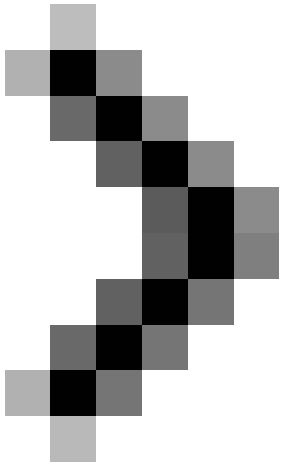
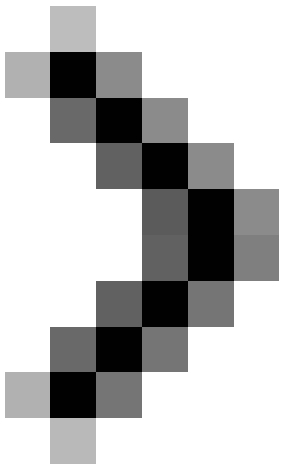
Introduction to Network Access Protection (Part 4)

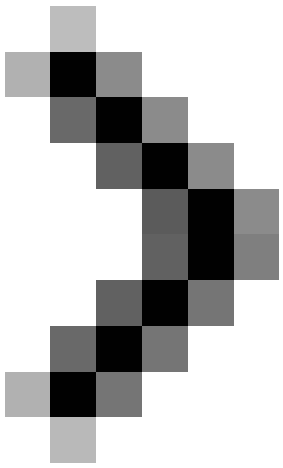
In the previous part of this series, we showed you how to configure the VPN component used to allow external users to access our network. In this part 4, we will go



Introduction to Network Access Protection (Part 1)



Introduction to Network Access Protection (Part 2)



Introduction to Network Access Protection (Part 3)

In the previous part of this series, we showed you how to configure the VPN component used to allow external users to access our network. In this article, I will continue the discussion by showing you how to configure the Network Policy Server component.

As I explained in this series, the Network Policy Server's job is to compare the security status of computers that need to access the network with the network's predefined policy. This policy sets out the requirements of access machines to ensure network security.

In other words, a system's protection policy requires workstations that are using the current Windows operating system and have all the latest patches. Regardless of what standard you use to decide whether this workstation is safe, you'll have to do some work. Safety standards vary widely from one company to another, so Microsoft has left this policy blank (at least until this beta version). As such, it will be mandatory to configure your own security policies.

To demonstrate, we will create a simple example to see if Windows firewall is enabled. If the firewall is enabled, we will consider the safety of the workstation.

As I mentioned in the previous sections, in the real world, you should not configure the Network Policy Server on the same VPN server. The VPN server is exposed to the outside world and configuring NPS on the same machine is to process complex issues about itself. Nothing in Windows can prevent you from using the same server for both the VPN and Network Policy Server components, since it is just to demonstrate that we will use the same server to configure both components. this.

Start the configuration process by entering the **MMC** command at the **RUN** command window to open an empty MMC. When this interface is open, select **Add / Remove Snap-in** from the File menu of the interface. In the Add / Remove Snap-in window, select the **Network Policy Server option** from the available list and click the **Add** button. You should look at the window asking if you want to manage your local computer or another computer. Make sure that the **Local Computer** option is selected and then click **OK** . Click **OK** again and the Network Policy Server component will open.

Here, you must navigate through the console tree to **NPS (Local)** | **Network Access Protection** | **System Health Validators** , as shown in Figure A. Now right-click on the **Windows System Health Validators** object found in the middle of the console, select **Properties** from the results menu. Windows will display the **Windows Security Health Validator Properties** dialog box as shown in Figure B.

