Taking a look at some of the basics of the new IPsec Connection Security Rules wizard and how easy it is to get the Connection Security Rules working.

The WFAS interface provided a new way to configure IPsec rules, in the form of Connection Security Rules. When you create Connection Security Rules, you are actually configuring IPsec policies that enable you to control the encryption and authentication of traffic moving between two hosts. Connection Security Rules are a lot easier to configure and understand than the old method of creating IPsec rules using the Windows 2000/2003 interface.

To see how easy it is to create Connection Security Rules, let's look at an example. In this example, we'll look at another feature that was introduced with Windows Server 2008 and carried over to Windows Server 2008 R2: the ability to configure Connection Security Rules in Group Policy. The WFAS snap-in in Group Policy enables you to configure Connection Security Rules and make them easily deployable throughout your organization, and this scales much better than having to run the old IPsec wizard on each machine in your organization for which you want to use IPsec.

To see how this works, we'll go to a domain controller and open the **Group Policy Management** editor. In the **Group Policy Management** editor, we'll right click on the **Default Domain Policy** and click **Edit**, as seen in Figure 1 below.

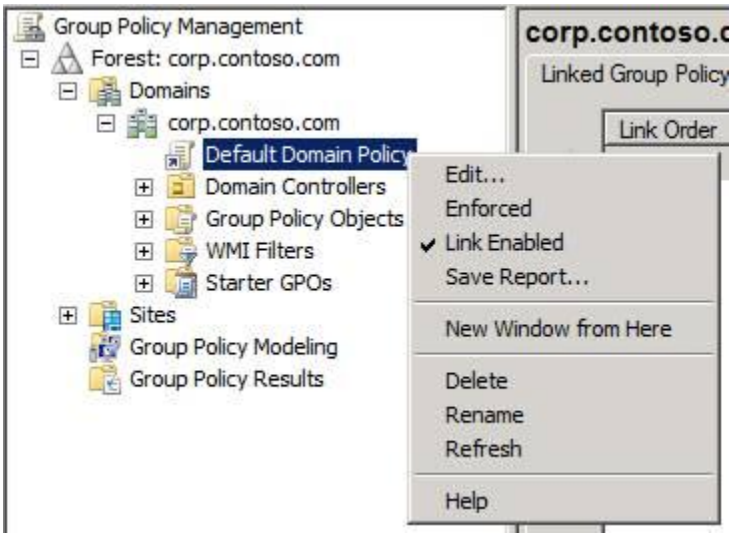


**Figure 1**

In the left pane of the console, we'll navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security – LDAP\Connection Security Rules**. This is shown in Figure 2.

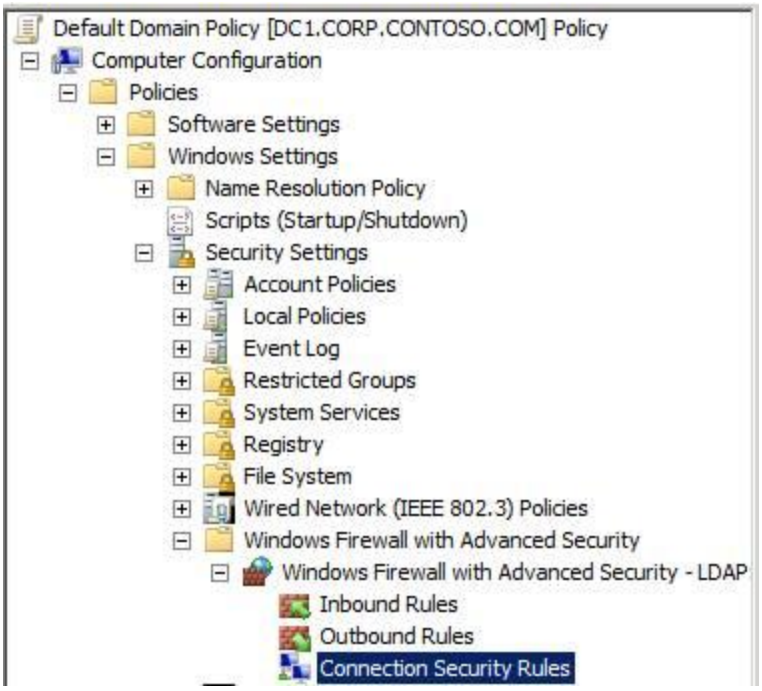


**Figure 2**

Now we'll right click on **Connection Security Rules** and click **New Rule**. This brings up the **Rule Type** page for the **New Connection Security Rule Wizard**, shown in Figure 3. As you can see, there are quite a number of options here. In this example, we'll create a **Server-to-Server** connection security rule. This rule will enable IPsec security between two machines on my lab network. We'll select the **Server-to-server** option and click **Next**.

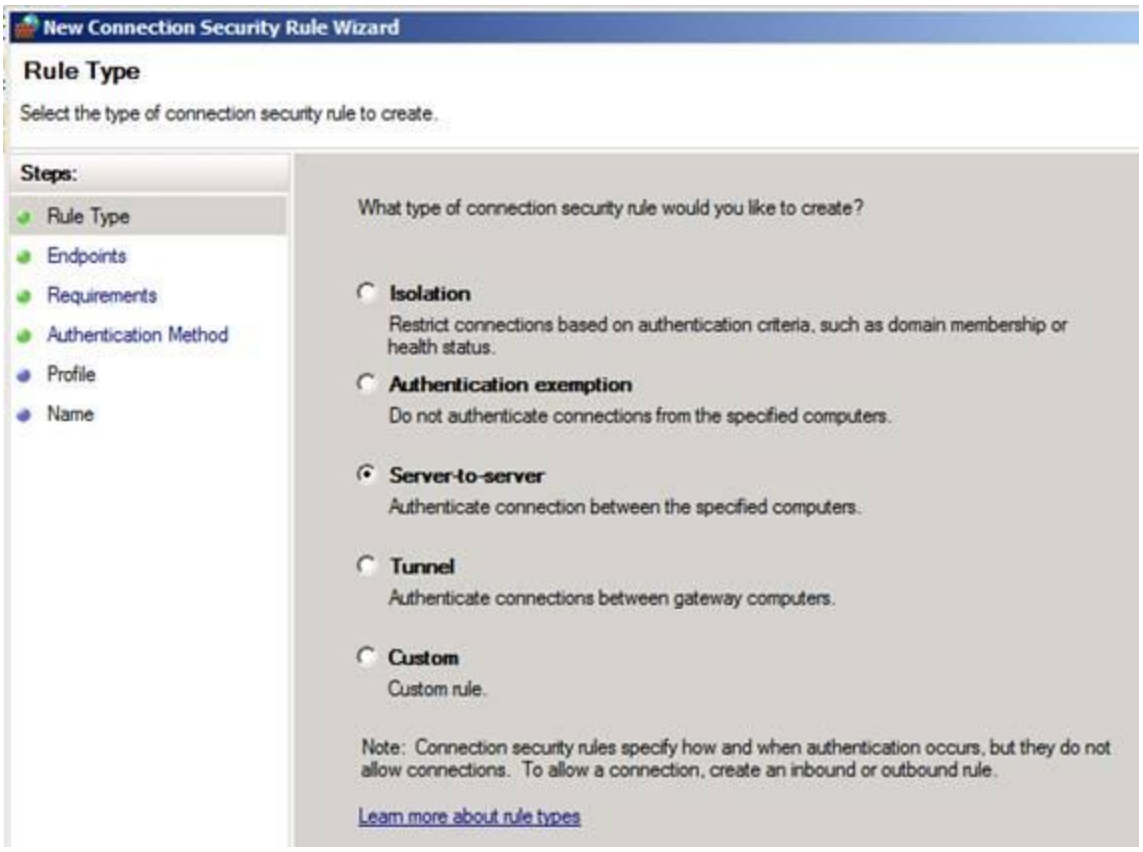


**Figure 3**

On the **Endpoints** page, shown in Figure 4, we define the endpoints to which we want this rule to apply. In this example, we have a server named **APP1** and we want to make sure that all connections to APP1 are secured with IPsec. For the **Endpoint 1** computer, click the **Add** button.

