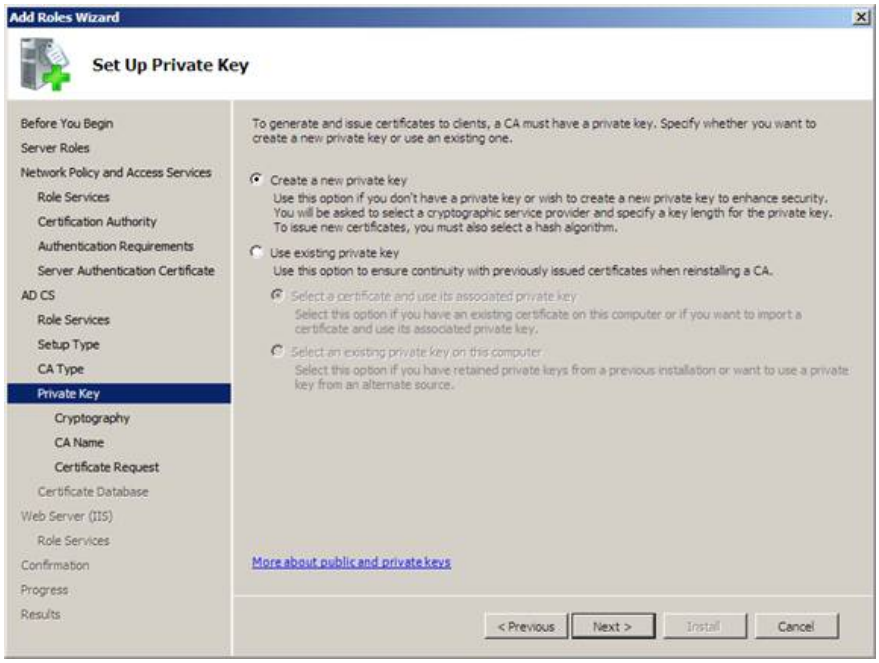

Figure 22

12. On the **Configure Cryptography for CA page** , click **Next** .
13. On the **Configure CA Name** page, the **Common name for this CA section** , type **msfirewall-WIN2008SRV1-CA** , and then click **Next** .

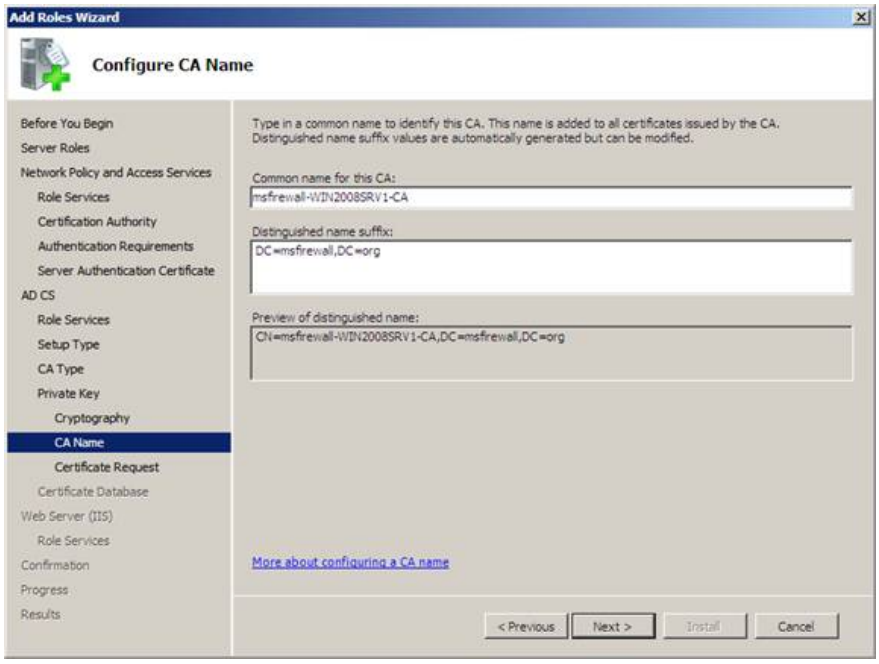

Figure 23

14. In the **Request Certificate from a Parent CA page** , select **Send a certificate request to a parent CA,** then click **Browse** . In the **Select Certification Authority** window, click **Root CA** , and then click **OK** .

