Overview of Windows Server 2008 Firewall with advanced security features (continued part 3)

In this article, I will show you how to create an IPsec isolation domain policy in a simple network, create a quarantine domain rule for servers and clients that require security (authentication), Configure the server to use ping connections sent to them to check the newly created rule.

Overview of Windows Server 2008 Firewall with advanced security features - Part 1
Overview of Windows Server 2008 Firewall with advanced security features - Part 2
Overview of Windows Server 2008 Firewall with advanced security features - Part 3

Thomas Shinder

In Part 3, how to create a logical domain policy using the IPsec and Windows Firewall with Advanced Security console built into the Windows Server 2008 Group Policy Editor, we showed you how to configure it. The default IPsec policy to use ESP encryption on IPsec-protected connections, then introduce how to create IPsec policy rules for domain controllers.

In this article, I will show you how to create an IPsec isolation domain policy in a simple network, create a quarantine domain rule for servers and clients that require security (authentication), Configure the server to use ping connections sent to them to check the newly created rule. Finally, this section examines the rule to confirm that IPsec is used for connections and that the connection is encrypted using ESP.

Create a quarantine domain rule for servers and clients

The next rule we will create is to isolate the domain for the server and the client. This rule will not require the same security as the previous rules that we created for connections with domain controllers. It only requires authentication and security when domain members connect with each other. Request authentication for inbound connections, security for outbound connections.

When you request security for inbound connections, it is required that computers that want to connect to a domain member verify the permissions for that domain member with Kerberos. If the computer does not authenticate, it means that the connection will fail. If the computer can authenticate, the connection will be allowed. This rule allows members to establish secure connections with each other while allowing domain members to connect to non-domain members (members cannot authenticate).

Navigate to the **Connection Security Rules** button in the left pane of the Group Policy Editor as you did when creating the previous rule.

Right-click **Connection Security Rules** , and then click **New Rule** .

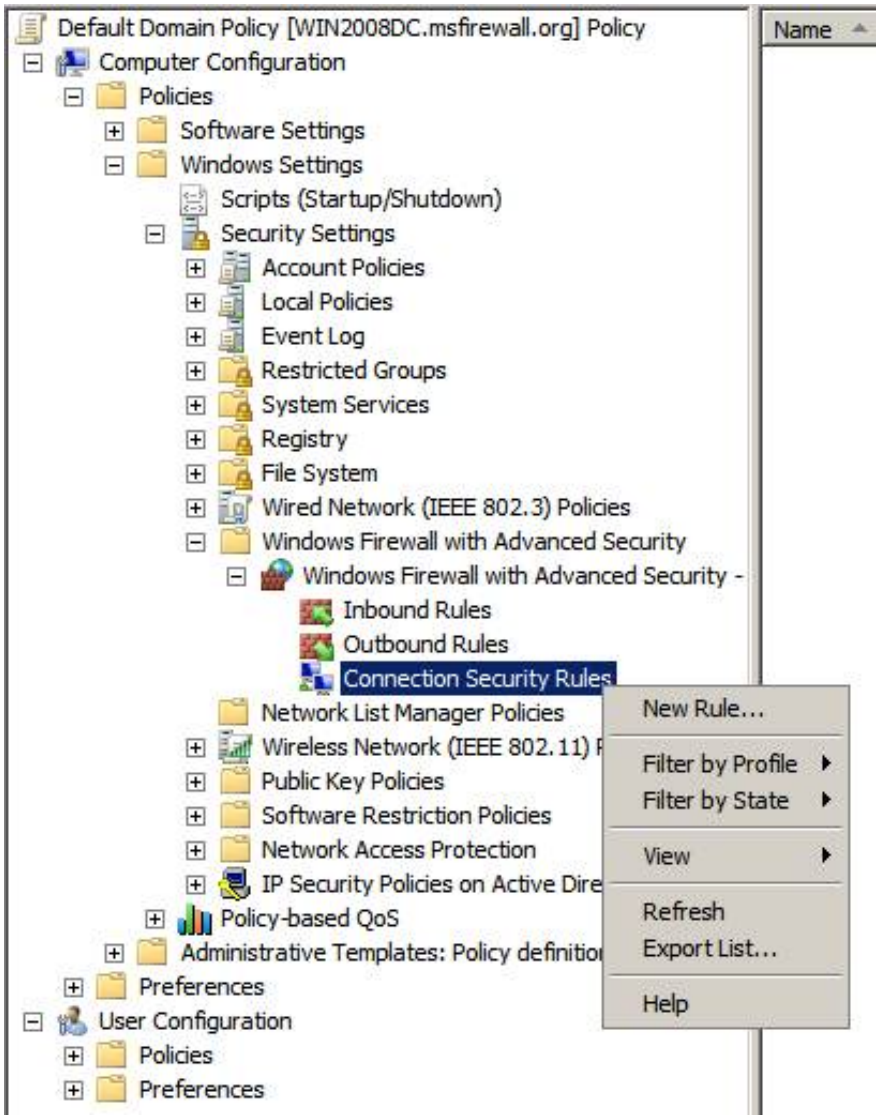


Figure 1

On the **Rule Type** page, select the **Isolation** option and click **Next** .

