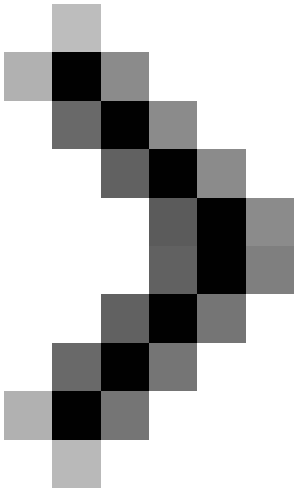
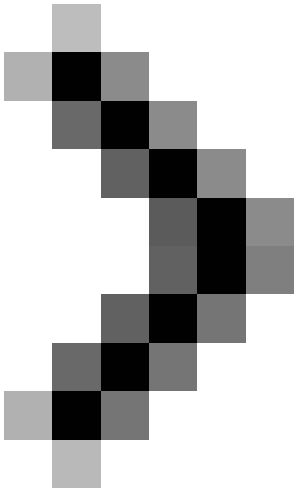
Overview of Windows Server 2008 Firewall with advanced security features - Part 3

In this article, I will continue the discussion by showing you how to use Group Policy to enforce domain isolation using IPsec.



Overview of Windows Server 2008 Firewall with advanced security features



Overview of Windows Server 2008 Firewall with advanced security features (Part 2)

Thomas Shinder

Part 3: Introducing domain isolation

In the first two articles of this series, I talked about the general configuration options of Windows Firewall and then discussed some details about the incoming and outgoing rules of the new firewall. this.

In this article, I will continue the discussion by showing you how to use Group Policy to enforce domain isolation using IPsec. The interface of Windows Firewall with advanced security features integrates Windows Server 2008 Group Policy, so it will allow you to use the console of Group Policy and Group Policy Editor to create firewall policies for computers in the entire domain, in an OU or in a site.

Domain Isolation (through the Windows Firewall with Advanced Security interface) allows you to protect all domain member computers from intruders from bad computers other than domain members. . Domain members are configured so that they must authenticate with other members before the connection is allowed between the two machines. Machines that are not domain members will not be able to authenticate, and thus the connection they want to make with the machines in the domain will fail.

It's possible in previous versions of Windows, but the interface for configuring IPsec policies is so complicated and so confusing that some Windows administrators or security administrators are concerned. about domain isolation issues. However, with the appearance of Windows Firewall with Advanced Security in Windows Server 2008 and Vista, these administrators are quite easy to configure domain isolation. It integrates with

Windows Server 2008 Group Policy to allow you to easily focus on configuration in a 'one station' solution.

In these two series (the third part is divided into two separate parts), we will demonstrate to you how to create a domain isolation solution for a simple network with three computers. These computers are:

• Domain controller to request security. You cannot enforce security because computers cannot seem to receive group policy when enforcing security. However, if you require security when connecting to a domain controller, domain members will be able to connect to the domain controller to get Group Policy policy, then they can protect the rest of the transmission. inform them with the domain controller. The IP address in this example will be **10.0.0.2** .

• A server requires security. Can be the file server type, database server, or Web server. When we demonstrate the connections at the end of the article, we will ping the server to see if the connection security rules work. The IP address in this example is **10.0.0.3**

• Windows Vista client. This computer will connect to the server and domain controller. The IP address in this example is **10.0.0.100**

Servers are Windows Server 2008 machines and all three servers are in the same domain.

You do not need to install any special roles or role services and features to isolate the domain.

Note that this is a very simple script and there are no exceptions that you need to create for infrastructure servers in your network, such as DNS, DHCP or WINS servers as well as for gateways. default.

In production networks, you need to create exceptions for IPsec policy enforcement so that non-domain members can still communicate with infrastructure servers, which is a very important issue.

Configure the default IPsec policy to require encryption

In the example that will be used in this article, we want to ensure that IPsec is used not only to control what computers can connect to another computer, but also to ensure that no one can steal it. Private information is shared between domain member computers. To do that, we can use ESP encryption.

To make ESP encryption part of the default IPsec settings, we need to enter the properties of Windows Firewall with Advanced Security in the Group Policy Editor.

Open the Group Policy Management Console on your domain controller, then open the Default Domain Policy for the domain (or test domain if you are using it in a test environment) in Group Policy Editor.

In the left pane of the Group Policy Editor, open some of the buttons as shown in the figure below. The path is:

Computer ConfigurationPoliciesWindows SettingsWindows Firewall with Advanced Security

Right-click the button and select **Properties** .