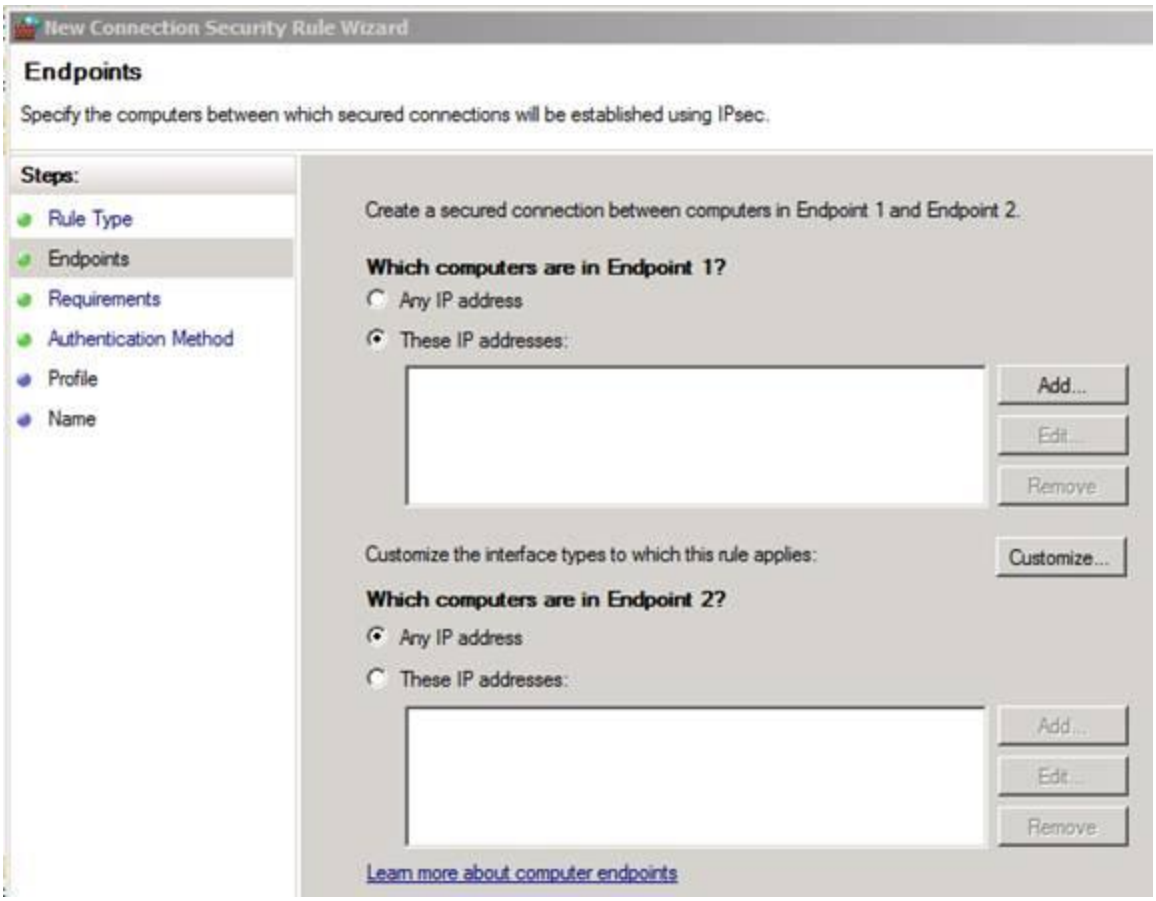


**Figure 4**

In the **IP Address** dialog box, shown in Figure 5, we'll select the **This IP address or subnet** option and enter the IP address of APP1. Then click **OK**.

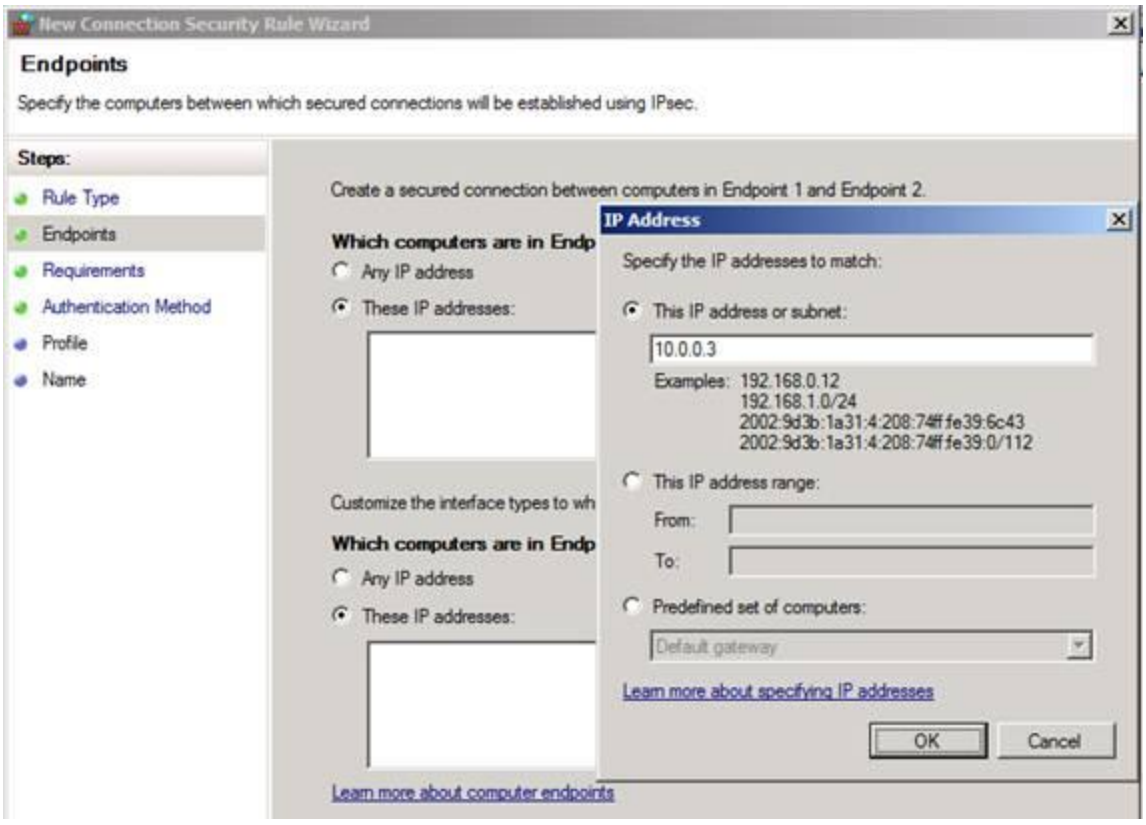


**Figure 5**

Now we'll configure the **Endpoint 2** to be any computer. We'll select the **These IP addresses** option for **Endpoint 2** and then click **Add**. In the **IP Address** dialog box, shown in Figure 6, we'll select the **This IP address or subnet** option and enter **10.0.0.0/24** and then click **OK**.

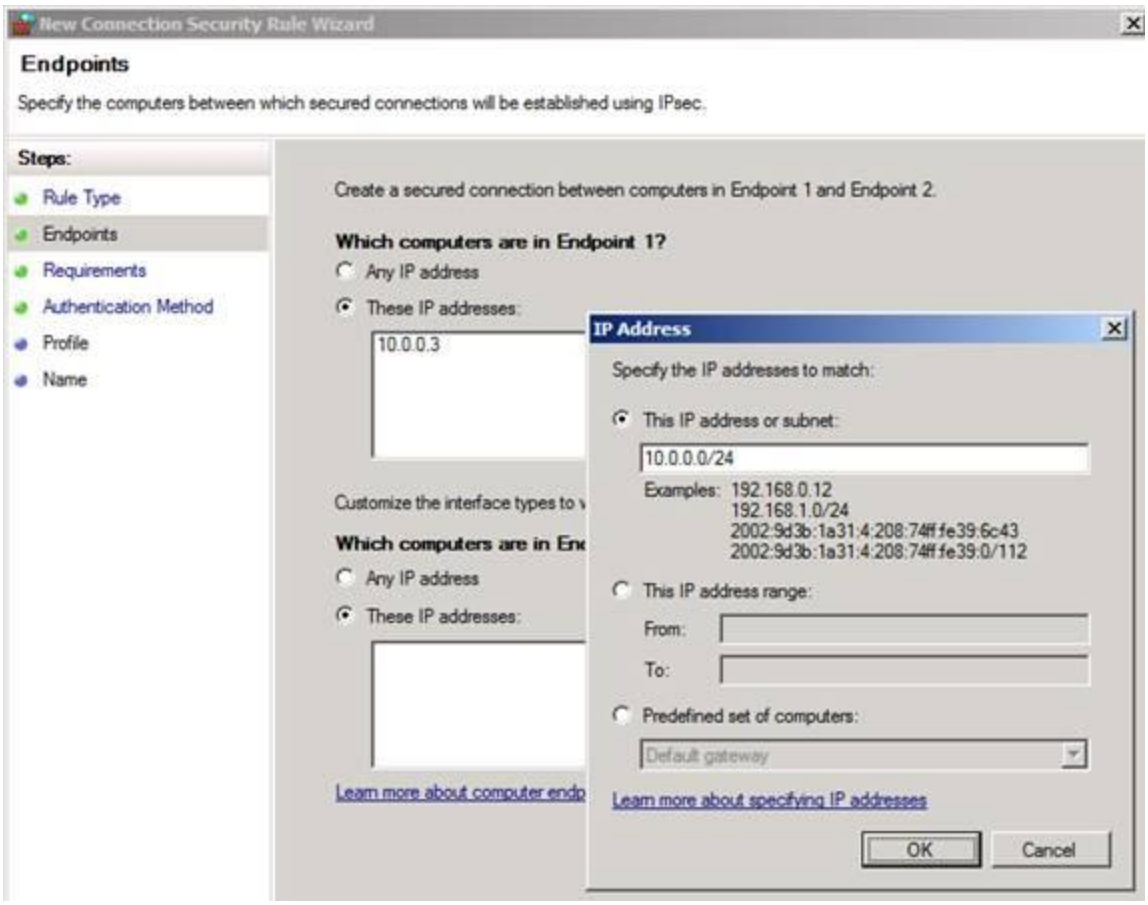


**Figure 6**

Now we see on the **Endpoints** page, as in Figure 7, we have the ability to define the endpoints for the IPsec connection. This rule will be applied to all endpoints that connect to APP1. Click **Next**.