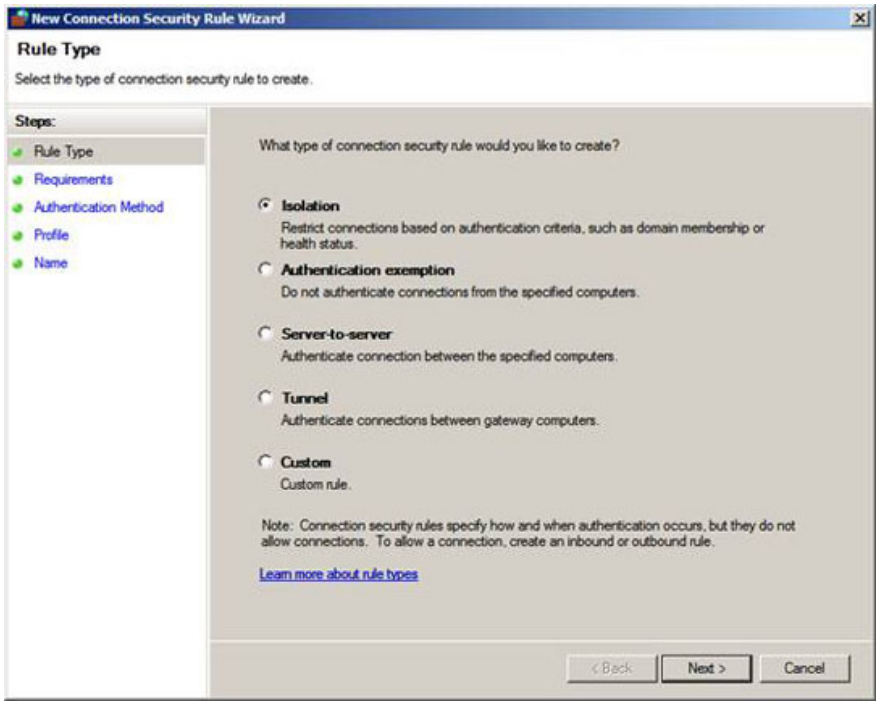


Figure 2

On the **Authentication Method** page, select **Default** and click **Next** .

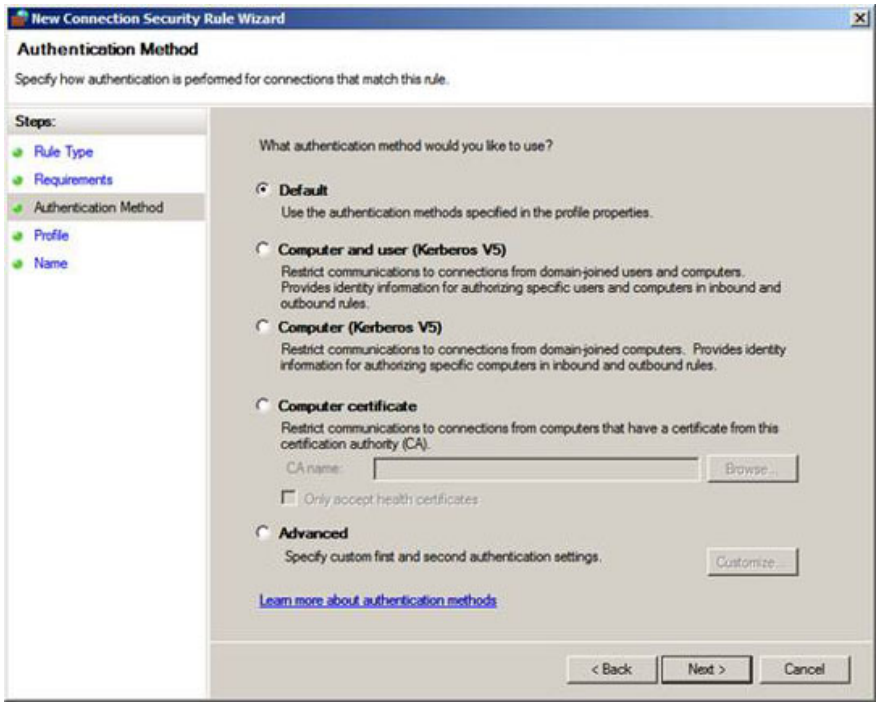


Figure 3

On the **Name** page, name the rule. In this example we set the **Client / Server Domain Isolation** and entered that instruction **Encrypts and secure connections between all machines that are not DCs or infrastructure servers (DNS, DHCP, Default Gateway, WINS)** .

Click **Next** .

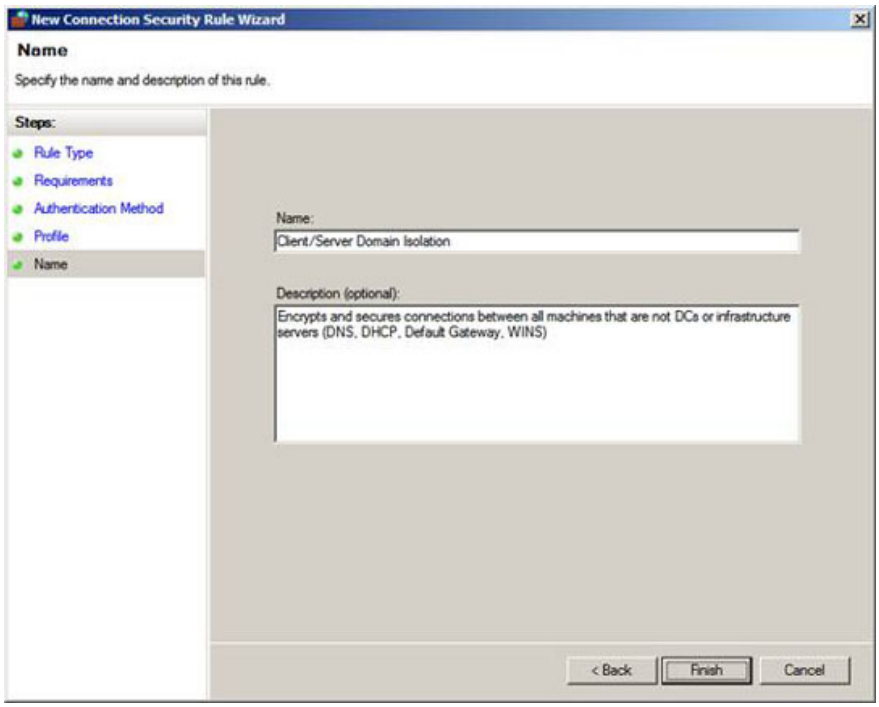
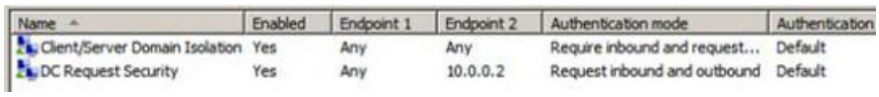


Figure 4

Notice the rule in the list of connection security rules. You might wonder if we will encounter any problems here, because **Client / Server Domain Isolation** rule has all IP addresses, including the domain controller's IP addresses.