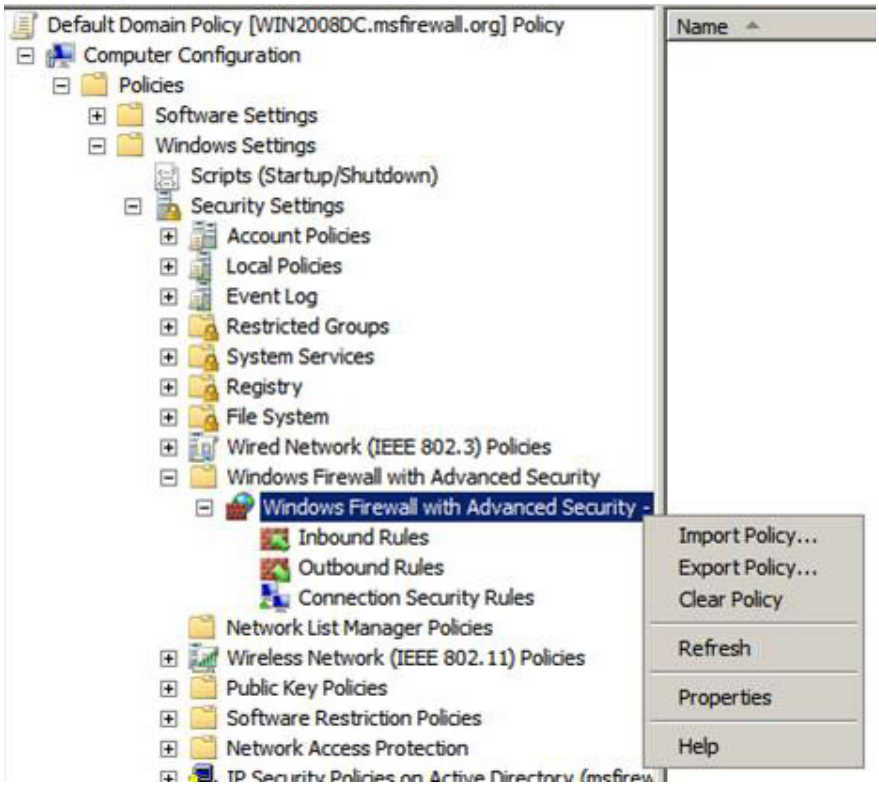


Figure 1

In the Windows Firewall with Advanced Security dialog box, click the **IPsec Settings** tab. On the IPsec Settings tab, click the **Customize** button.

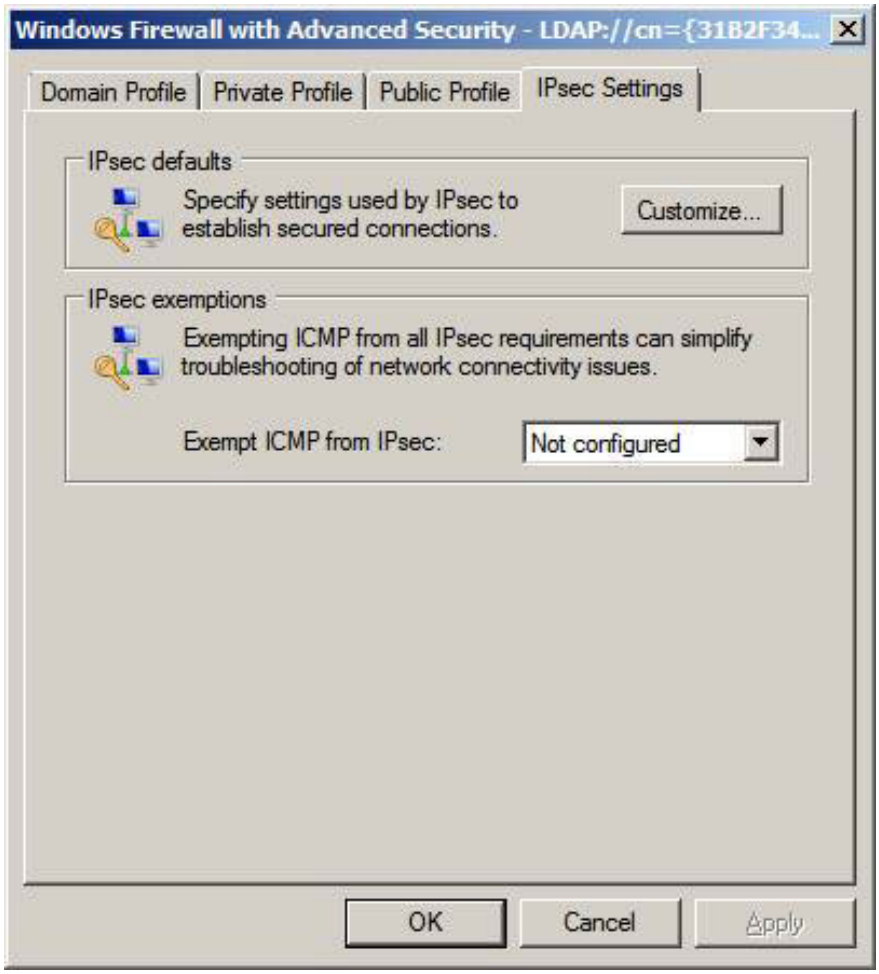


Figure 2

In the Customize IPsec Settings dialog box, select the **Advanced** option in the Data protection (Quick Mode) pane. Click the **Customize** button.