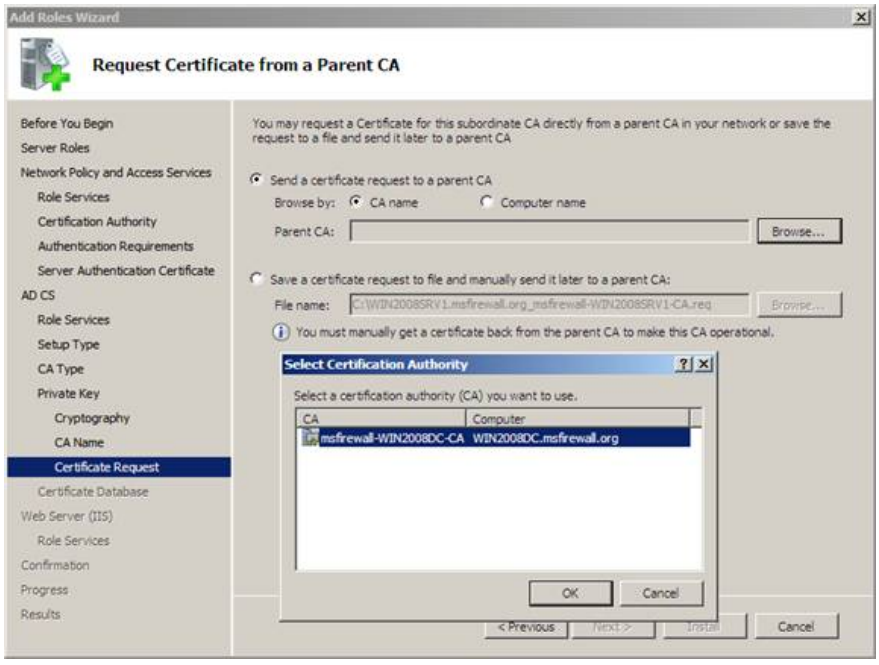

Figure 24

15. Verify that **WIN2008DC.msfirewall.orgRoot CA** is displayed next to **Parent CA** , and then click **Next** .

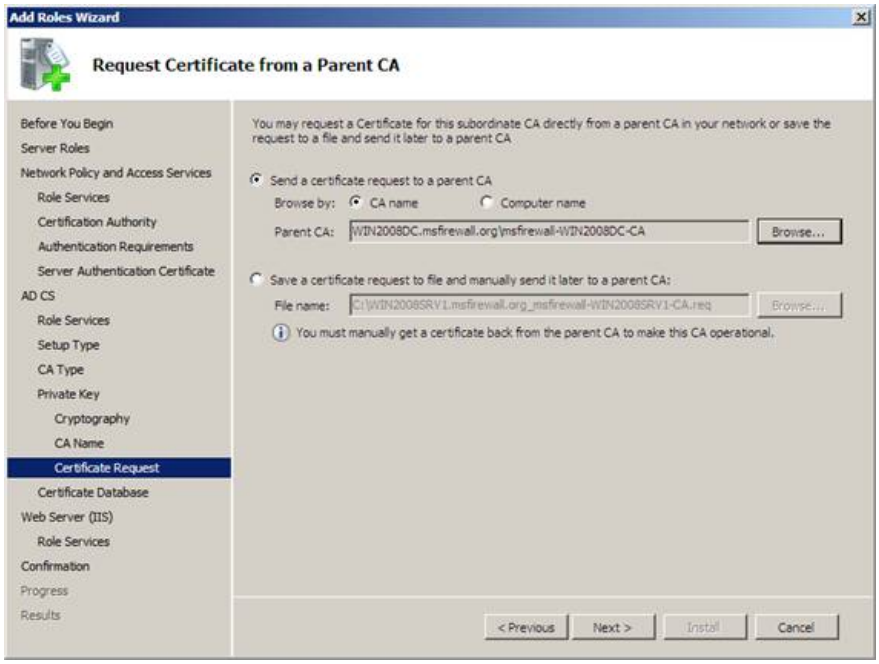

Figure 25

16. Click **Next** three times to accept the default database, Web server, and service settings for the role, and then click **Install** .

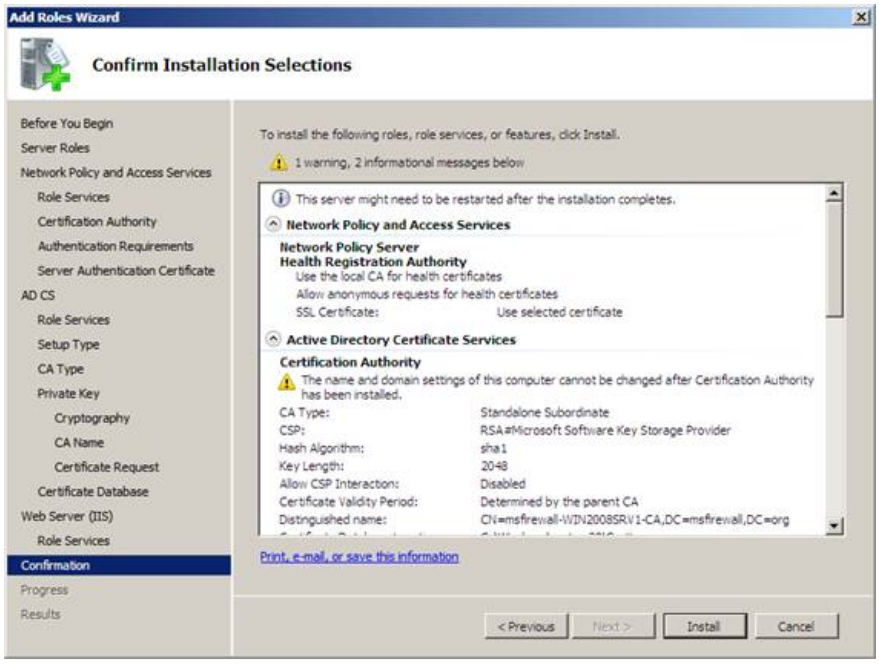

Figure 26

17. Verify that all installations are successful, then click **Close** . Note that the installation results say that **Attempt to configure Health Registration Authority failed** . **L?i l?y tên c?a c?c b? Authority** , don't worry too much about that failure. We will configure the **Health Registration Authority** in the next steps.