However, this does not matter because the rules are evaluated from the most specific to the least specific. Therefore, a more specific rule will be evaluated before a less specific rule. In the case of the two rules we have here, **DC Request Security** rule is more specific because **Endpoint 2** is a specific IP address, while **Client / Server Domain Isolation** rule is **Endpoint 2** any IP address.



Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication
Client/Server Domain Isolation	Yes	Any	Any	Require inbound and request...	Default
DC Request Security	Yes	Any	10.0.0.2	Request inbound and outbound	Default

Figure 5

Note that in a production environment we need to create some exception rules for certain devices that are exempt from authentication. DHCP, DNS, WINS and default gateway addresses need to be used by machines that are not domain members and thus cannot authenticate using Kerberos.

Create Firewall Rule to allow incoming Ping

To check the configuration, you can use the ping command to ping the server from a particular Vista client. To do this, it is necessary to allow ICMP pings to send requests to the test server. Create a rule that allows Vista clients to ping the server using Windows Firewall with Advanced Security MMC.

On the server, open **Windows Firewall with Advanced Security** from the **Administrative Tools** menu.

To the left of the console pane of **Windows Firewall with Advanced Security,** right-click the **Inbound Rules** button in the left pane and click **New Rule** .

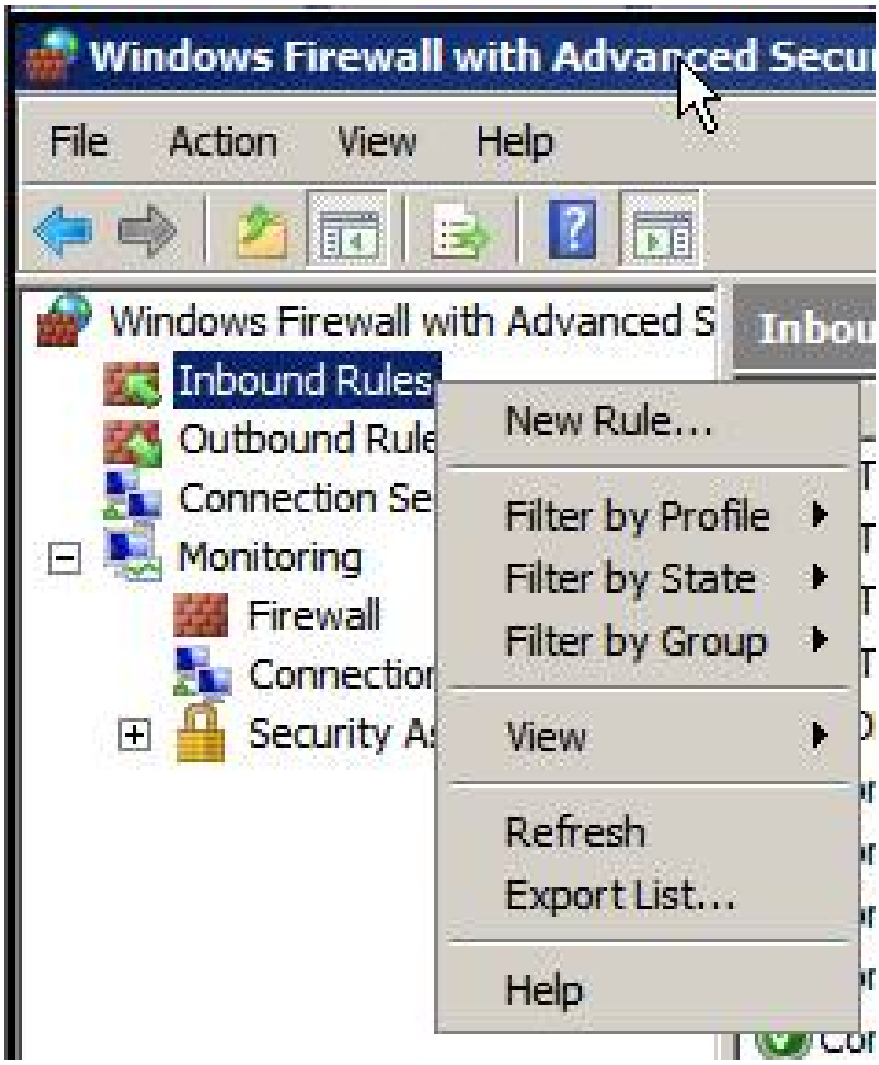


Figure 6

On the **Rule Type** page, select the Custom option and click **Next** .

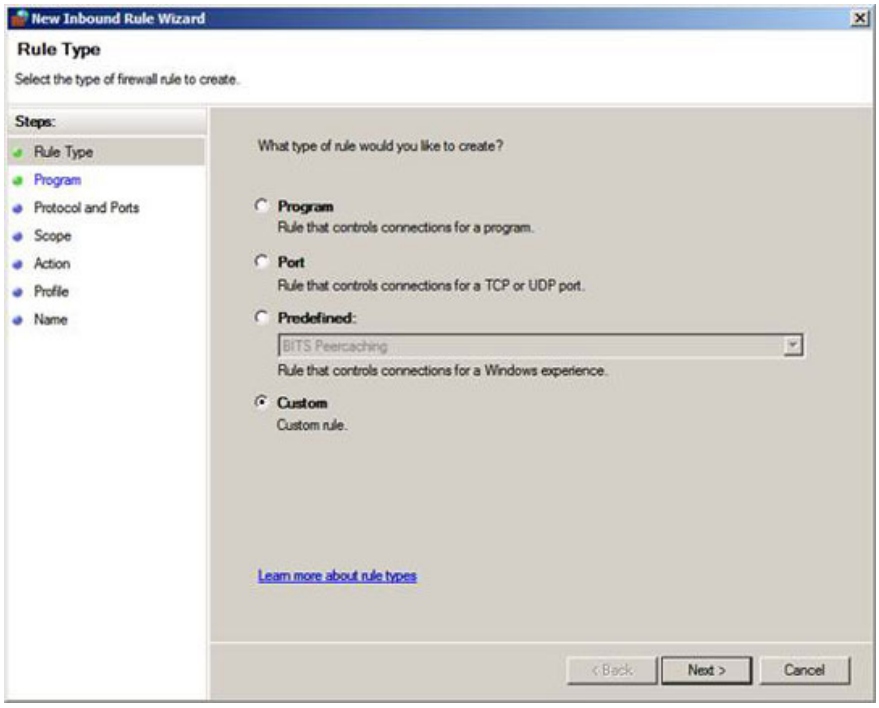


Figure 7

On the **Program** page, select the **All Programs** option and click **Next** .