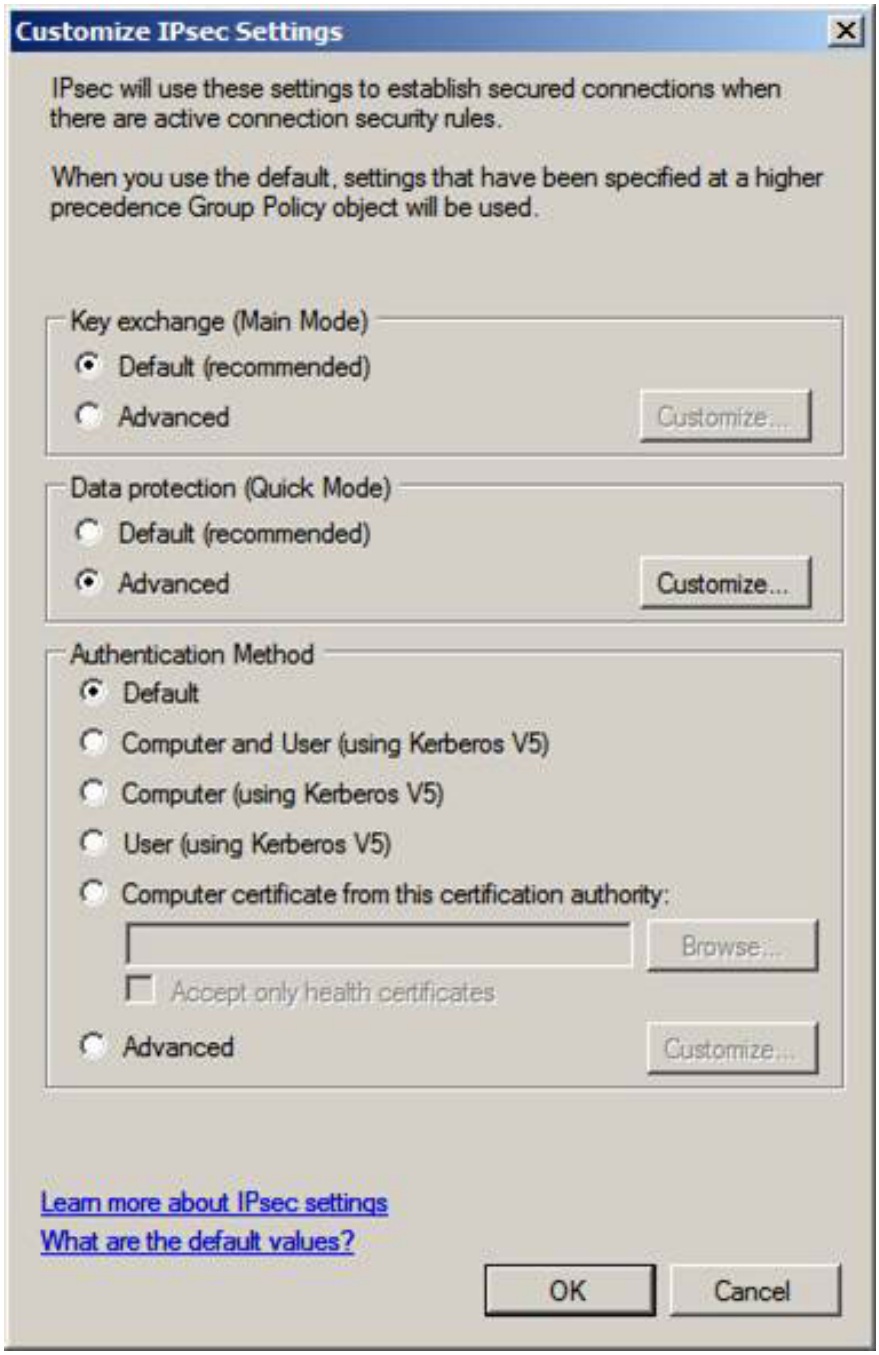


Figure 3

In the Customize Data Protection Settings dialog box, check the **Require encryption checkbox for all connection security rules** . Note that AES-128 will be used by default, but if the client / server combination does not support this level of encryption, they will return to 3DES (triple DES). Click **OK** .

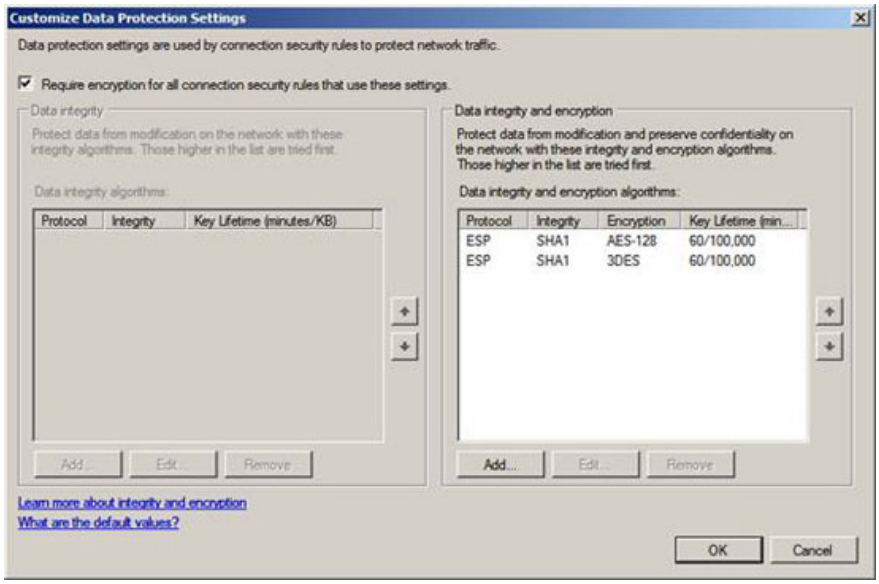


Figure 4

Now that we have configured the default IPsec settings to enable encryption of the connection between isolated hosts, we can perform a job to create connection security rules.

Create a security rule for the Domain Controller

It should be noted that domain isolation testing and testing with IPsec has a big problem related to domain controllers. Whenever we configure IPsec policies to require security for DC, connections from domain members will fail and domain members will not be able to access the login screen. However, if you configure IPsec rules to require security, domain members will be able to log in and connect to the domain controller. In addition, when security 'requests' are configured, clients will be able to establish secure IPsec connections for domain controllers after receiving Group Policy on the connection that we assume is not secure.