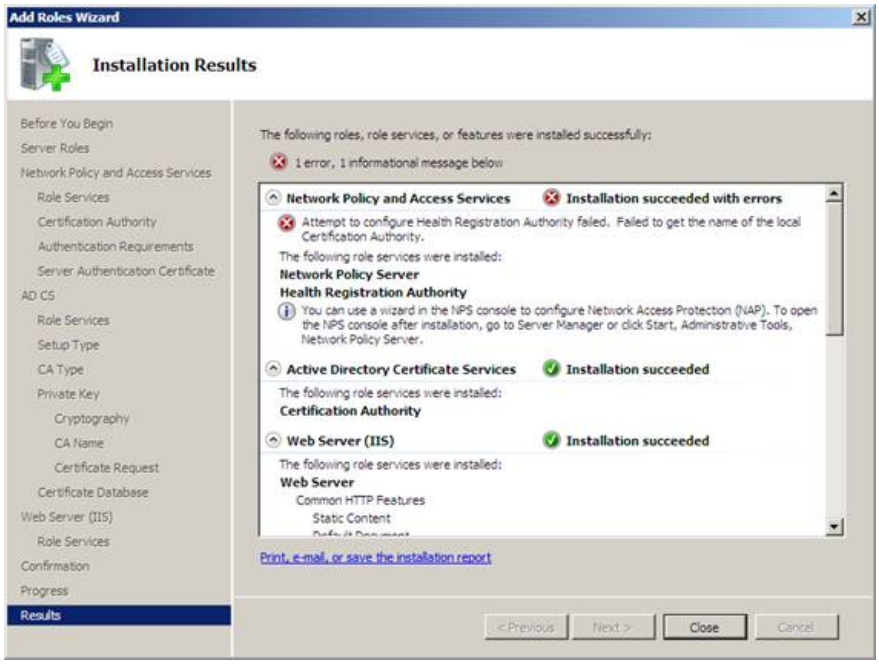

Figure 27

18. Leave the **Server Manager** window open to perform the procedure below.

Configure the lower CA on the Network Policy Server

The subordinate CA must be configured to automatically issue certificates when the NAP clients of the person who has the full NAP policy requirements request a certificate. By default, the private CA will wait until the administrator authorizes before the certificate is issued. We do not want to wait for the administrator's permission, so we will configure a private CA to automatically issue certificates when the request arrives.

Perform the following steps on **WIN2008SRV1** machine:

1. On **WIN2008SRV1** , click **Start** , click **Run** , type **certsrv.msc** , and then press ENTER.
2. In the Certification Authority interface, right-click **msfirewall-WIN2008SRV1-CA** , and then click **Properties** .