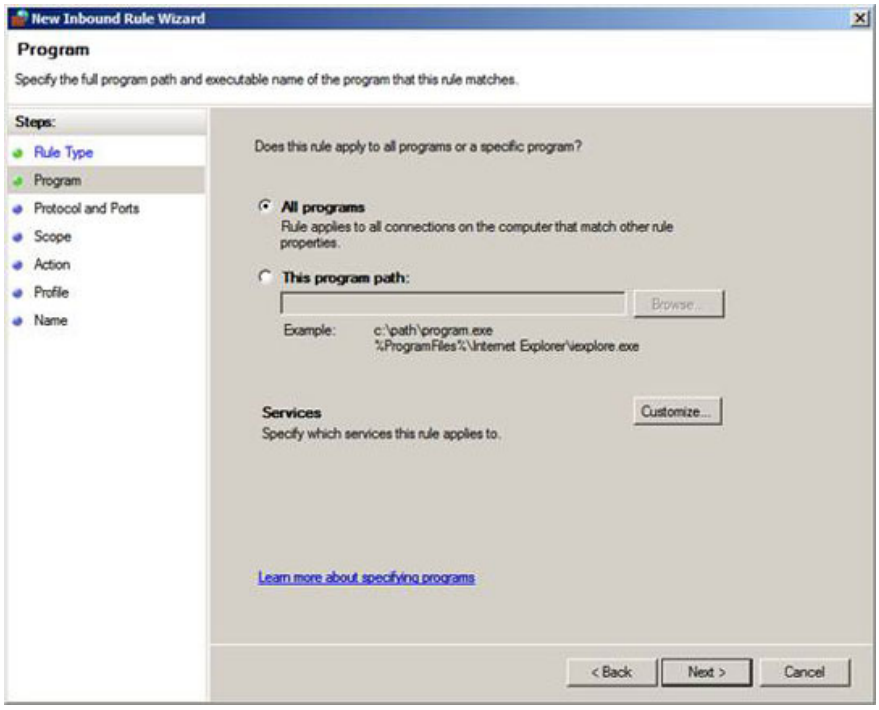


Figure 8

On the **Protocol and Ports** page, click the down arrow in the **Protocol Type** list and select the **ICMPv4** option **.**

Click the **Customize** button. In the **Customize ICMP Settings** dialog box **,** select the **Specific ICMP types option** . Then check the **Echo Request** checkbox. Click **OK** .