We can request security when connecting to a domain controller. This will establish a secure connection with the domain controller, even without requiring security for the connection.

In the Group Policy Editor, navigate to the Connection Security Rules button in the left pane of the console in Windows Firewall Advanced Security Node, as shown in the figure below. The full path for this button is:

Computer ConfigurationPoliciesWindows Settings Windows Firewall with Advanced SecurityConnect Security Rules

Right-click the **Connection Security Rules** button and select **New Rule** .

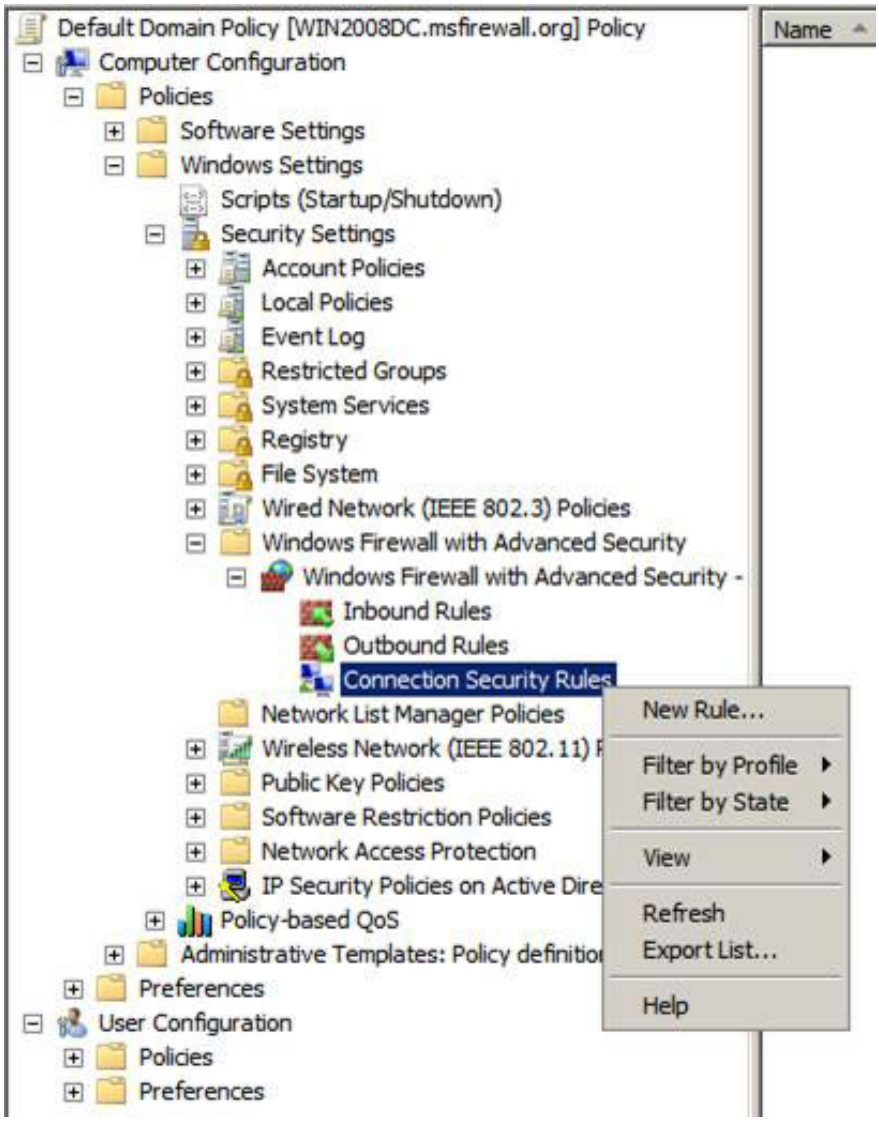


Figure 5

On the Rule Type page, in the New Connection Security Rule Wizard, select the **Isolation** option and click **Next** .