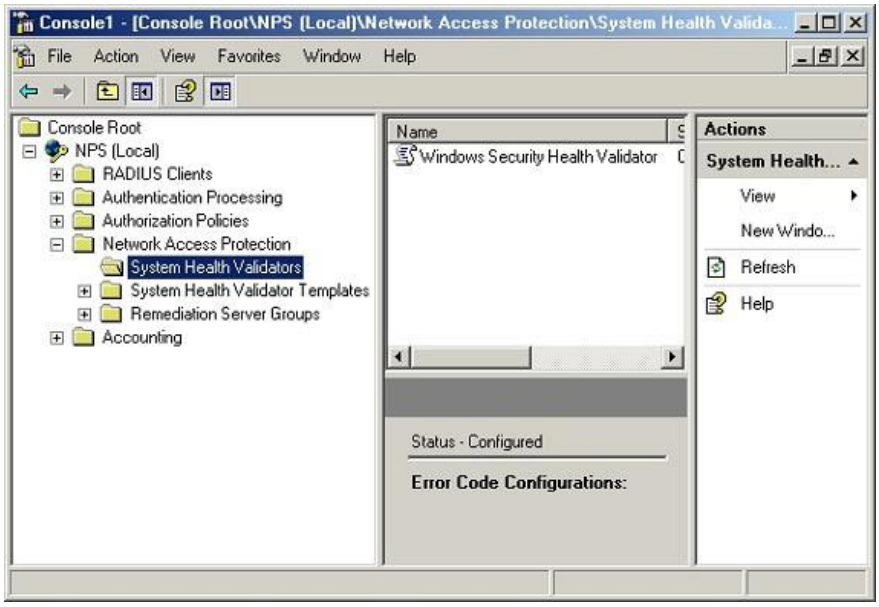


Figure A : Navigate through the incoming tree interface
NPS (Local) |Network Access Protection |System Health Validators

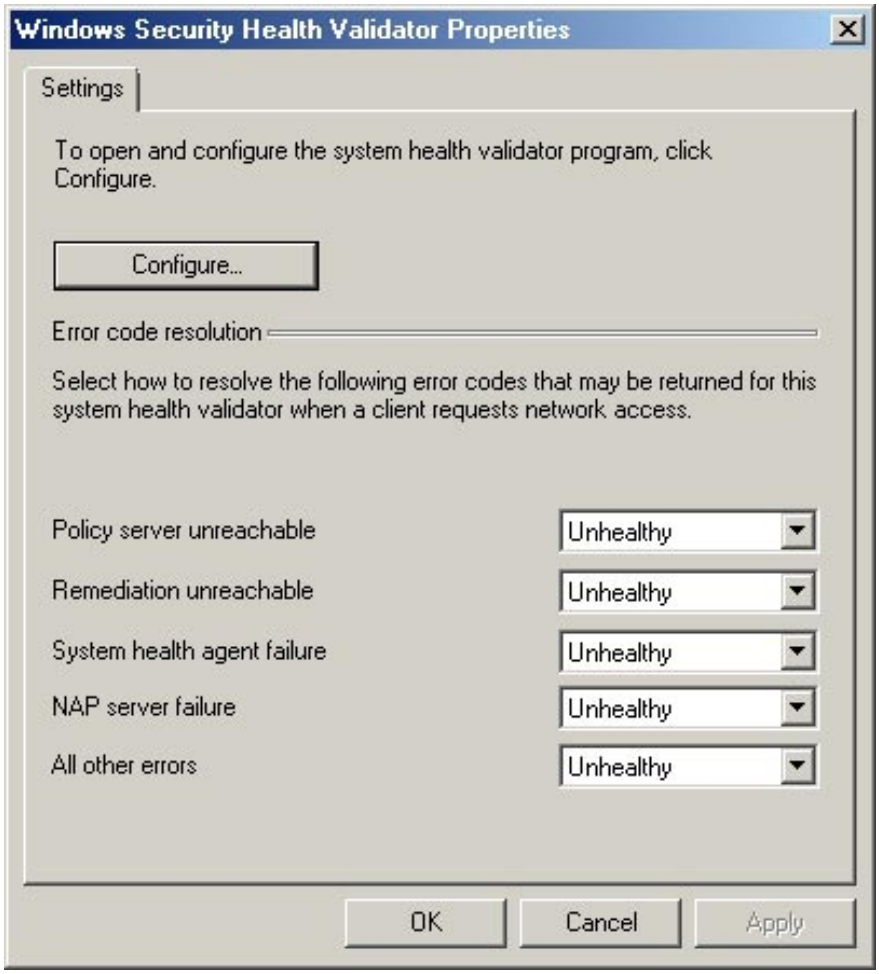


Figure B : Windows Security Health Validator Properties dialog box
Used to configure valid safety standards.