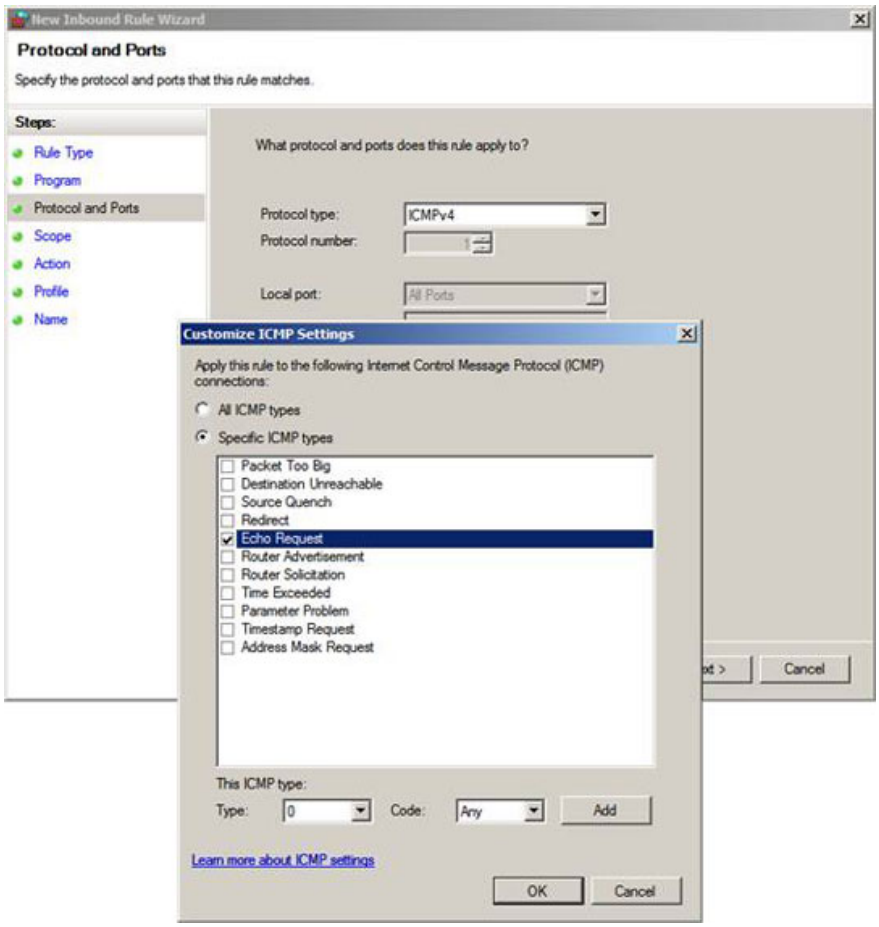


Figure 9

Click **Next** on the **Protocol and Ports** page **.**

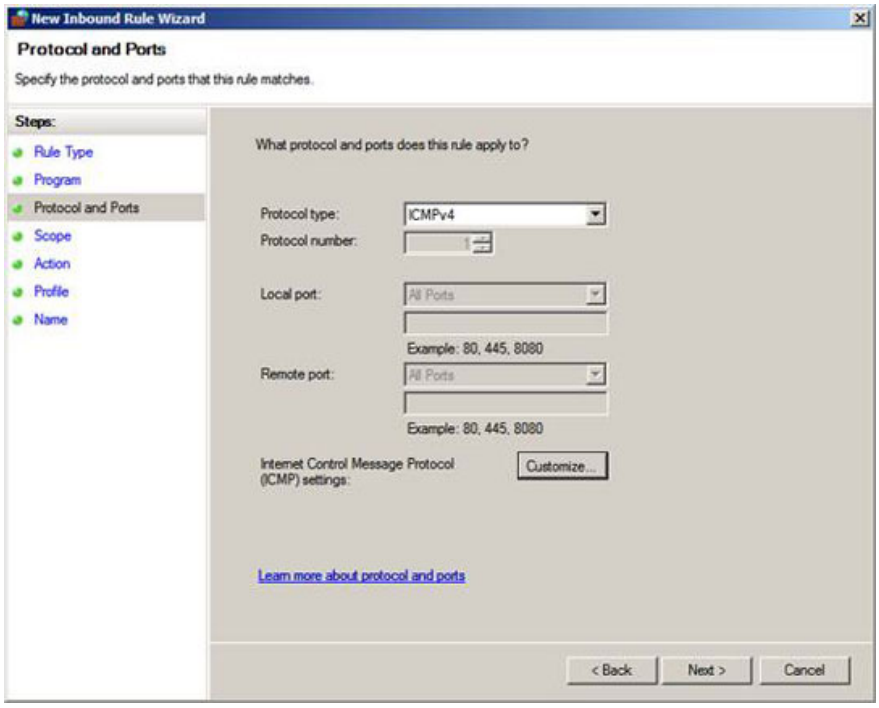


Figure 10

In the **Scope** dialog box, use the default settings for local and remote **IP addresses** , **Any IP address.** Click **Next** .

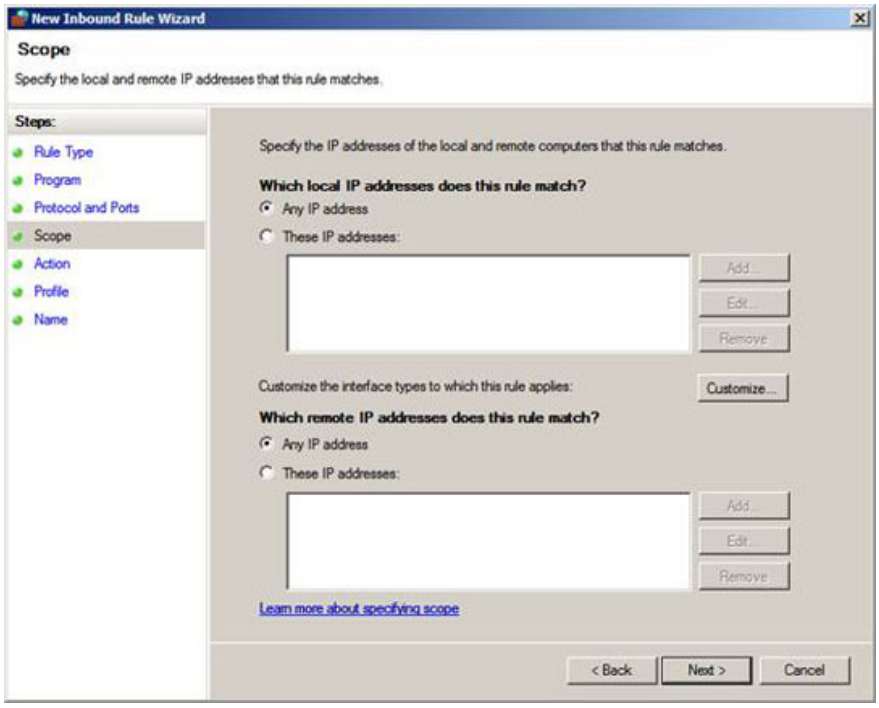


Figure 11

On the **Action** page, select the **Allow the connection option** and click **Next** .

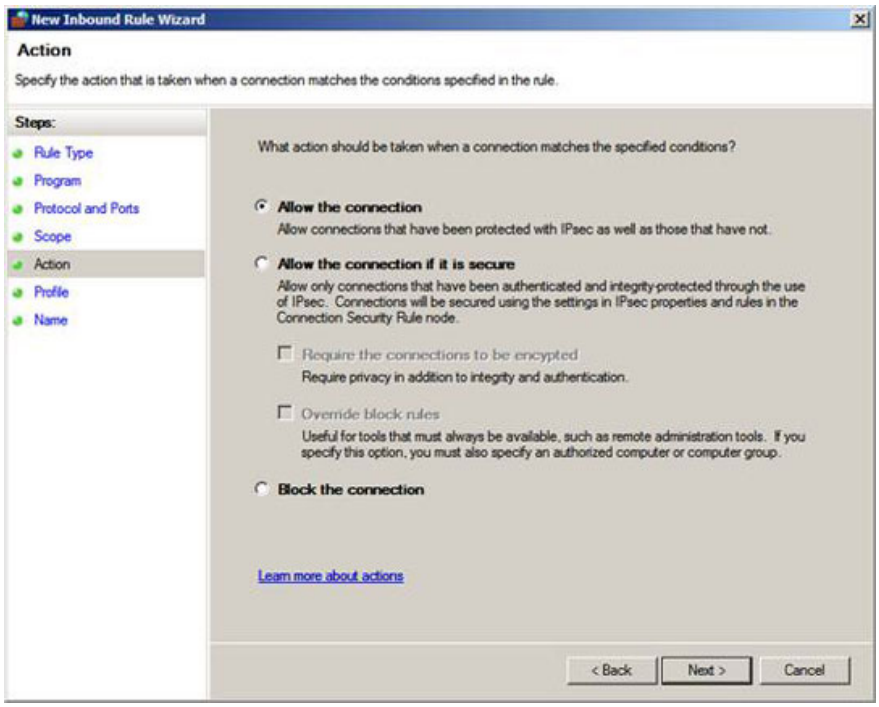


Figure 12

On the **Profile** page, remove the check marks from the **Private** and **Public** boxes and click **Next** .