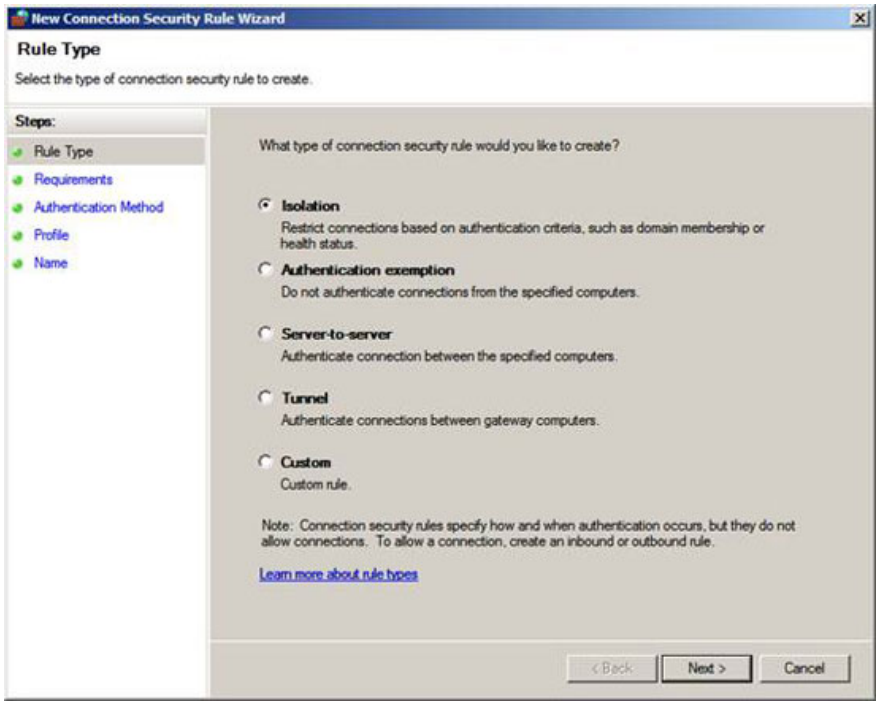


Figure 6

In the Requirements page, select Request **authentication for inbound and outbound connections** . When you select this option, authentication is required when the computer creates an outbound connection to another computer, and when another computer makes an inbound connection to this computer. If authentication is successful, IPsec security will be applied to sessions. However, if authentication fails, the computers will return to unauthenticated connections.

Click **Next** .

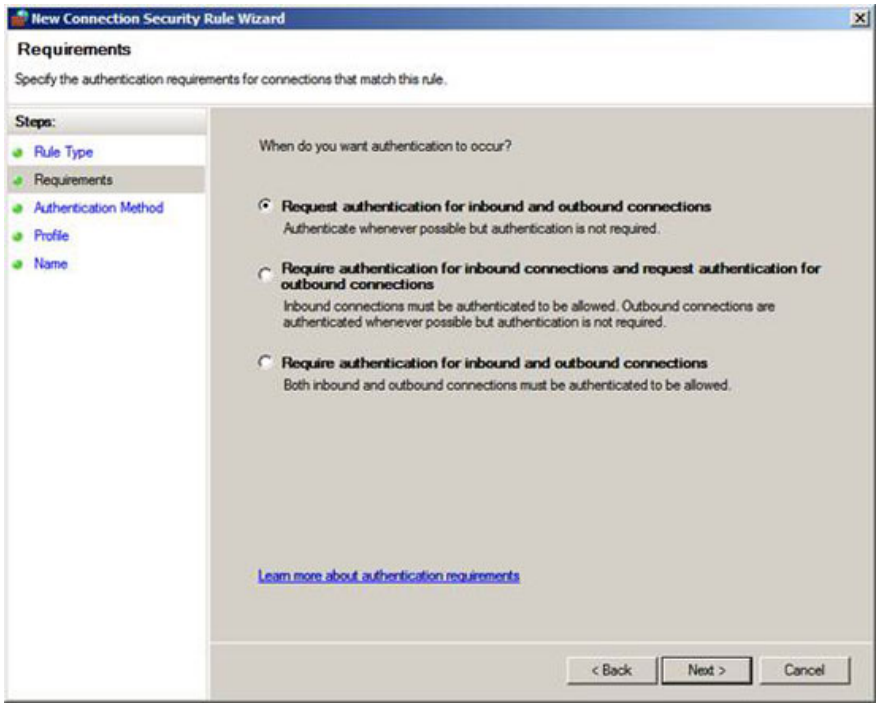


Figure 7

On the Authentication Method page, select the **Default** option. This option is determined by the IPsec Defaults settings from the **Properties** of the Windows Firewall with Advanced Security dialog box we saw. We have looked at the details of that dialog box in part one of this series, so you should check the detailed information about IPsec's default policies.

The default settings will use Kerberos authentication. Since all domain members can use Kerberos for authentication, there is no need for anything when you need to do it on clients and servers. There are several ways to authenticate, such as computer certificate - Computer Certificate or pre-shared key - pre-shared key. But the safest method is still Kerberos, plus that Kerberos is easy for administrators, which is the most obvious way to do it.

Click **Next** .

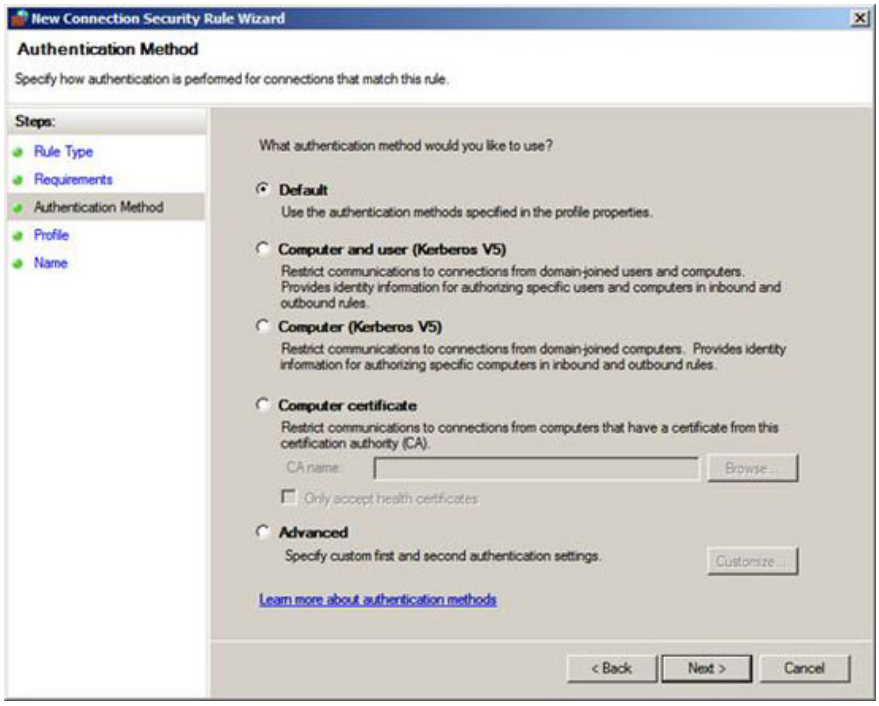


Figure 8

On the Profile page, remove the **Private and Public** checkboxes. You won't want your mobile computers to worry about isolating IPsec domains when they're not in the network.