Figure 28

3. Click the **Policy Module** tab, and then click **Properties** .

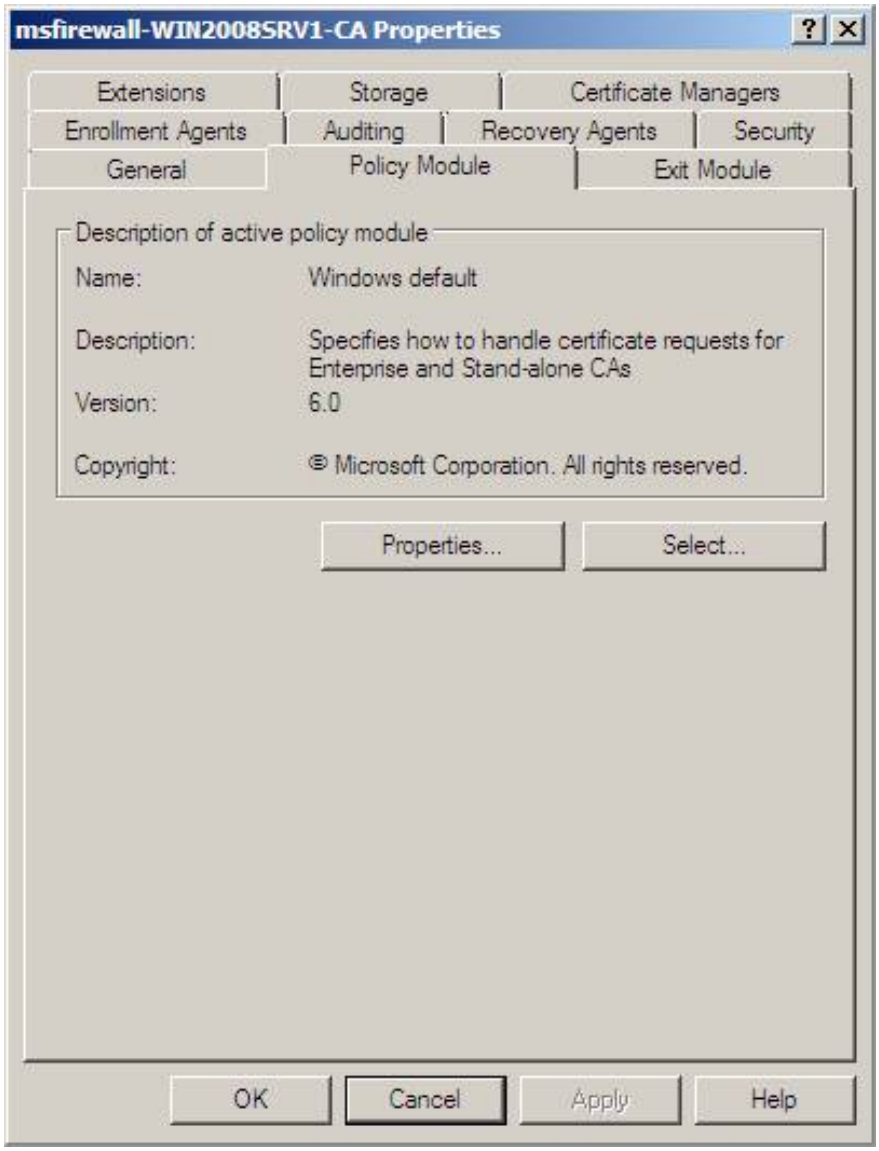

Figure 29

4. Select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate** , then click **OK** .

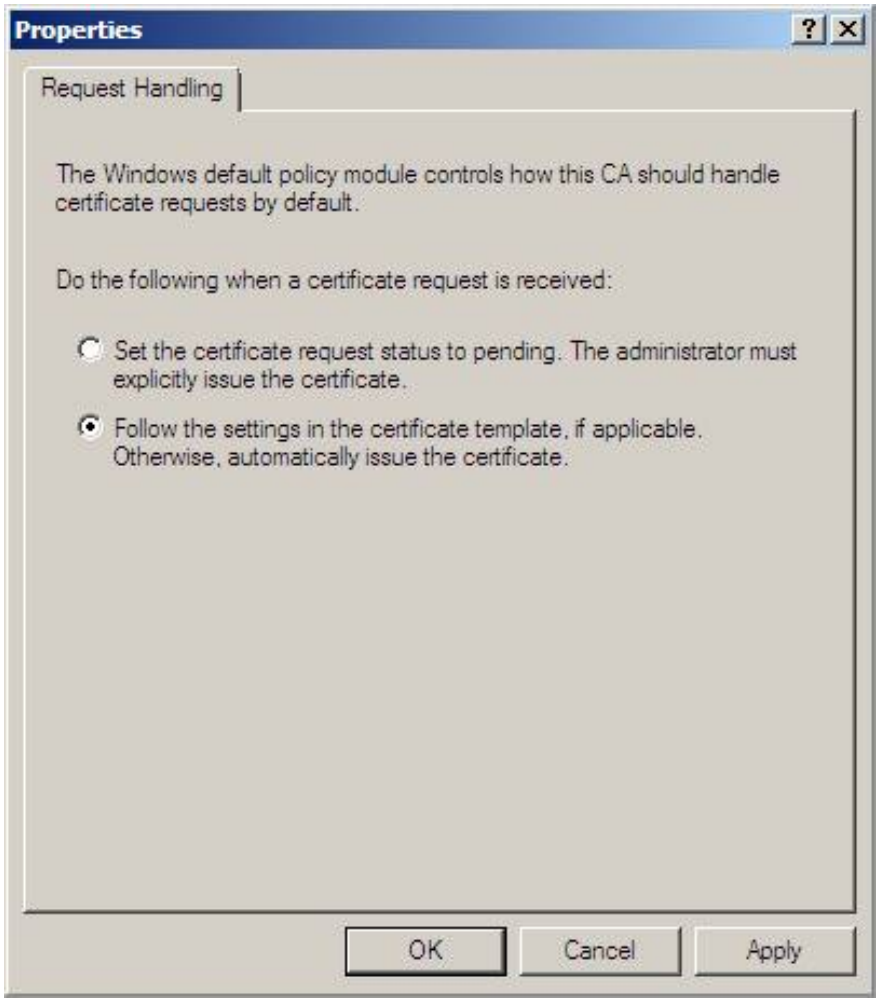

Figure 30

5. When prompted that AD CS must be restarted, click **OK** . Click **OK** , right-click **msfirewall-WIN2008SRV1-CA** , point to **All Tasks,** and then click **Stop Service** .