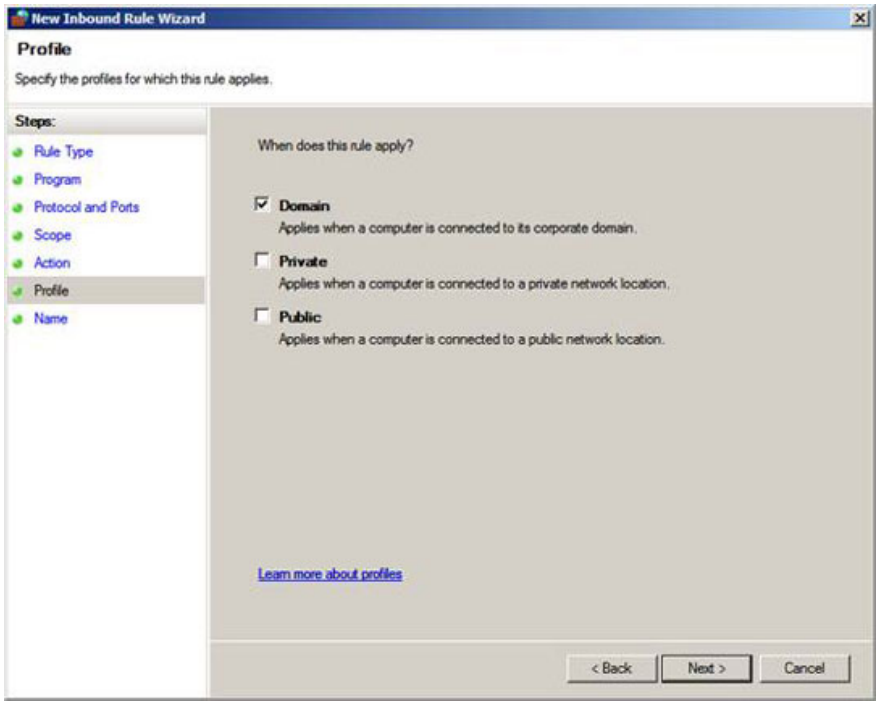


Figure 13

On the **Name** page, name the rule. In this example we name it **Allow ICMP Request** . Then click **Finish** .

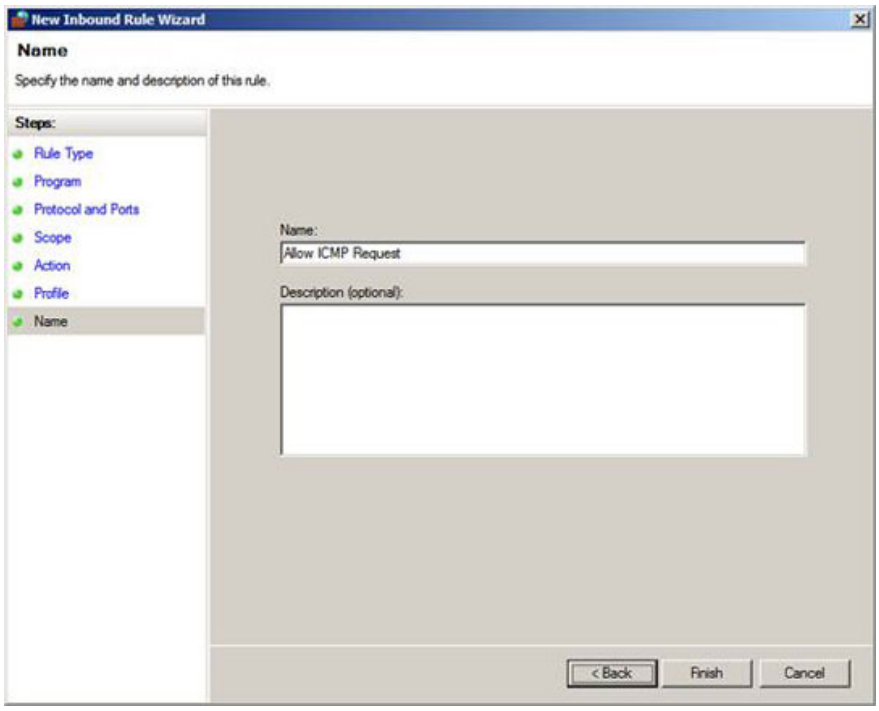


Figure 14

You can see **Allow ICMP Request** rule in the list of incoming rules.