Click **Next** .

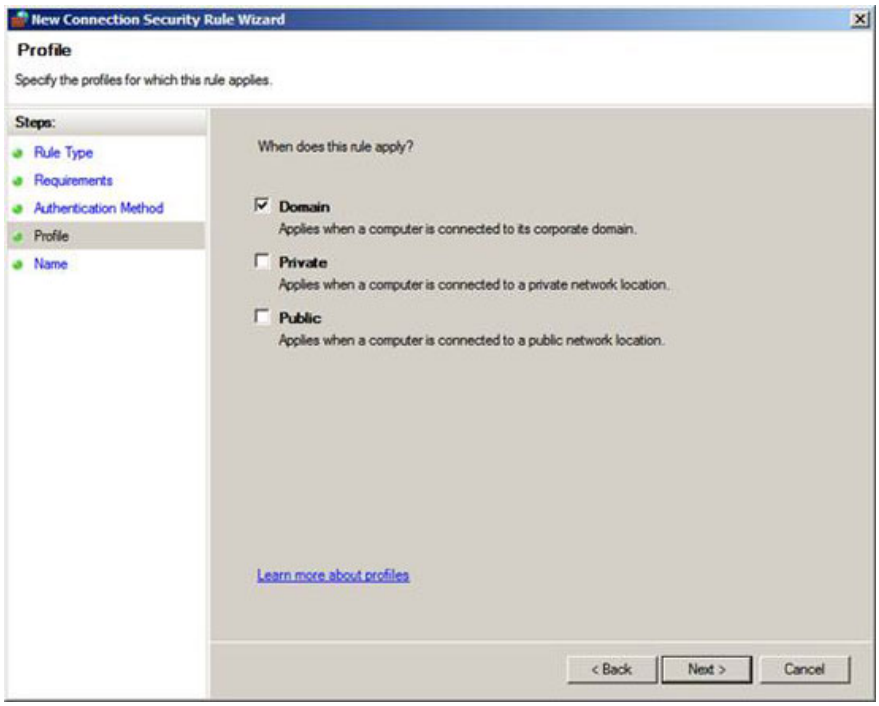


Figure 9

On the Name page, put a name. In this example we have named the rule **DC Request Security** . Click **Finish** .

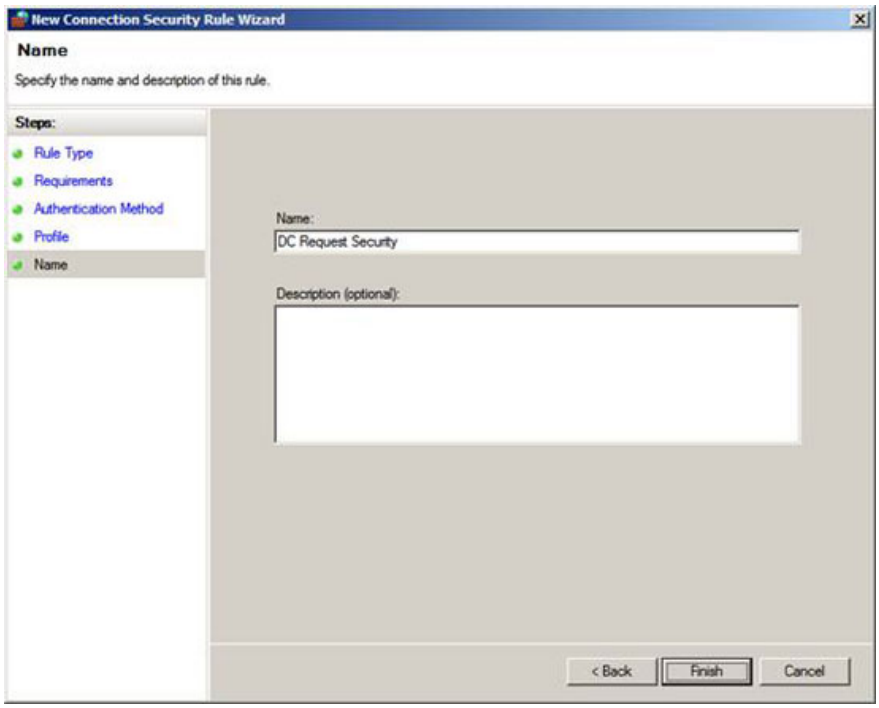


Figure 10

You should see the rule in the list of rules as shown in the figure below. We are still not done with the rule, because we have to configure the IP addresses that this rule also applies. As you can see in the current line, the rule applies to any Endpoint 1 and Endpoint 2. Endpoints can be an IP n and a different IP address, or one can be a group of IP addresses and the other endpoint is an IP address.

In this example we need to create an endpoint that is all the IP addresses on the network and the second endpoint is the IP address of the domain controller used in this example.