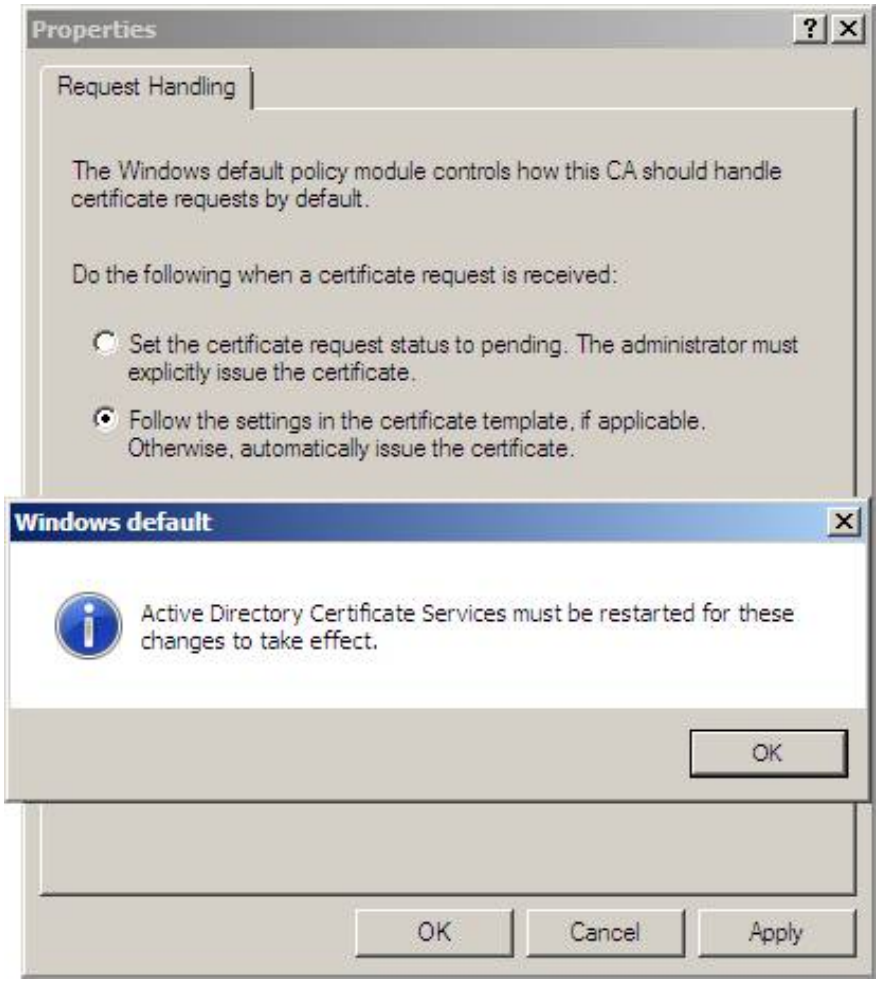

Figure 31

6. Right-click **msfirewall-WIN2008SRV1-CA** , point to **All Tasks** , and click **Start Service** .

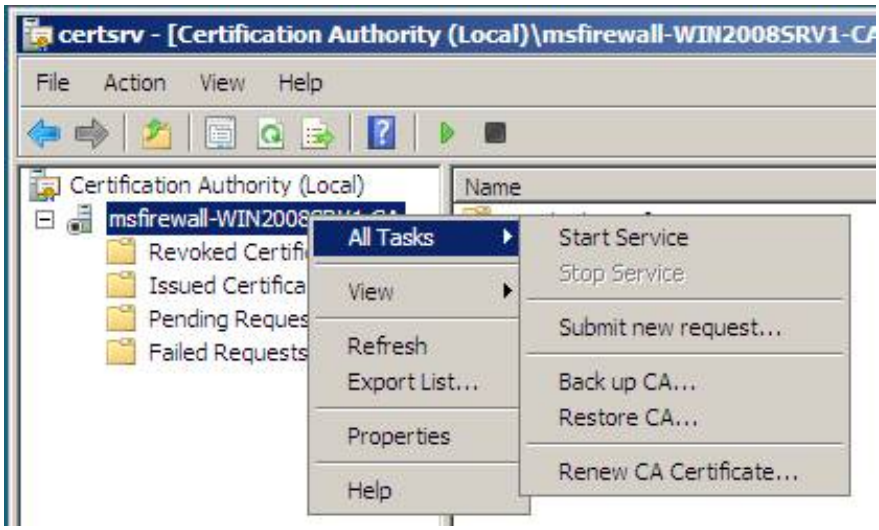

Figure 32

7. Go to the **Certification Authority** interface to perform the procedure below.

Activate the permissions for the Health Registration Authority to request, issue, and manage certificates.