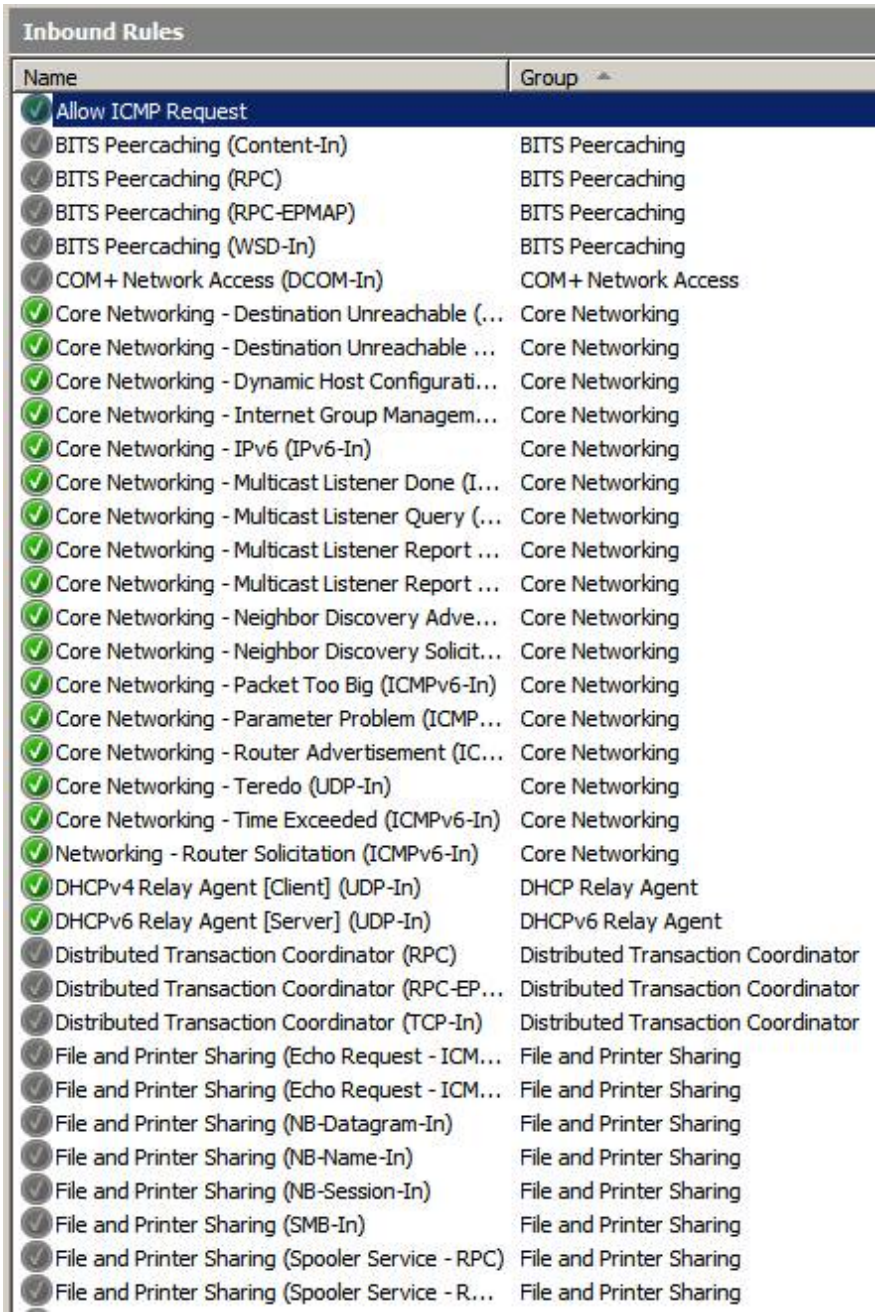


Figure 15

Observe the action of connection security

OK, now we're ready to see if things work! Go to the server and open the **Windows Firewall with Advanced Security** console, click the **Connection Security Rules** button in the left pane of the interface. You need to see the rules you created in Group Policy. If you do not see these rules, follow these instructions:

1. At the domain controller, open a command prompt and type **gpupdate / force** , and then press ENTER to update Group Policy on the domain controller.
2. After updating Group Policy on the domain controller, update Group Policy on the server by opening a command prompt and typing **gpupdate / force** , press ENTER to update Group Policy for the server.

3. If still not working, try restarting the server and login again.

Then refresh the entire view of **Connection Security Rules** on the server to see an updated list of these rules. This is a similar list that you see in Group Policy Editor.

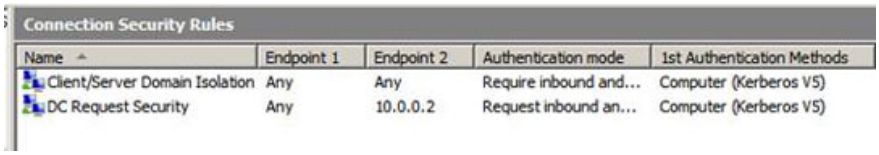


Figure 16

Click the **Main Mode** button in the left pane of the console. You must see that the server has established secure connections for both domain controllers and Vista clients. If you don't see secure connections to the Vista client, follow these instructions:

1. Run **gpupdate / force** trene Vista client
2. The Connection Security Rules configuration has been applied on Vista clients by checking them in the **Windows Firewall with the Advanced Security** MMC snap-in on this client.
3. If you don't see the work, restart the client
4. Ping to the Vista client from the server

After performing these steps, you need to see secure IPsec connections between the server and domain controller and the Vista client.

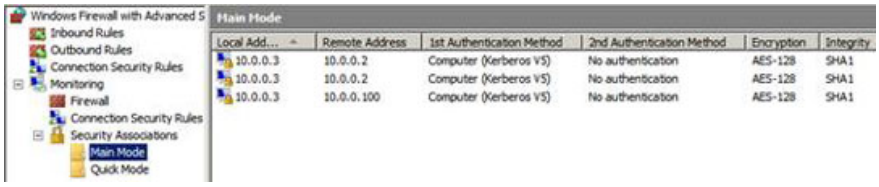


Figure 17

When you double click on one of the entries in the details pane of the **Main Mode** button, you can see the details of the secure connection.

