Create a Site-to-site VPN on ISA 2006 (Part 7)

In the previous article we also looked at the impact of RPC communications over the ISA Firewall. In this article there are a few other points with more difficult questions to answer. Hope, after analyzing and 'bringing the problem to light', uncle

Create a Site-to-site VPN on ISA 2006 (Part 1)
Create a Site-to-site VPN on ISA 2006 (Part 2)
Create a Site-to-site VPN on ISA 2006 (Part 3)
Create a Site-to-site VPN on ISA 2006 (Part 4)
Create a Site-to-site VPN on ISA 2006 (Part 5)
Create a Site-to-site VPN on ISA 2006 (Part 6)

Some effects of RPC communication over the ISA Firewall.

In the previous lesson, we have Enterprise Policies, which allow us to put the Domain Controller into the branch office. We have also learned how to configure automatic firewalls, particularly useful when deploying large-scale ISA Firewall arrays.

After the first 6 parts, they have now successfully created and launched the Site-to-Site VPN operation, and are ready to deploy the branch office Domain Controller at the branch office. Next, install Active Directory that integrates DNS server on DC and configure the branch office ISA Firewall to use DNS server as a primary DNS server. This will help eliminate dependencies on the Site-to-Site VPN connection, increasing the high availability of DNS services.

In the previous article we also looked at the impact of RPC communications over the ISA Firewall. In this article there are a few other points with more difficult questions to answer. Hopefully, after analyzing and 'bringing the problem to light', we can exploit more knowledge and experience from the ISA Firewall community through their answers.

Strict removal of Strict RPC-compliance on internal communications rules

A common problem that occurs since communications are done through the ISA Firewall is that the autoenrollment function does not work correctly. Another problem that is also closely related to it is that the MMC snap-in certificates do not work. Previously, there was a article in the Microsoft Basic Guide that indicated that if we removed strict RPC compliance on the Access Rule, these two functions would work normally.

We need an automatic revocation certificate because it relates to an enterprise CA that installs on the main office's Domain Controller. Enterprise CA allows you to set the CA certificate automatically in the Trusted Root Certificate Authorities machine certificate store of all domain members. It is very convenient, because all

domain members will automatically trust all certificates issued by our PKI enterprise.

Follow these steps to remove Strictly RPC-compliant on the Internal Access Rule Rule:

1. In the ISA Firewall console, expand the **Enterprise** node, then the **Enterprise Policies** node. Select the **Branch Policy** button and right-click **Branch DCs** > **Main DC** Access Rule, click the **Configure RPC protocol button** .

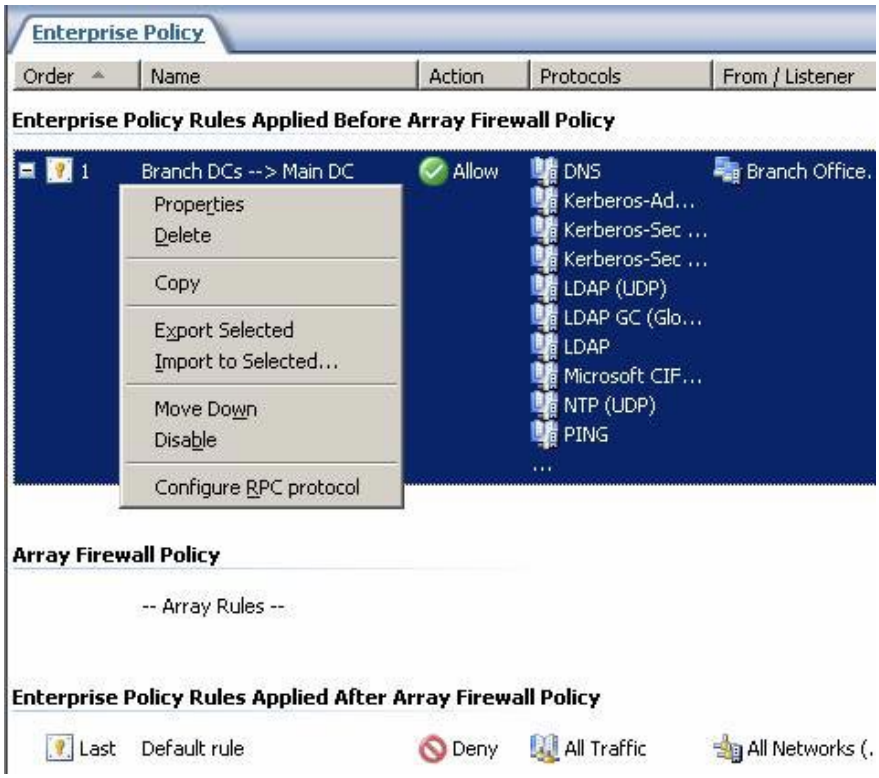


Figure 1

2. In the **Configure RPC protocol policy** dialog box, uncheck the **Enforce strict RPC compliance check box** . Click **OK** .