Click the dialog box's **Configure** button, Windows will show you the **Windows Security Health Validator** dialog box as shown in Figure C. As you can see in the figure, this dialog box allows you to define a valid system health policy. . By default, this dialog box is configured with the Windows firewall, Windows can be upgraded and the Virus-Spyware removal program is installed and upgraded. If you're only interested in making sure the Windows firewall is enabled, select the **A Firewall is Enabled for all Network Connections** checkbox and uncheck all other checkboxes. Click **OK** or once to continue.

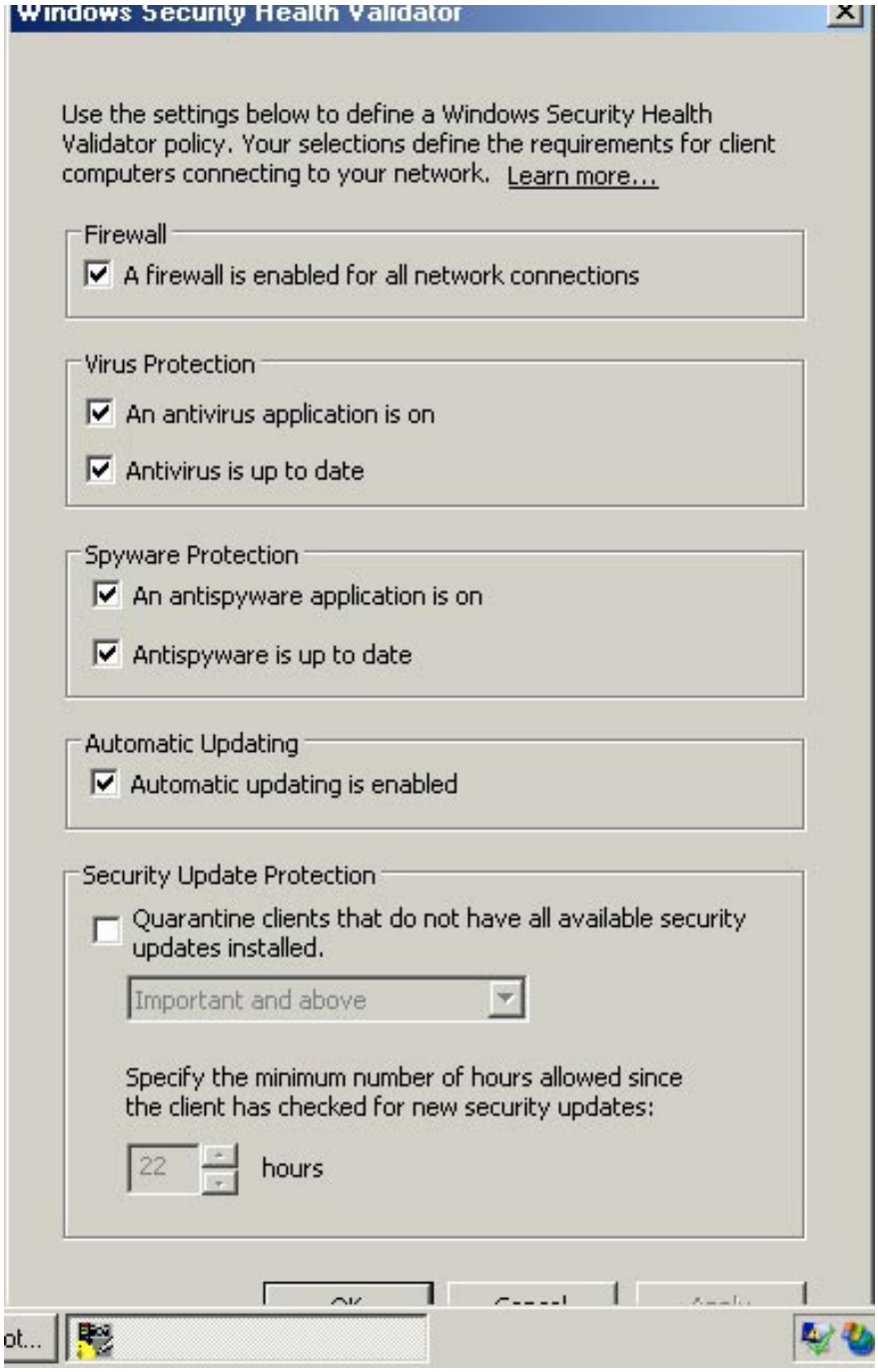


Figure C : Select the section **A Firewall is Enabled for all Network Connections** and cancel the selection of other components.