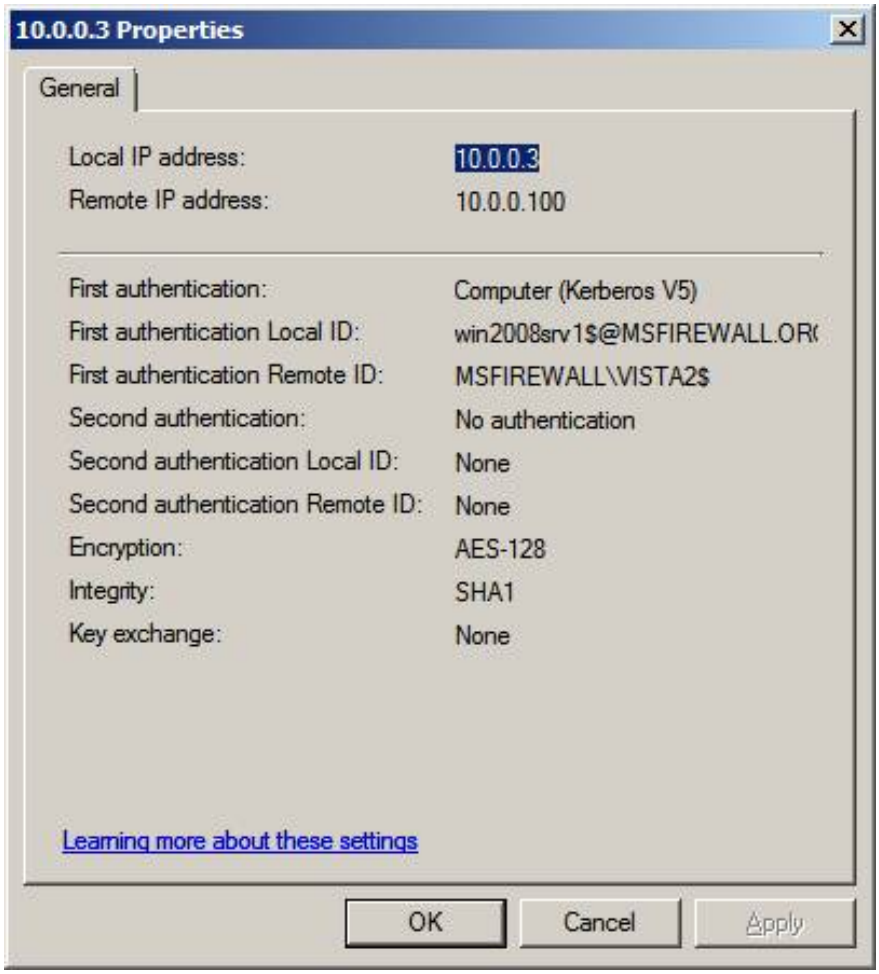


Figure 18

Click the **Quick Mode** button in the left panel of the console. You need to see secure connections for both domain controllers and Vista clients.

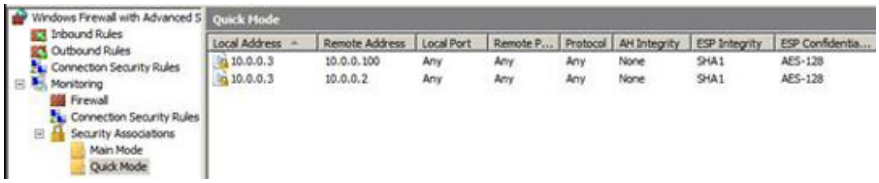


Figure 19

If you double click on one of the entries in the details pane of the **Quick Mode** button, you will see the details of the connection. Notice that **ESP confidentiality** is used and is using AES-128 bit encryption. This means that this connection is completely secure on the network and cannot be stolen by intruders.

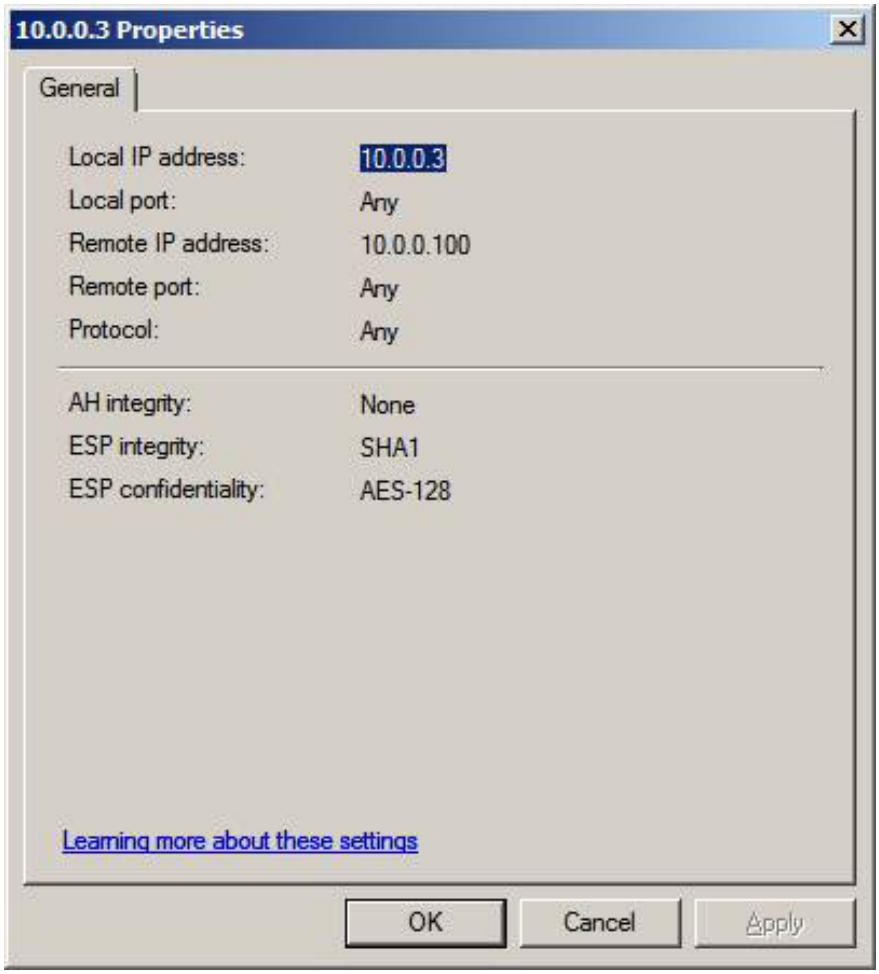


Figure 20

Conclude

In this article, I have shown you how to configure quarantine domain rules for servers and clients, and then configure the firewall on the server to allow incoming ping requests. Also in this article we checked to see if everything worked as expected by using the test features included in the Windows Firewall with Advanced Security console. This section also focuses on creating a simple quarantine domain policy to demonstrate how to configure isolated domain policies with the new tools available in Windows Server 2008 and Vista. More importantly, we demonstrate to you how to use Group Policy to focus on configuring domain isolation policy as a centralized management solution.

In the next part of this series we will demonstrate how to isolate the server. How useful is it when computers are not domain members? In that case we will show you how to use authentication methods to protect connections between computers that are not domain members.