Right-click **DC Request Security Rule and** click **Properties** to create these changes.

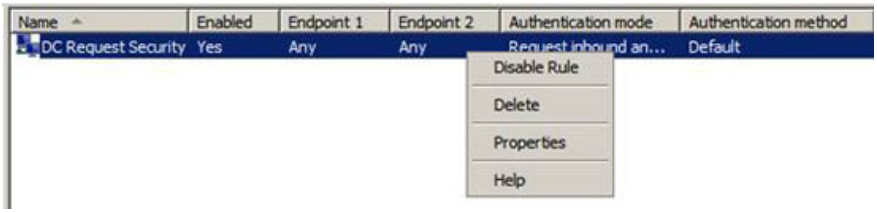


Figure 11

In the DC Request Security Properties dialog box, select the **These IP addresses option** in the Endpoint 2 box. Then click the **Add** button.

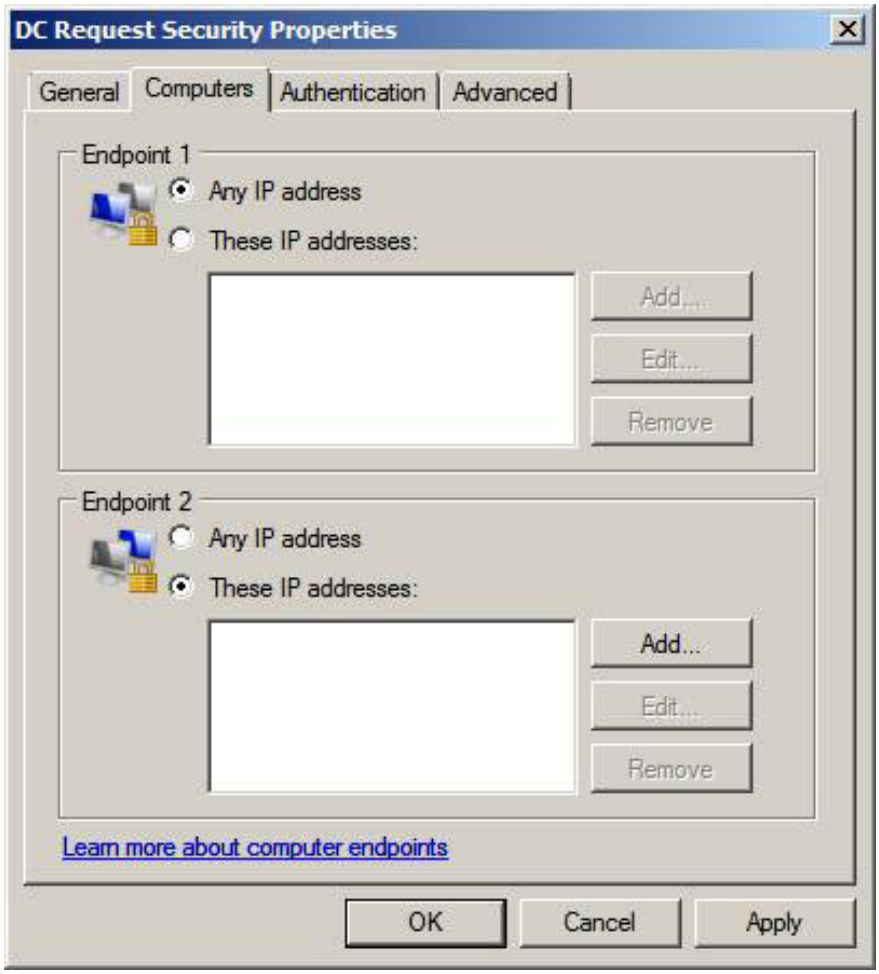


Figure 12

In the IP address dialog box, put that IP address of the domain controller. Select **this IP address or subnet option** and enter that IP address. Note that you also have other options like **This IP address range** and **Predefined set of computers** . The **Predefined set of computers** option allows you to choose from a number of infrastructure servers, such as DHCP, DNS, WINS and default gateway so that computers that cannot be authenticated can be exempted from authentication with infrastructure server. Examples are Macs, Unix, Linux and other operating systems that can use Kerberos for authentication.

Click **OK** .