The Health Registration Authority must have security permissions attached to request, issue, and manage certificates. It must also be allowed to manage subordinate CAs to disable expired certificates from the certificate store.

When the Health Registration Authority is activated on a different computer than the CA issuing computer, the permissions must be assigned to the HRA machine. In this configuration, HRA and CA are located on the same computer. In this scenario, the permissions must be assigned to **Network Service** .

Follow the steps below on **WIN2008SRV1** :

1. In the left pane of the console, click **msfirewall-WIN2008SRV1-CA** , and then click **Properties** .
2. Click the **Security** tab, and then click **Add** .

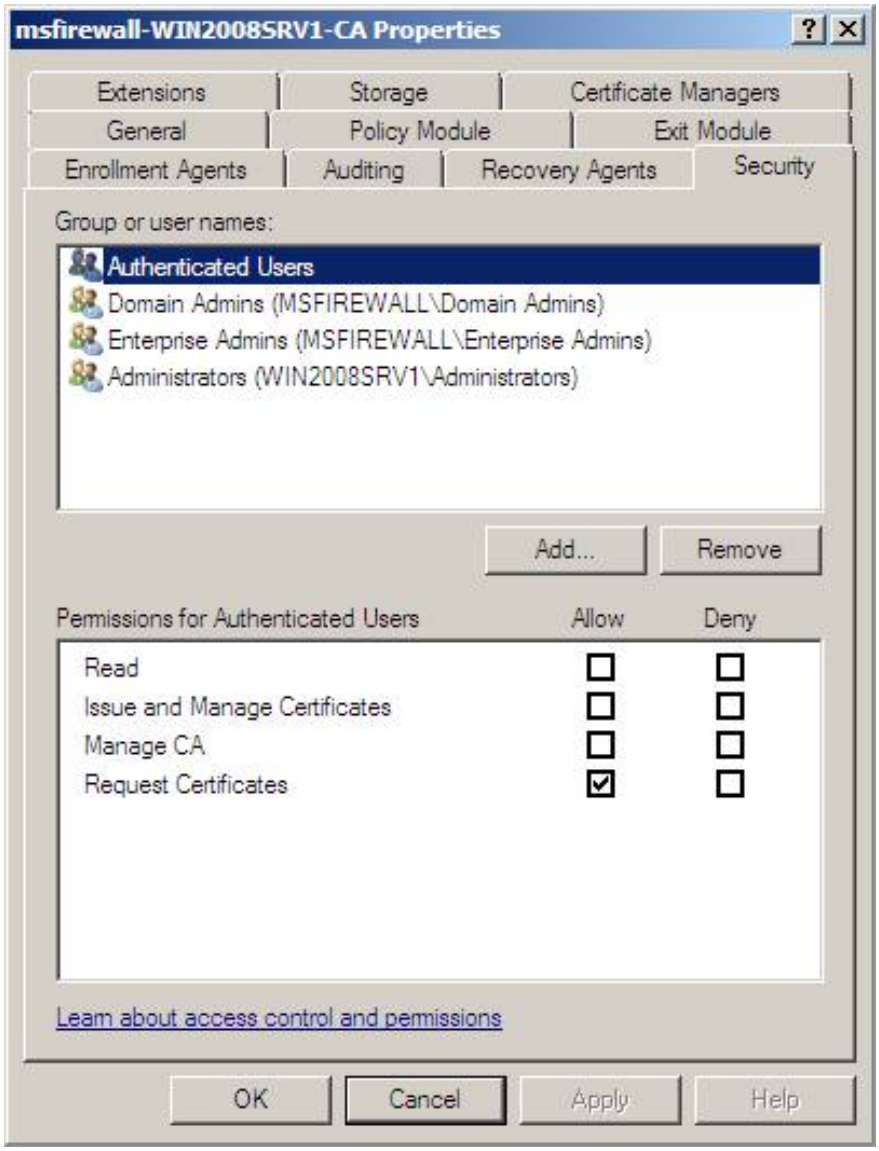

Figure 33

3. In **Enter the object names to select (examples)** , type **Network Service** and then click **OK** .

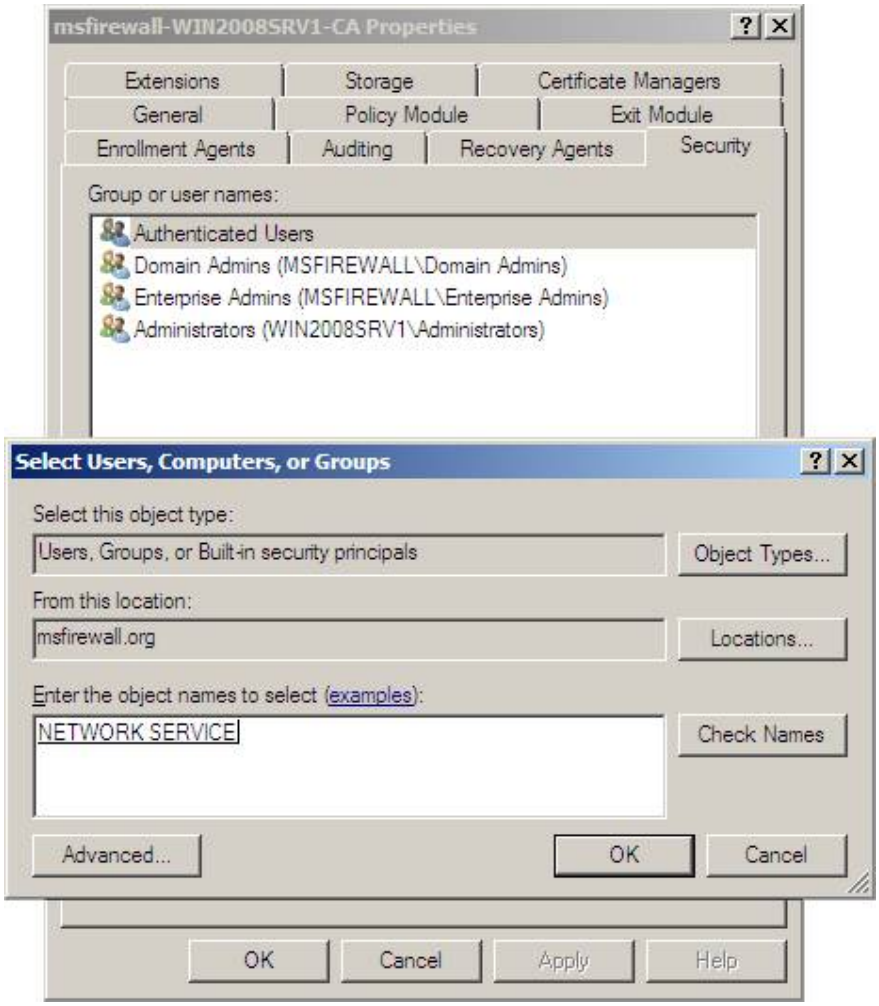

Figure 3 * 4

4. Click **Network Service** , under **Allow** , select the **Issue and Manage Certificates** , **Manage CA** , and **Request Certificates** check boxes, and then click **OK** .

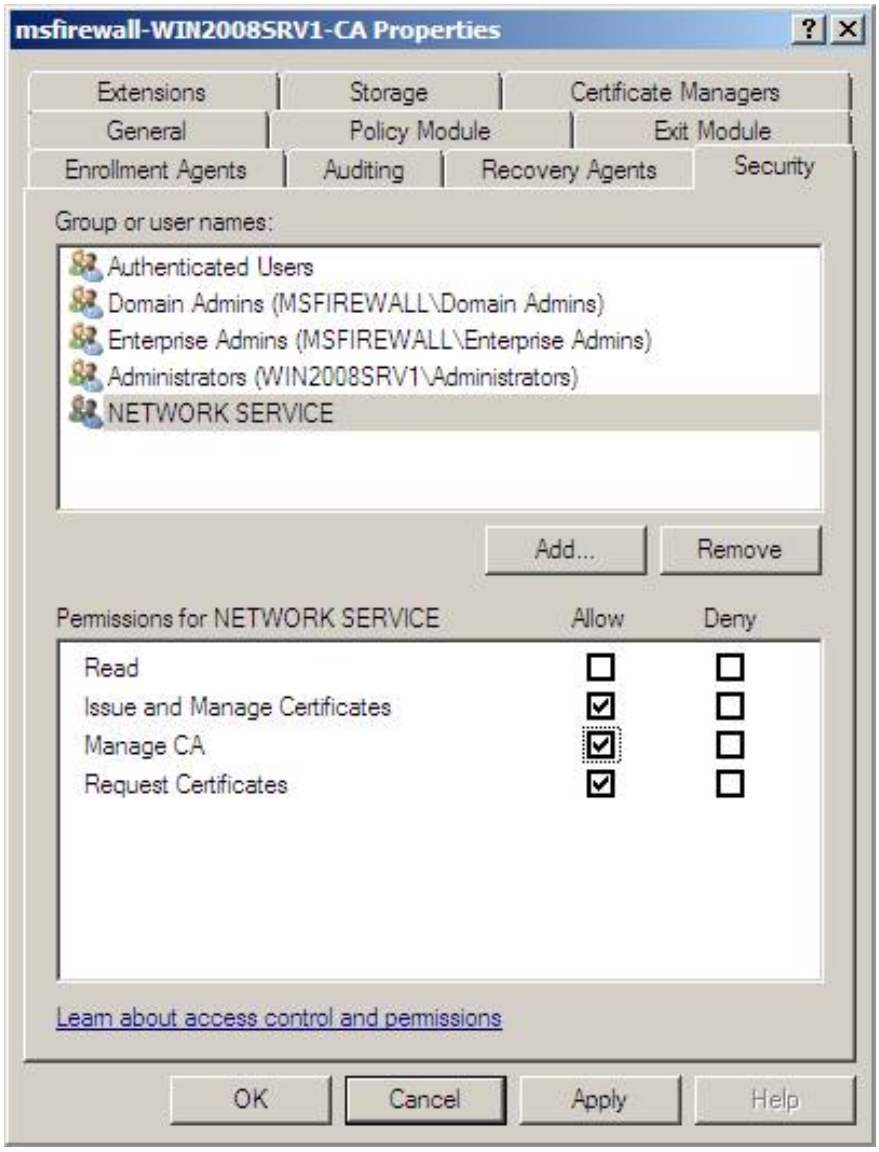

Figure 35

5. Close the **Certification Authority** console.

Configure the Health Registration Authority to use a subordinate CA to issue 'health' certificates

You must inform the Health Registration Authority about which CA can use to issue 'health' certificates. You can use either a private CA or a business CA. In this example network, we are using the private CA installed on **WIN2008SRV1** .

Follow the steps below on **WIN2008SRV1** :

1. On **WIN2008SRV1** , click **Server Manager** .
2. In **Server Manager** , open **RolesNetwork Policy** and A **ServicesHealth Registration Authority (WIN2008SRV1) Certification Authority** .

Note:
If Server Manager is open when you install the HRA server role, then you need to close it and then reopen to access the HRA interface.