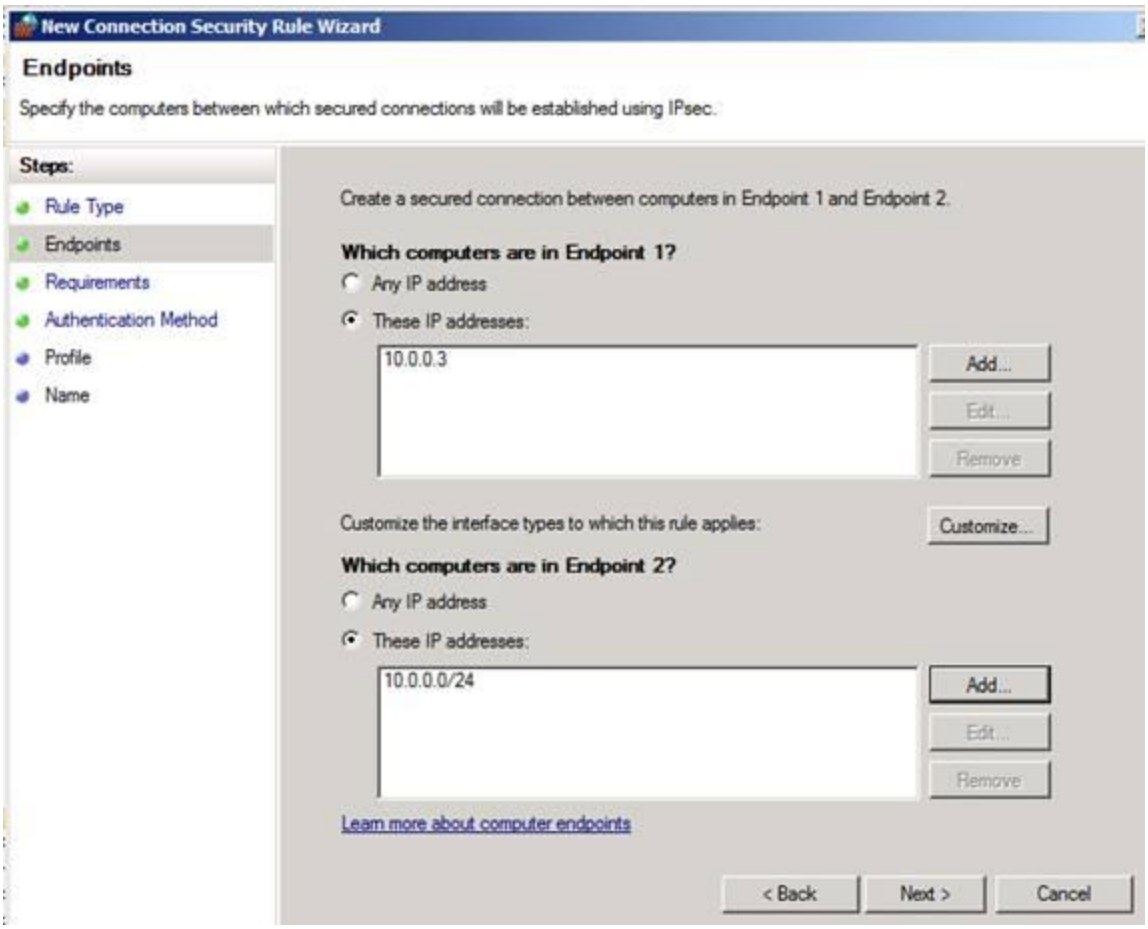


**Figure 7**

Before we leave the **Endpoints** page, notice that there is a **Customize** button. When you click this button, you can see the **Customize Interface Types** dialog box that's shown in Figure 8. By default, the rule applies to all interfaces, but if you want to limit the types of interfaces that the rule is applied to, you can change from **All interface types** to **These interface types**. We will use the default settings, so we won't change anything here.

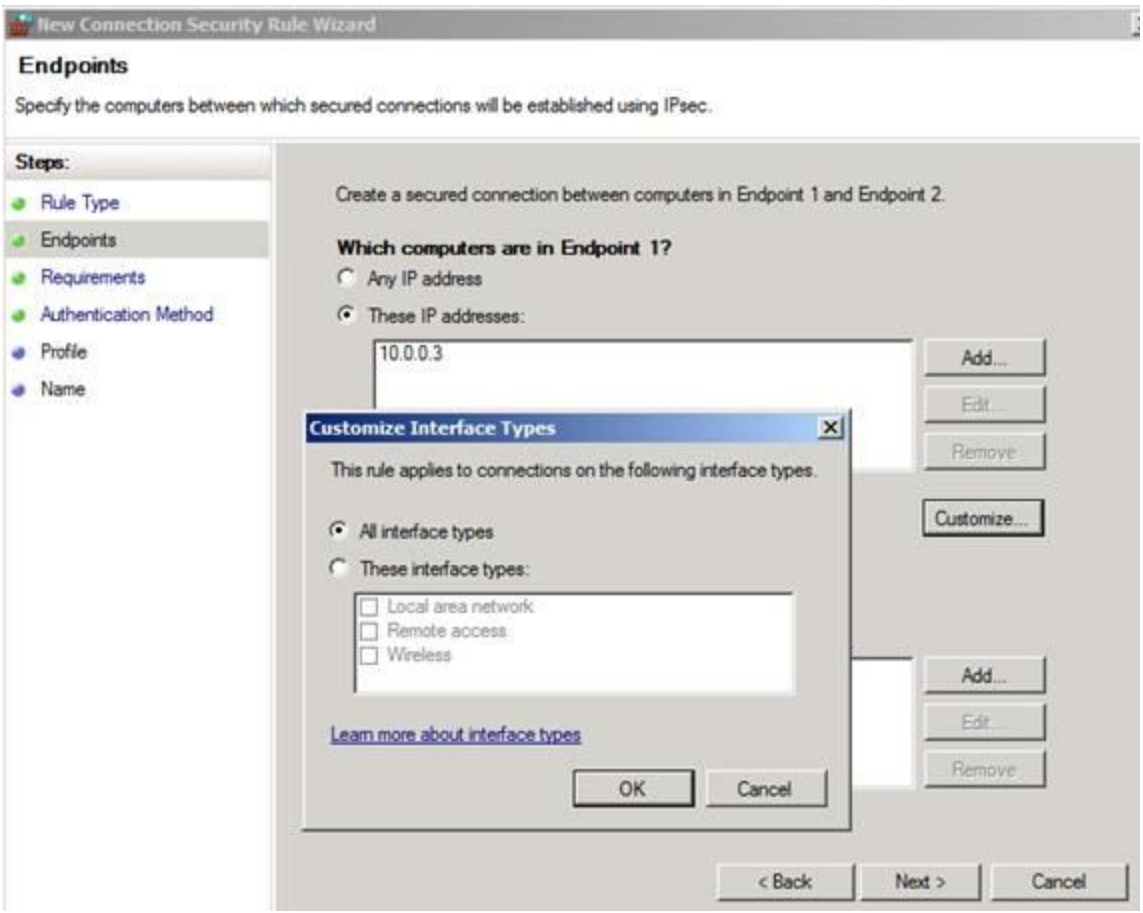


**Figure 8**

On the **Requirements** page, shown in Figure 9, you can choose what kind of authentication you want to use. In this example, we'll choose **Require authentication for inbound connections and request authentication for outbound connections**. When we do this, whenever we have a combination of Endpoint 1 and Endpoint 2 hosts communicate, there will be a request for authentication when the computer sends an outbound request, and authentication will be required when there is an inbound request. This means that whenever a computer tries to connect to APP1, authentication will be required on the inbound connections to APP1. It's a little confusing, but when you think about it, it does make sense. It also means all other computers, when connecting to APP1, are going to request authentication from APP1, but in those cases it's optional. What we're really interested in are the inbound connections to APP1, and this rule is able to mandate that incoming connections to APP1 require authentication.