Now that you have configured the System Health Validators, you must then configure the System Health Validator template. System Health Validator templates define valid client results of the system. In essence, this means defining what constitutes a removal or passing when done on a client.

To configure the NPS protection form, right-click the **System Health Validator Template template** and select the **New** command from the menu. Windows will then display a new **Create New SHV Template** dialog box displayed as shown in Figure D.

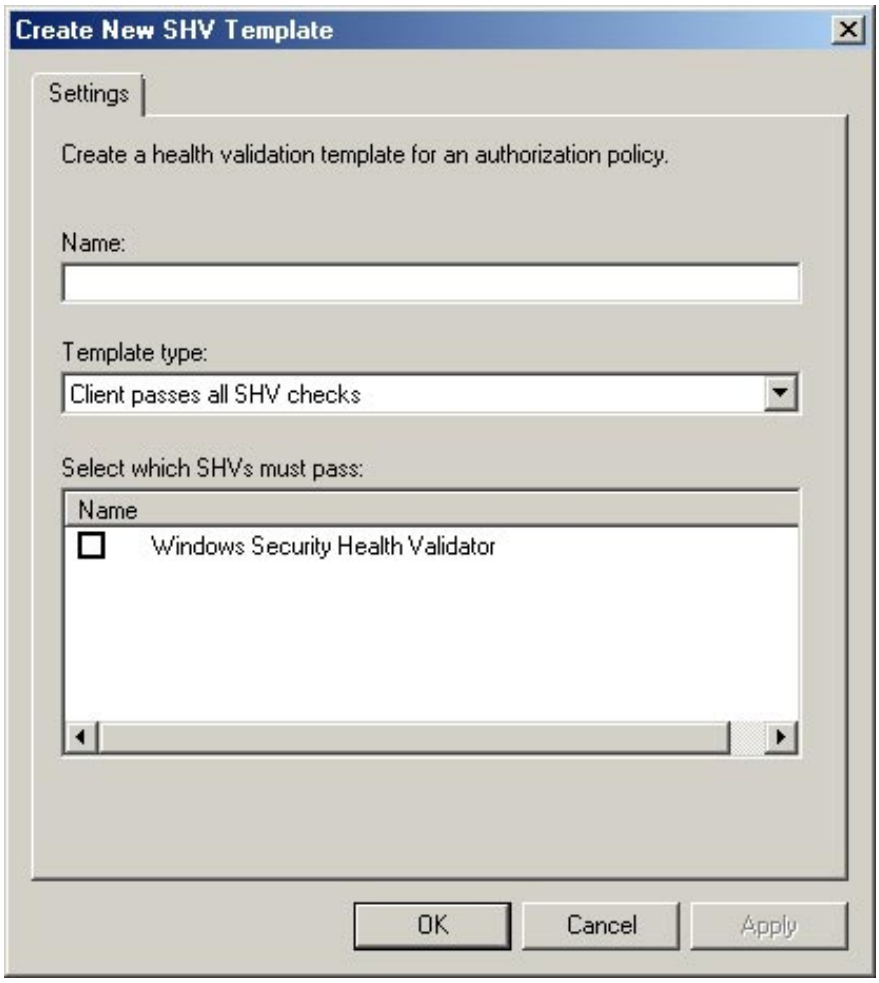


Figure D : You must create a new template

As you can see in the figure, the dialog box prompts you to enter the name of a new template. Enter ***Compliant*** into the **Name** field. Make sure that the **Template Type** drop-down list is set to **Client Passes all SHV Checks** . Select the **Windows System Health Validator** checkbox and click **OK** .

We have now created a template that defines what to follow. We have to create a second template to define their meaning for a system with that compliance. To do this, right-click **System Health Validator Templates** and select **New** . You should watch the screen that has worked recently.