3. In the left pane of the HRA console, right-click the **Certification Authority** and click **Add certification authority** .

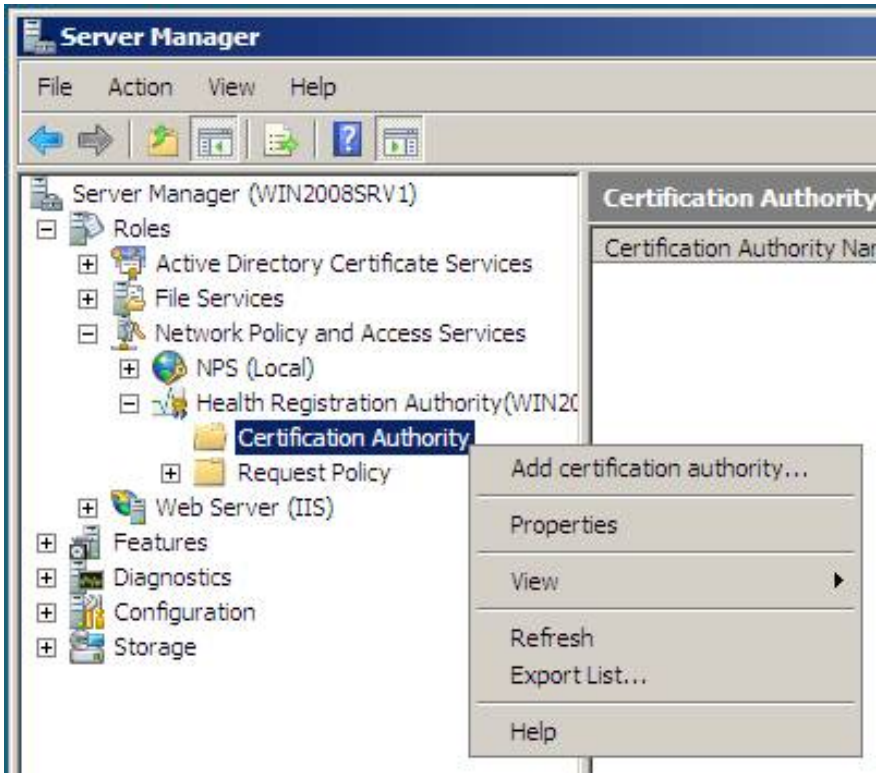

Figure 36

4. Click **Browse** , click **msfirewall-WIN2008SRV1-SubCA** , and then click **OK** . See example below.

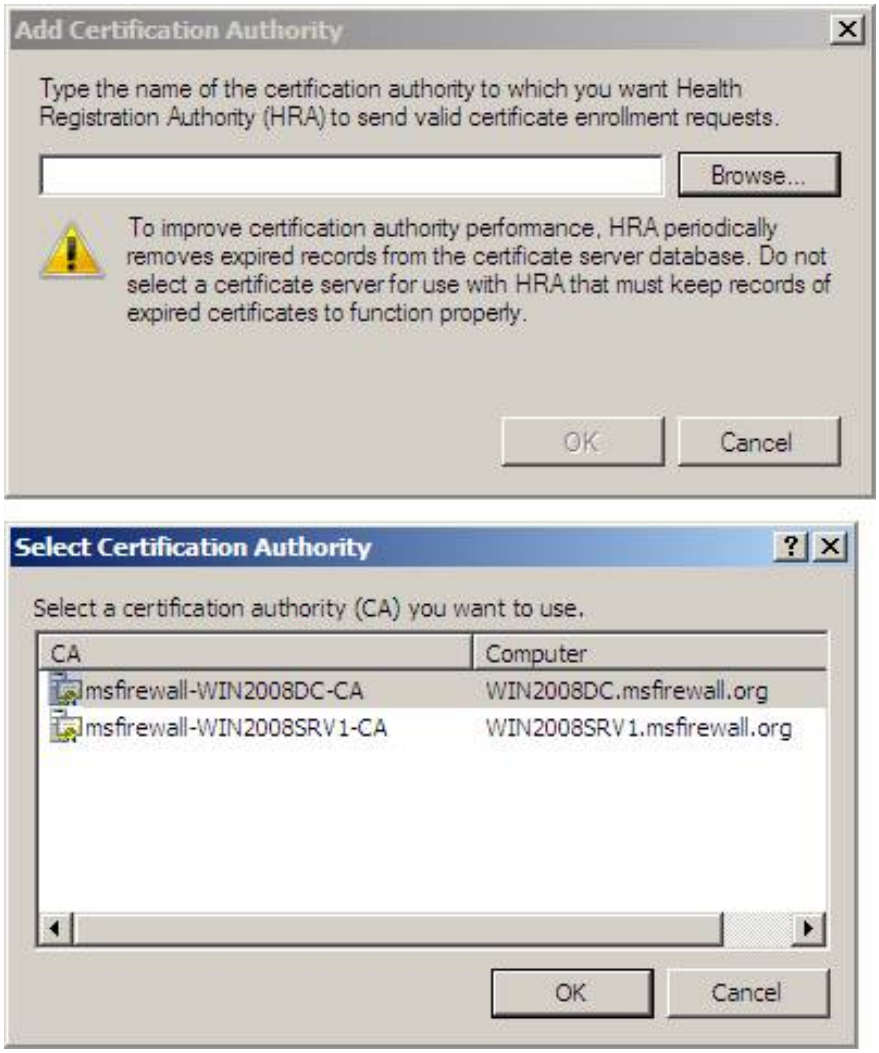

Figure 37

5. Click **OK** , then click **Certification Authority** and verify that **WIN2008SRV1.msfirewall.orgmsfirewall-WIN2008SRV1-CA** is displayed in the details pane. Next we will configure the properties of this private CA.

The Health Registration Authority can be configured to use a private CA or enterprise CA. The CA properties (which we will configure next) configured on the Health Registration Authority must match the type of CA selected.