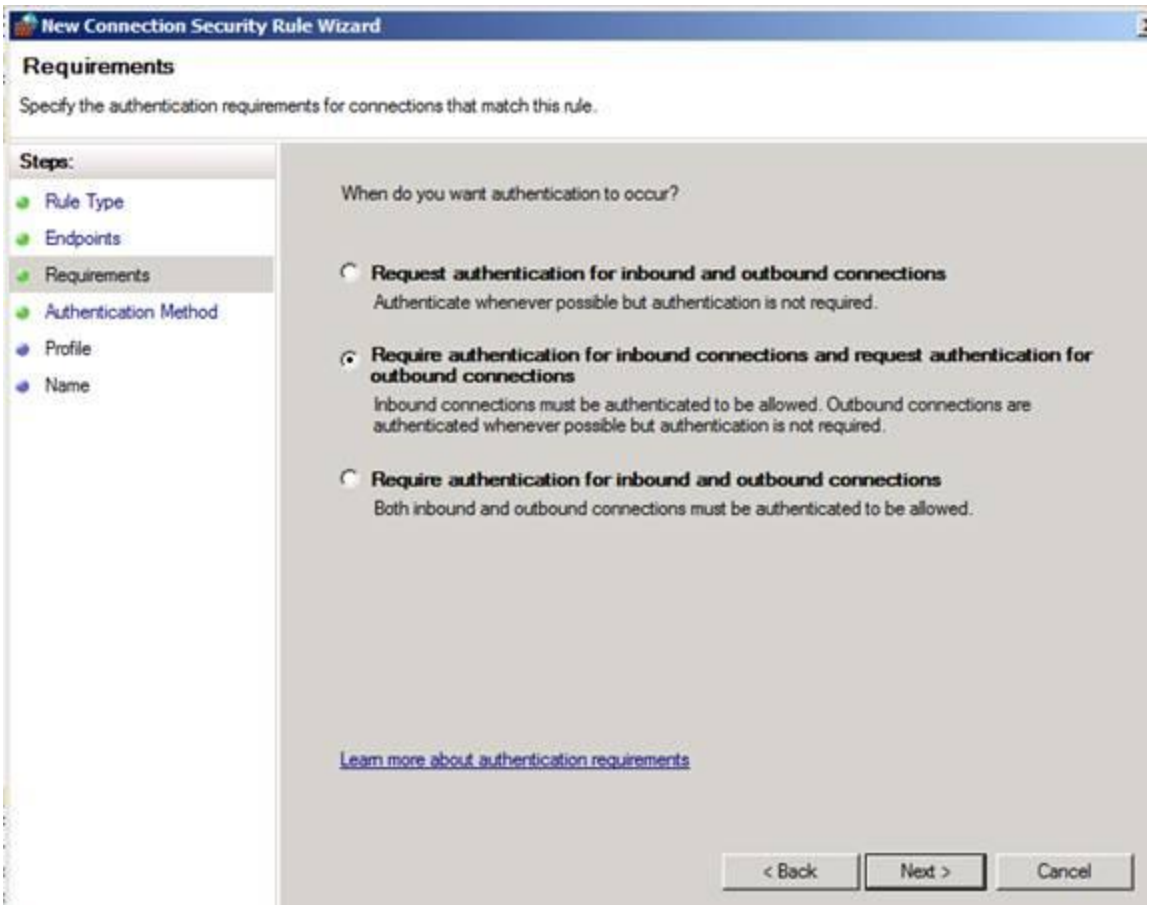


**Figure 9**

On the **Authentication Method** page, shown in Figure 10, you choose the authentication method. The default setting (which we'll use) is the **Computer Certificate** option. The default **Signing Algorithm** is **RSA (default)** and the default **Certificate Store type** option is **Root CA (default)**. Click the **Browse** button to find the root CA certificate you use in your organization.

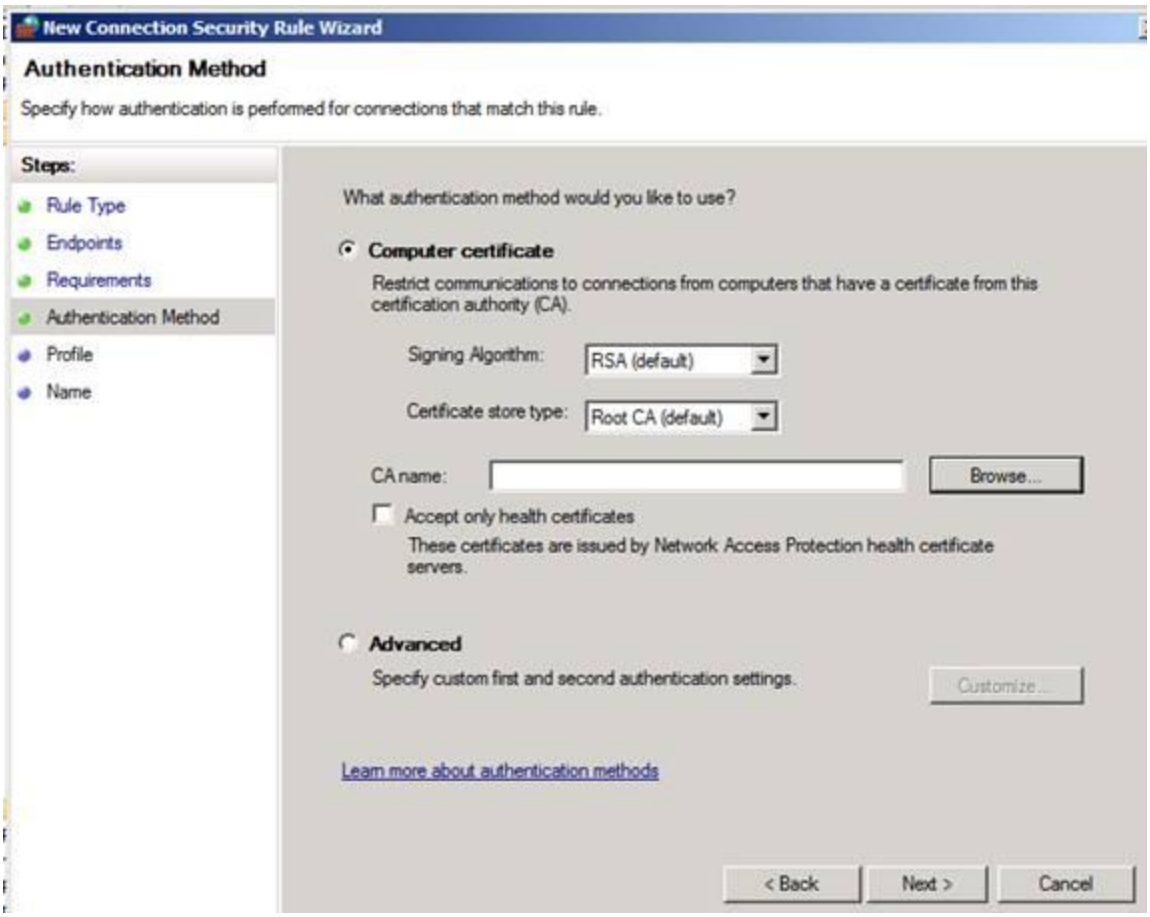


**Figure 10**

In the **Windows Security** dialog box, as shown in Figure 11, you'll see a list of certificates. The root CA for my organization in the lab is **corp-DC1-CA** so I'll select that one and click **OK**.

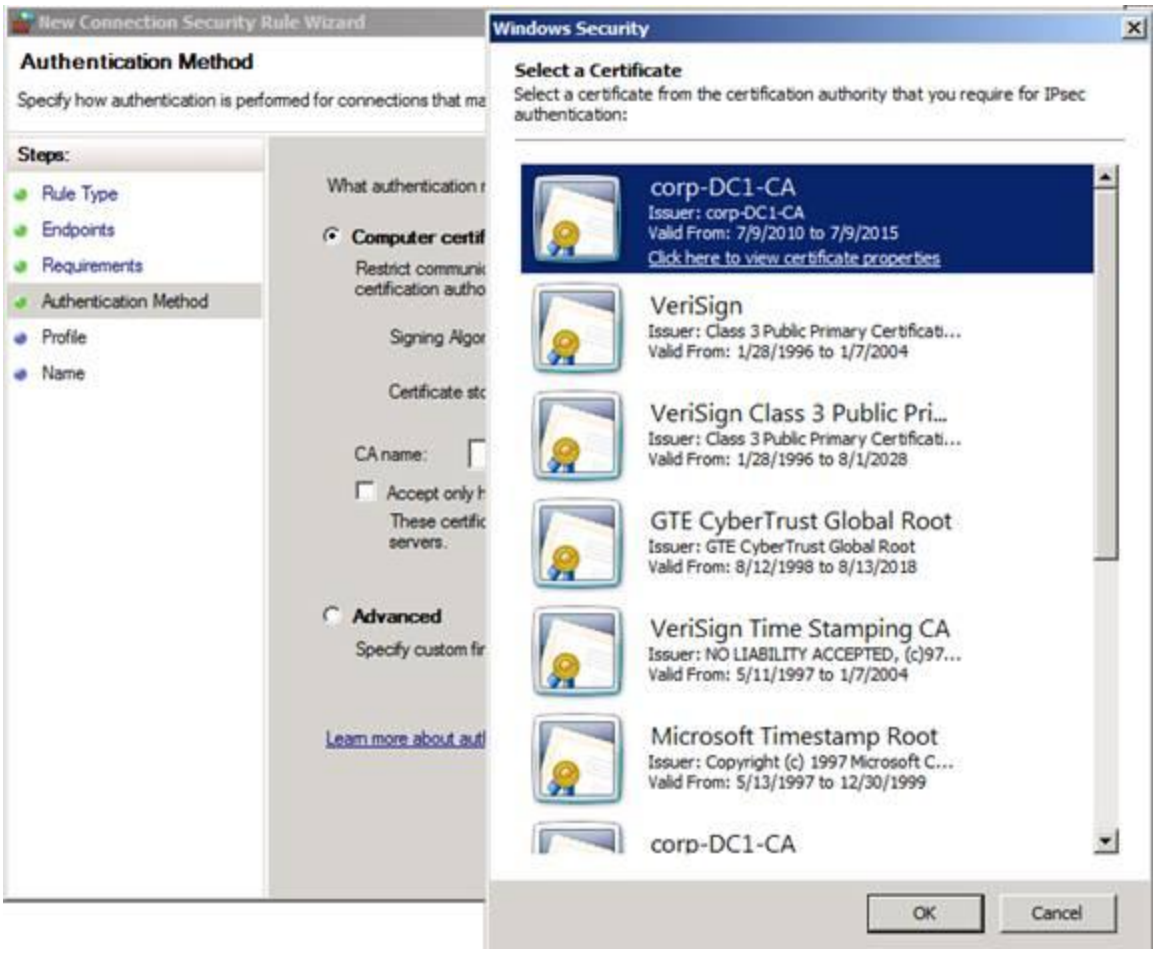


**Figure 11**

Now you can see on the **Authentication Method** page, in Figure 12, that we're using a computer certificate for authentication and that we trust certificates issued by the CA noted in the **CA name** text box. Now we'll click **Next**.