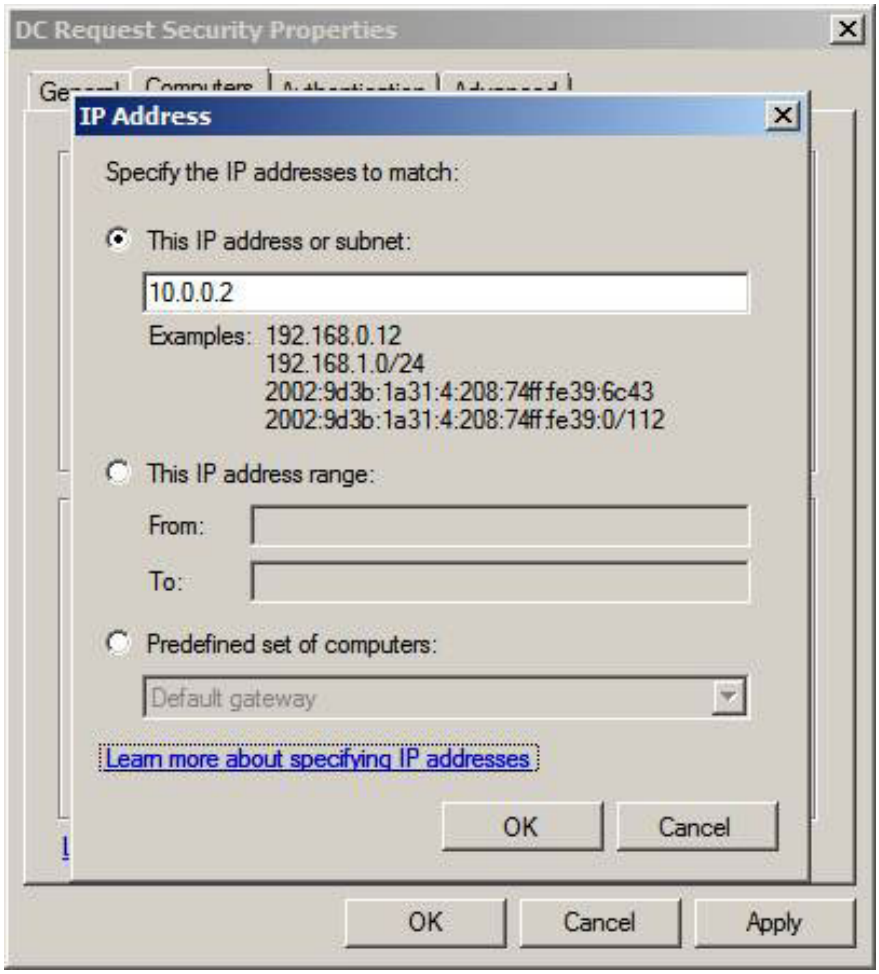


Figure 13

You will see the IP address of the DC in the Endpoint 2. Click **OK** in the **DC Request Security Properties** dialog box.

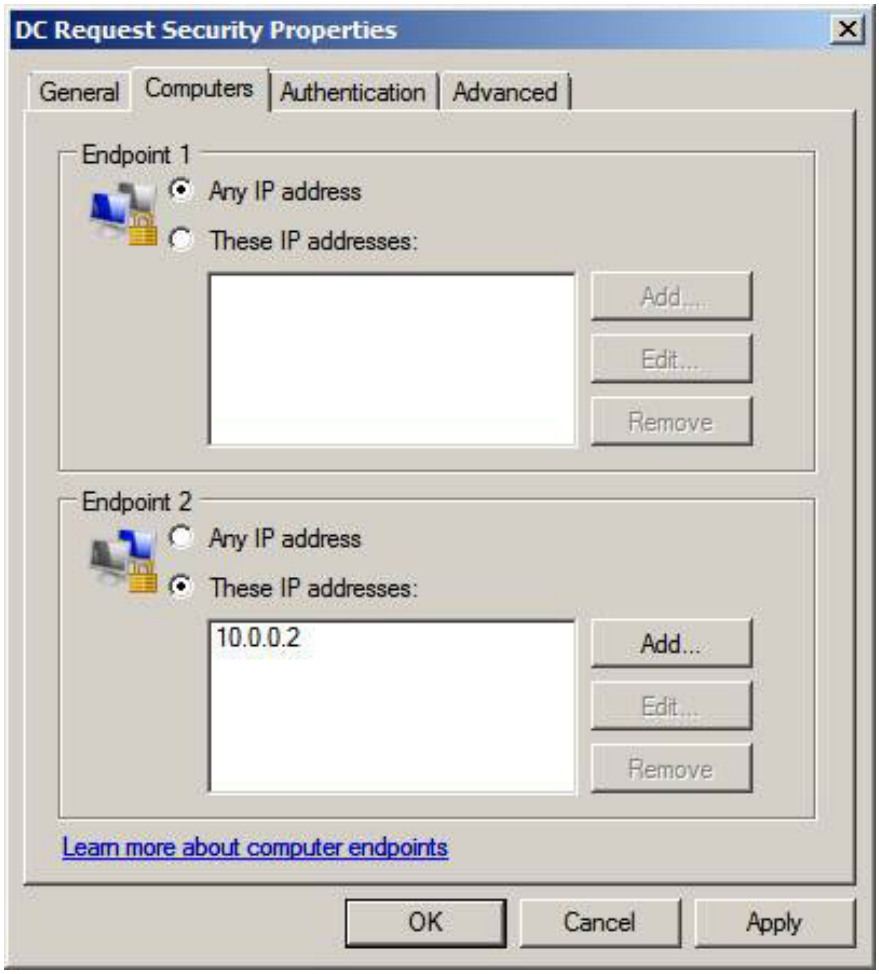


Figure 14

You will also see the domain controller's IP address in the Endpoint 2 column on the DC Request Security line

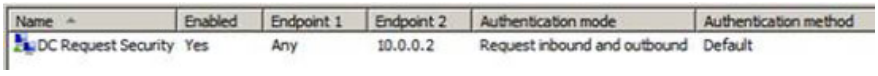


Figure 15

Now that DC has requested the security policy in place, we can create a domain isolation rule for the server and client to request security when connecting to other domain members.

Conclude

In this section (3a), part one of two sections on how to create a domain isolation policy using the Windows Firewall with Advanced Security interface integrated in the Windows Group Policy Editor, we have configured the IPsec policy to wear. intended to enforce ESP encryption. Then encrypted an IPsec policy rule for the domain controller and changed it by setting Endpoint 2 to the domain controller's IP address.

In Part 3b of this series, we will create a server and client domain isolation rule, and then configure the server to

accept Ping requests.