Figure 38

6. Right-click **Certification Authority** , and then click **Properties** .

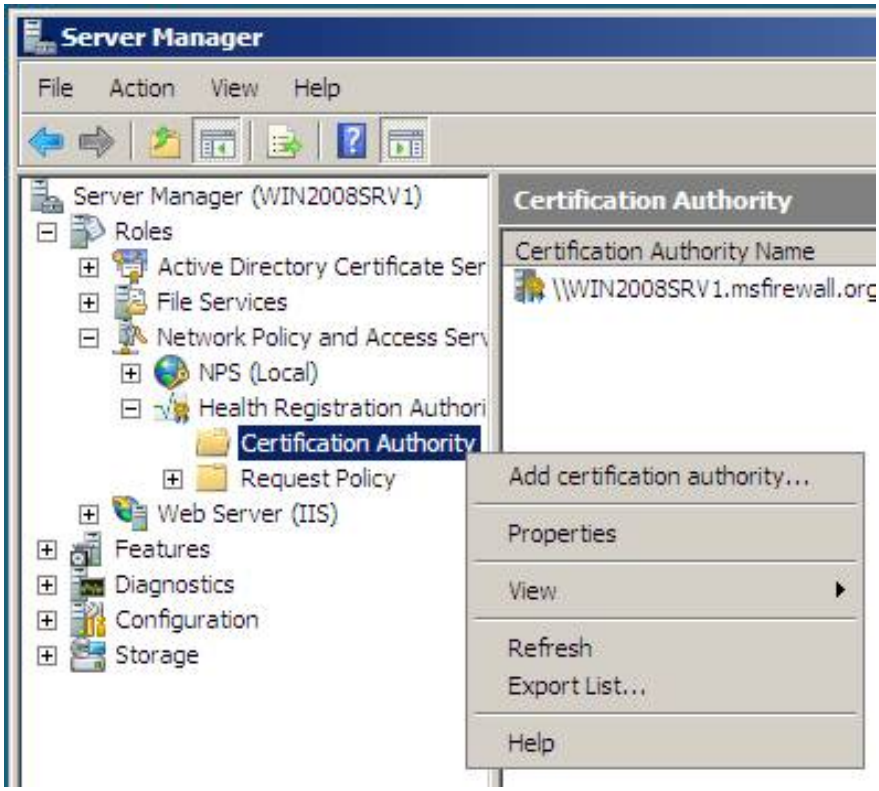

Figure 39

7. Verify that the **Use standalone certification authority option** has been **ticked** and the value is in **Use standalone certification authority is selected and that the value under Certificates approved by Health Registration Authority will be valid for** 4 hours, then you should Click **OK** . See the example below.

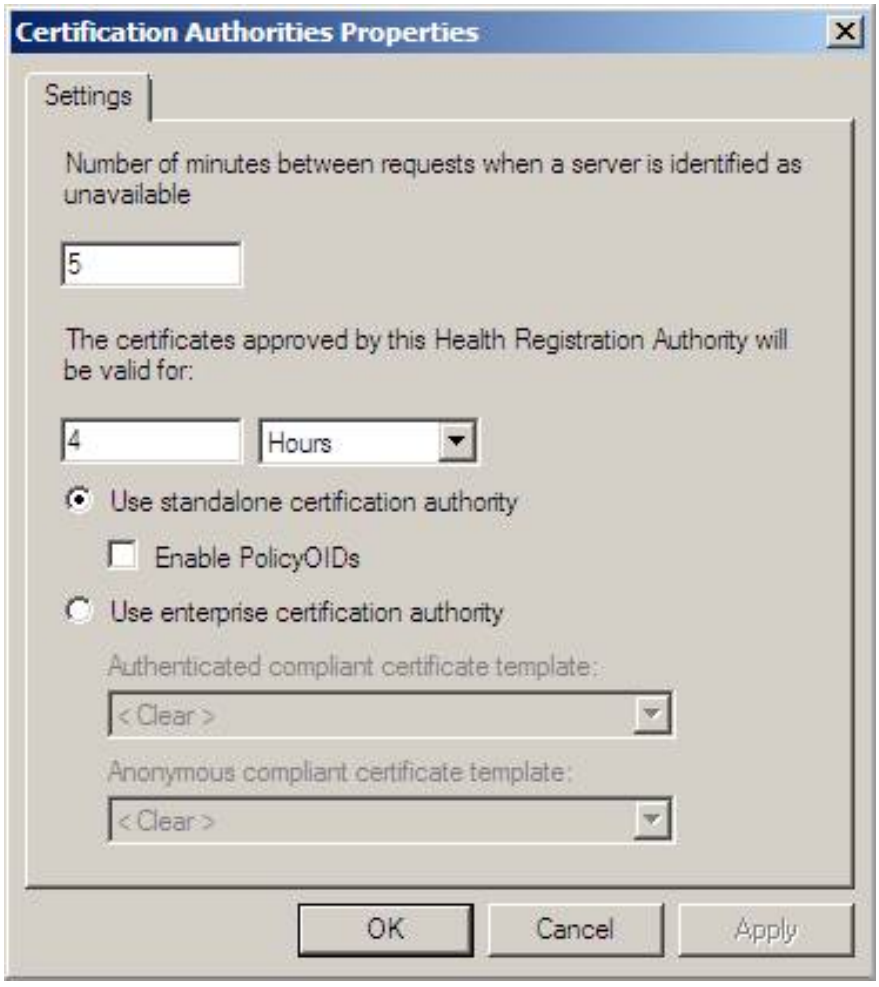

Figure 40

8. Close **Server Manager** .

Conclude

In the second part of this article series, I showed you how to use IPsec enforcement with NAP, introducing you to the procedures needed to create an NPS server. On this server we have installed and configured the Windows Server 2008 Network Policy Server, the Health Registration Authority and the subordinate CA. With these components, we can already be ready for the next step, the IPsec enforcement policy step.

You finished reading the article "**Deploying IPsec Server and Domain Isolation with Windows Server 2008 Group Policy - Part 2**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.