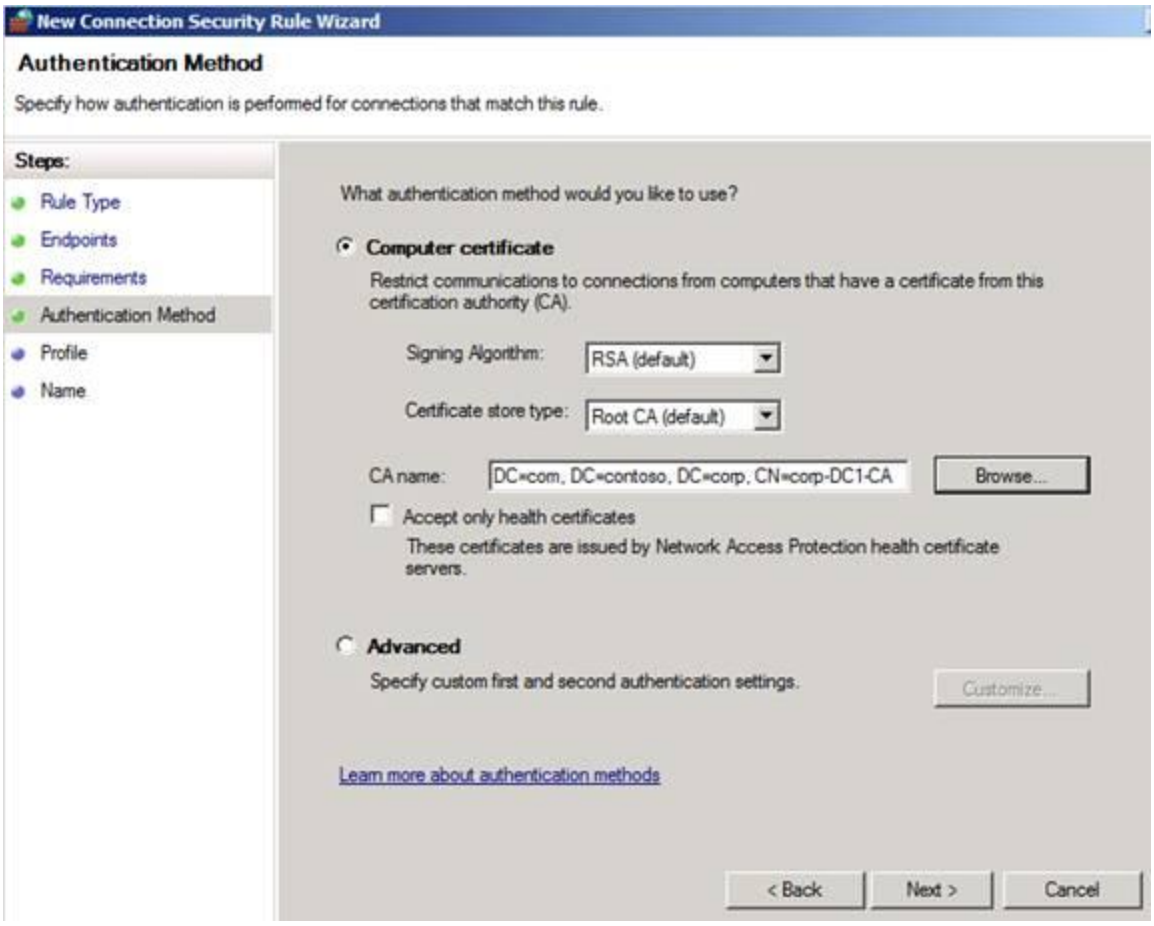


**Figure 12**

On the **Profile** page, shown in Figure 13, we select what WFAS profiles we want to apply to this Connection Security Rule. Since this really only applies to machines that are connected to the domain, we'll use the **Domain** profile only and uncheck the other profiles. This will avoid problems if domain members connect to other networks that use the same private address spaces and the same IP addresses.

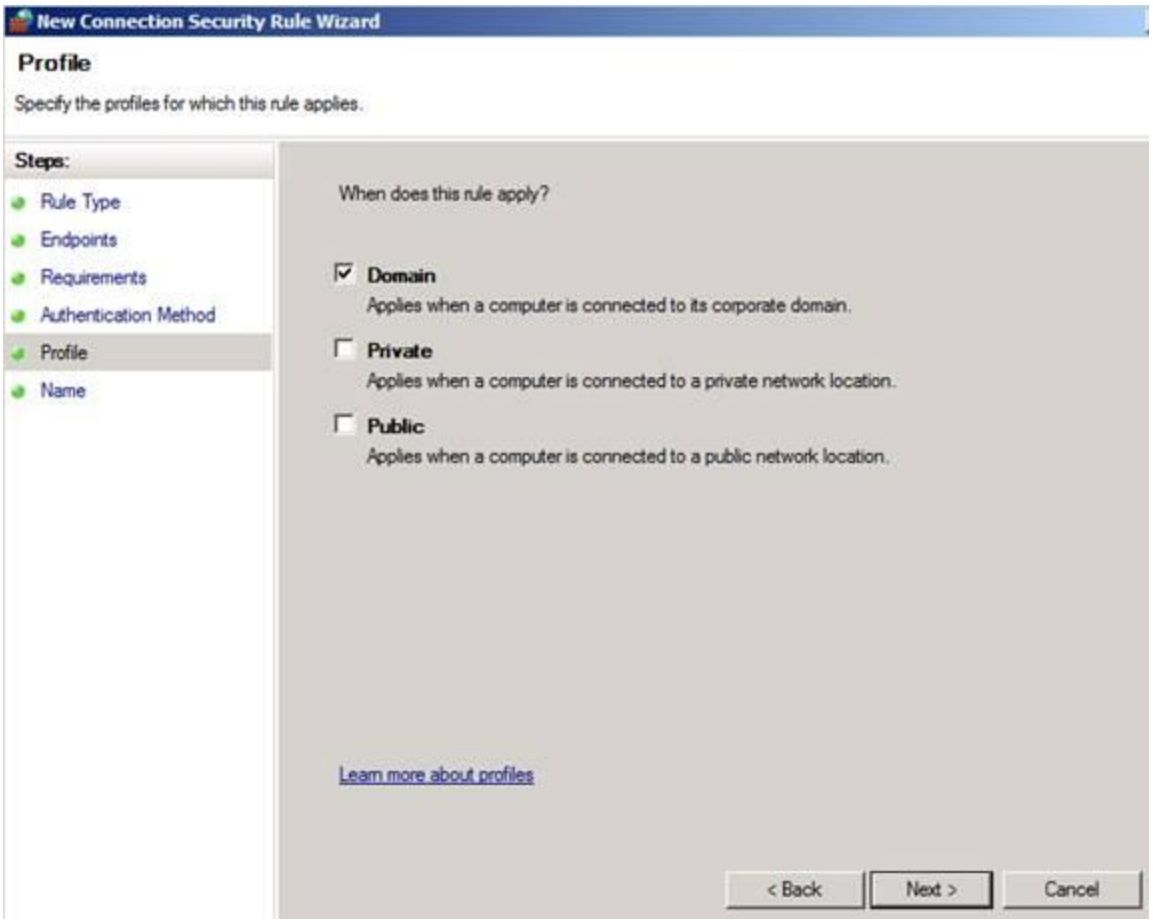


**Figure 13**

On the **Name** page, shown in Figure 14, enter a name for the rule and click **Finish**.


**Figure 14**

The rule shown in Figure 15 is now created in Group Policy and will be automatically deployed to domain members. If you double click on the rule in the Group Policy editor, you can see the dialog box for the rule where you can make changes. Just click on the appropriate tab and make the changes here and the rule will be updated for all the machines to which this Group Policy is applied.