Now, name the ***NonCompliant*** template. Set the **Template Type** for **Client Fails** or **More SHV Checks** . Select **Windows Security Health Validator** and click **OK** . If you return to the main window of the Network Policy Server interface and select **System health Validator Templates** , you will see both the ***Compliant*** and ***NonCompliant*** templates displayed in the central window of the interface as shown in Figure E.

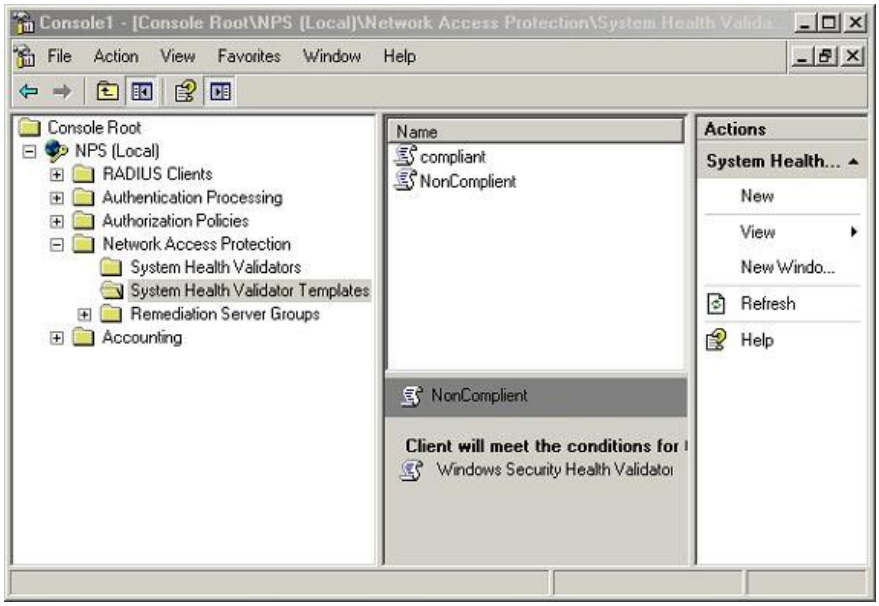
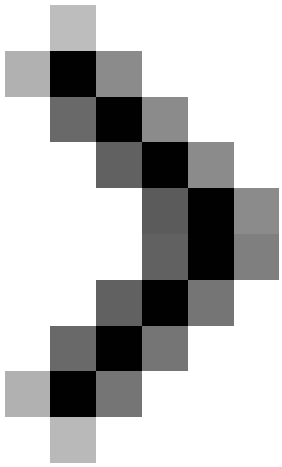


Figure E

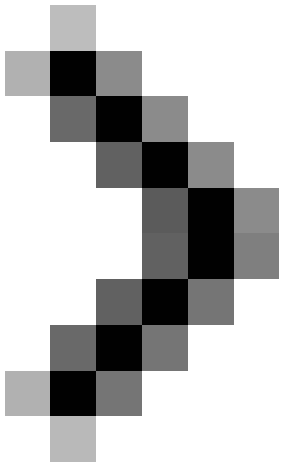
If you return to the main window of the Network Policy Server interface and select **System health Validator Templates** , you will see both ***Compliant*** and ***NonCompliant*** templates displayed in the center window of the interface.

Conclude

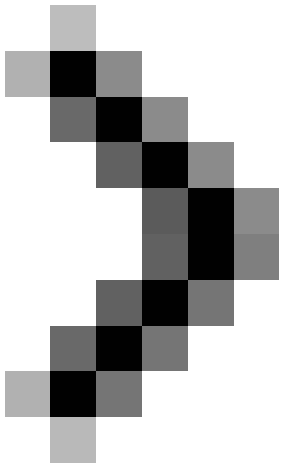
In this article, we have shown you how to configure Windows to check to determine if clients are requesting access to a network with a firewall enabled. Please continue to see the following.



Introduction to Network Access Protection (Part 5)



Introduction to Network Access Protection (Part 6)



Introduction to Network Access Protection (Part 7)

You finished reading the article "**Introduction to Network Access Protection (Part 4)**" 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.