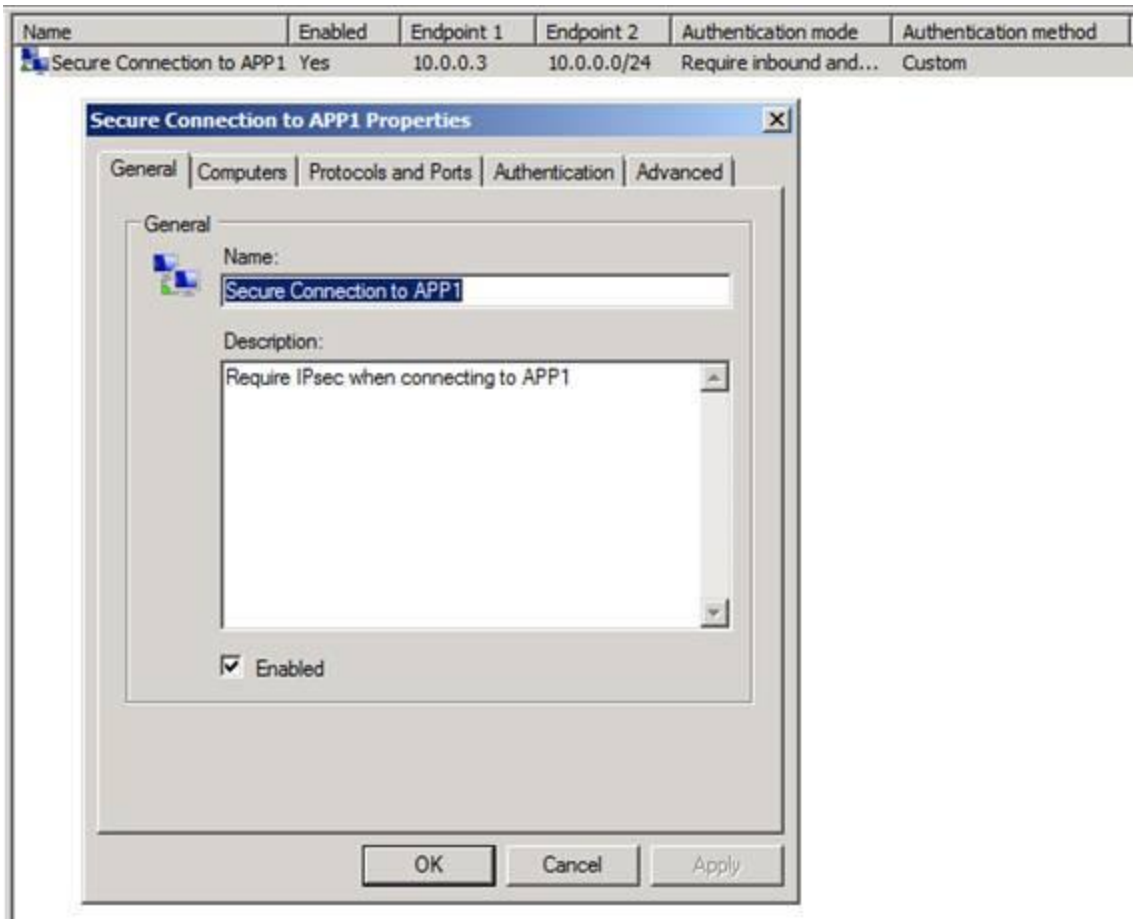


**Figure 15**

You might have noticed that there were no options for configuring the IPsec settings in the rule. The reason for that is that IPsec settings are set on a global basis, which is unfortunate, but that's how Microsoft decided to do that. If you want to see the IPsec settings, you need to right click on the **Windows Firewall with Advanced Security** node as seen in Figure 16 below, and then click **Properties**.

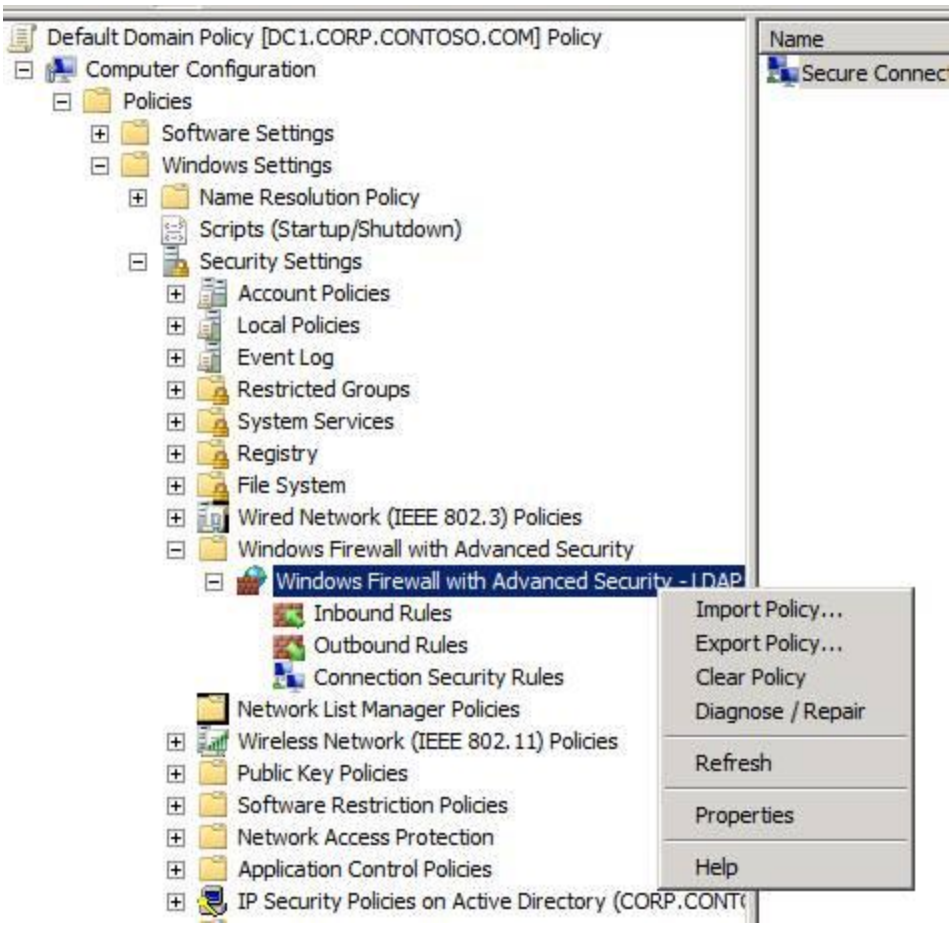


**Figure 16**

This brings up the **Windows Firewall with Advanced Security** dialog box that's shown in Figure 17. If you click the **IP Settings** tab on that dialog box, you can see the **IPsec defaults** section. Also notice that there are sections for **IPsec exemptions** and **IPsec tunnel authorization**. If we click the **Customize** button in the **IPsec defaults** section, you can see that the **Key exchange (Main Mode)**, **Data protection (Quick Mode)**, and **Authentication method** options are all set to **Default**.

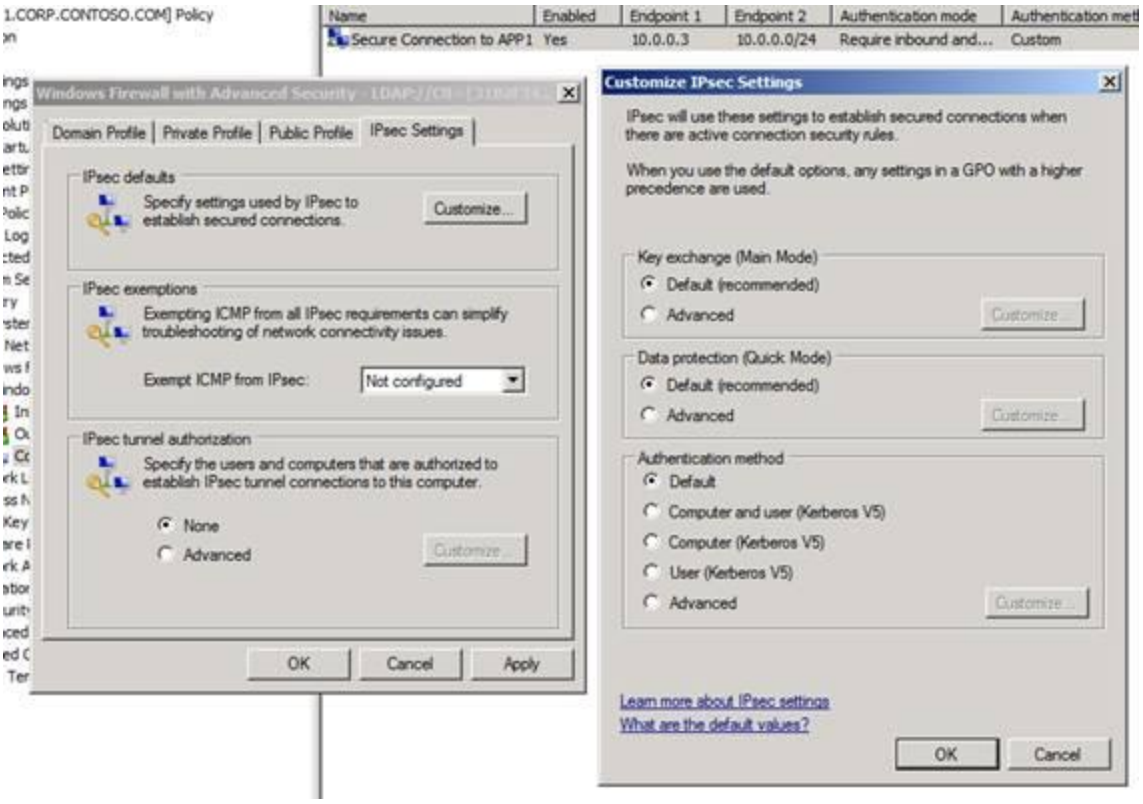


**Figure 17**

The tables below show the default IPsec settings:

**Key exchange**

| Settings | Value |
|---|---|
| Key lifetimes | 480 minutes/0 sessions* |
| Key exchange algorithm | Diffie-Hellman Group 2 |
| Security methods (integrity) | SHA1 |
| Security methods (encryption) | AES-128 (primary)/3-DES (secondary) |

*A session limit of zero (0) causes rekeys to be determined only by the **Key lifetime (minutes)** setting.

**Data integrity**

| Setting | Value |
|---|---|
| Protocol | ESP (primary)/AH (secondary) |
| Data integrity | SHA1 |
| Key lifetimes | 60 minutes/100,000 kilobytes (KB) |

**Data encryption**

| Setting | Value |
|---|---|
| Protocol | ESP |
| Data integrity | SHA1 |
| Data encryption | AES-128 (primary)/3-DES (secondary) |
| Key lifetimes | 60 minutes/100,000 KB |

# Authentication method

Computer Kerberos version 5 authentication is the default authentication method.

When we go to one of the domain computers that will connect to APP1 and open the WFAS console, you can see in the **Connection Security Rules** node the new Connection Security Rule, as shown in Figure 18. Note that this is just a listing of the rule; it doesn't indicate that the rule was active. It just indicates that the rule is available on the computer.

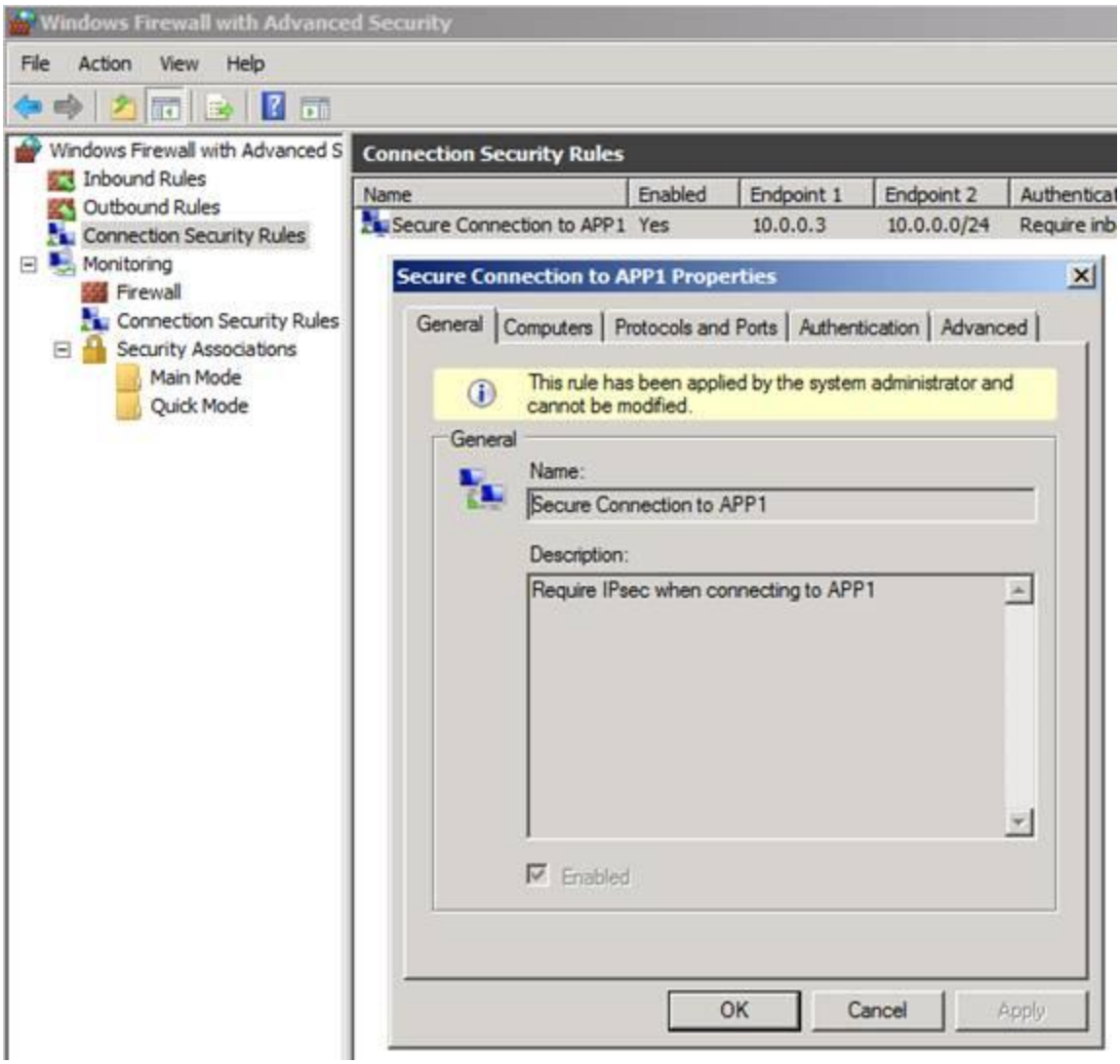


**Figure 18**

If you click on the **Monitoring\Connections Security Rules** node, you can see any active Connection Security Rules. In this case, we can see that there is an active Connection Security Rule, indicating that our IPsec connection worked! When we double click on the active rule, we can see the details of the connection, as seen in Figure 19 below.

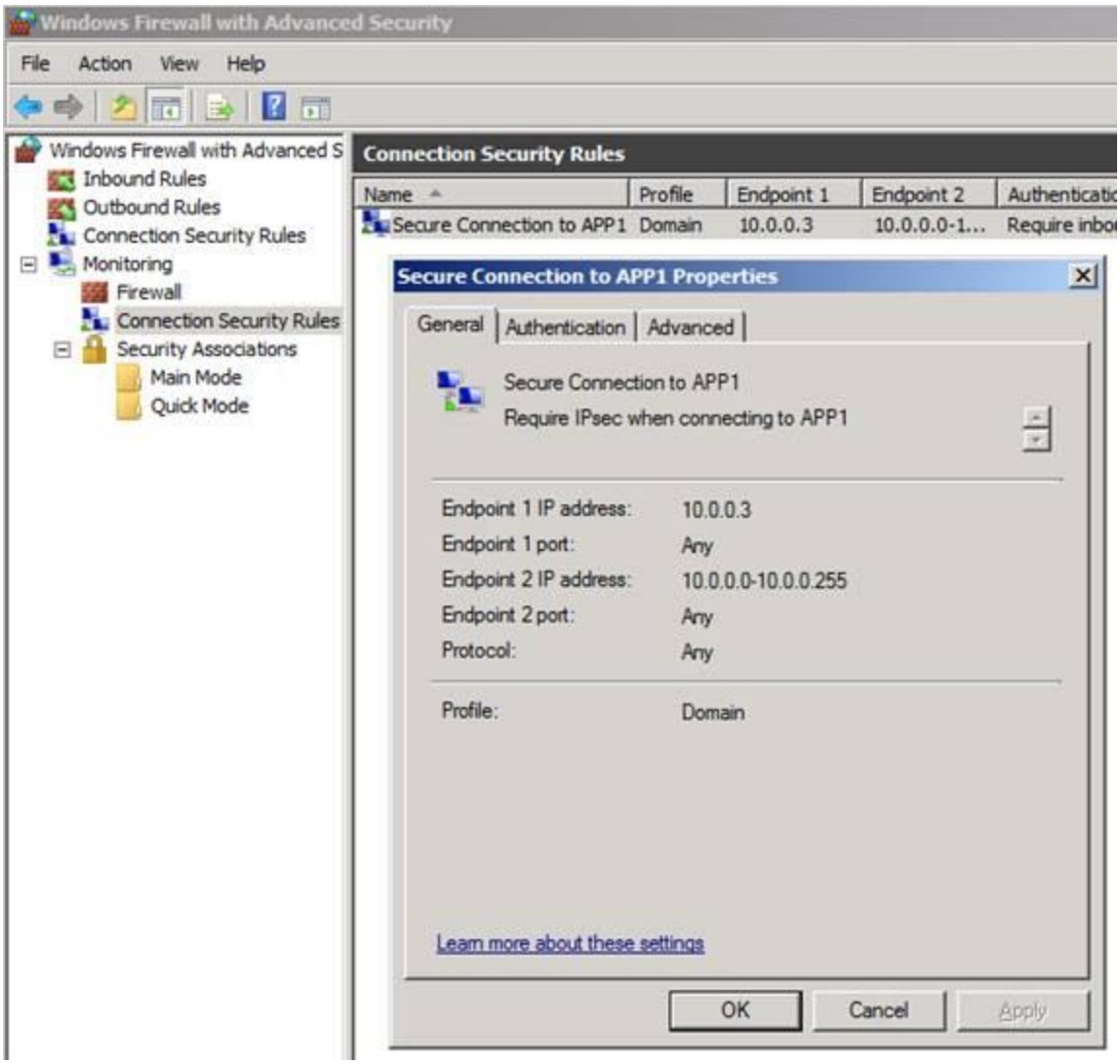


**Figure 19**

Now we'll move to the **Monitoring\Security Associations\Main Mode** section in the left pane of the WFAS console. Here we see information about the **Main Mode** connection, including information about the authentication method, and information about the encryption and integrity algorithms, as seen in Figure 20. If you compare this information with the tables above, you'll see that they match the default settings as described in those tables.

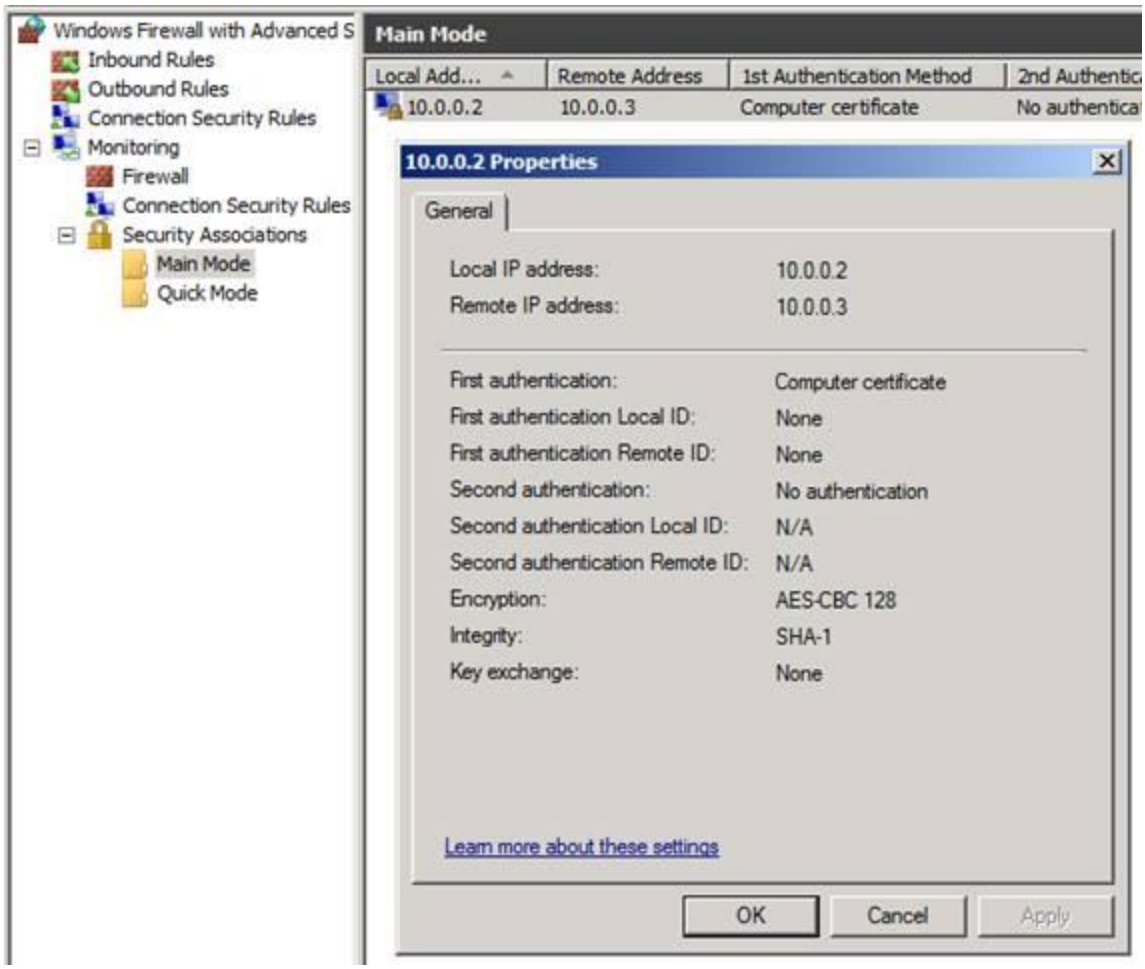


**Figure 20**

Similarly, you can see detailed information about the Quick Mode connection when you click on the **Quick Mode** node in the left pane of the console, as shown in Figure 21.

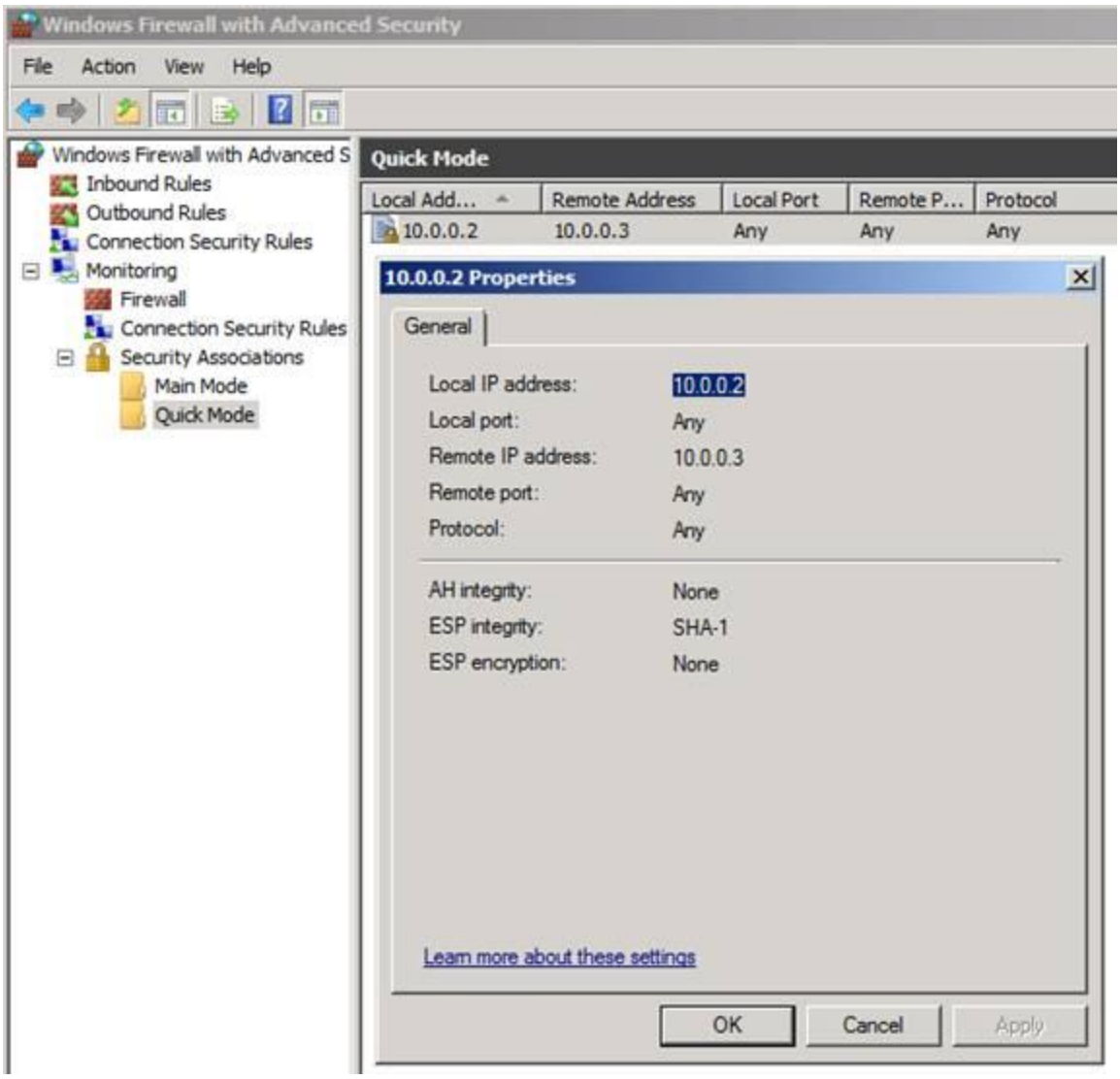


**Figure 21**

n this article, we went over some of the basics of the new IPsec Connection Security Rules wizard and showed how easy it is to get the Connection Security Rules working. In the next article in this series, I'll show you how you can create IPsec tunnel rules and how to configure a Windows Server 2008 R2 machine as an IPsec gateway – something you might find interesting when thinking about how to create secure segments on your network or as an interesting remote access solution