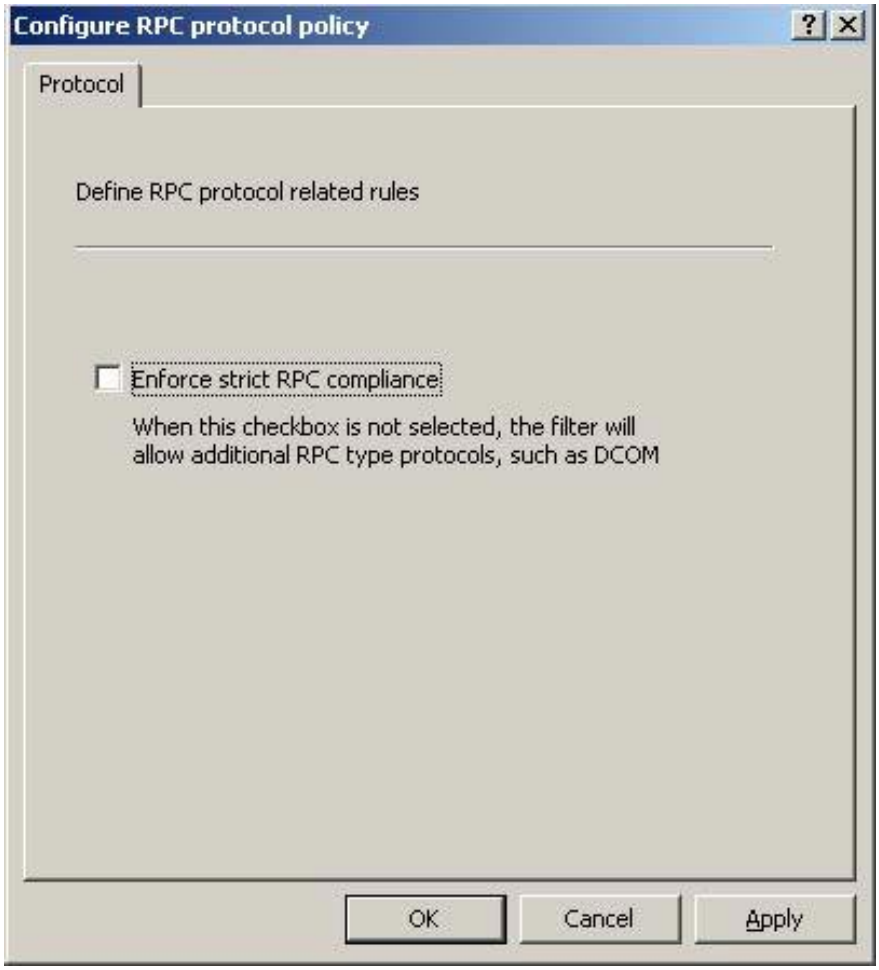


Figure 2

3. Click **Apply** to record the changes and update the firewall policy. Click OK in the **Apply New Configuration** dialog box.

Many people ask whether we should enable Strict RPC compliance after installing the branch office DC. In fact, there is no satisfactory answer to this problem yet, because the exact details of the setup are not publicly available. To check, you can assume that it will be more secure when strict RPC compliance is enabled. But does this security component break down some essential basic functions? After all, the best option for us is to remove this component.

However, the final decision is up to you. If you don't need autoenrollment, you can use strict RPC compliance.

But notice that there is no such thing as the correct answer or the wrong answer here. Just a choice of which security situation is best suited to your situation.

Run CDPromo on the branch office Domain Controller

Now we are ready to install the Domain Controller at the branch office. How this works depends on your environment. Many companies create a test environment with a rebuilt IP address scheme similar to the branch office's. Then install, configure DC in the main office first, then attach to the following branch office. Some other companies installed DC machines in the branch office, then sent their headquarters IT specialist to install

the DC.

Each of these methods has its own advantages and disadvantages. I personally prefer to send IT professionals to the branch office. Because DC deployment is an extremely important issue, it is often best to have someone know how to handle potential problems that arise directly at the deployment site.

Perform the following steps to install DC on the branch office Domain Controller:

1. **Go to Start** > **Run** > enter **dcpromo** in the **Open** box. Click **OK** .
2. Click **Next on** the **Welcome to the Active Directory Installation Wizard page** .
3. Read the information on the **Operating System Compatibility** page and click **Next** .
4. On the **Domain Controller Type** page, select the option **Additional domain controller for an existing domain** and click Next.

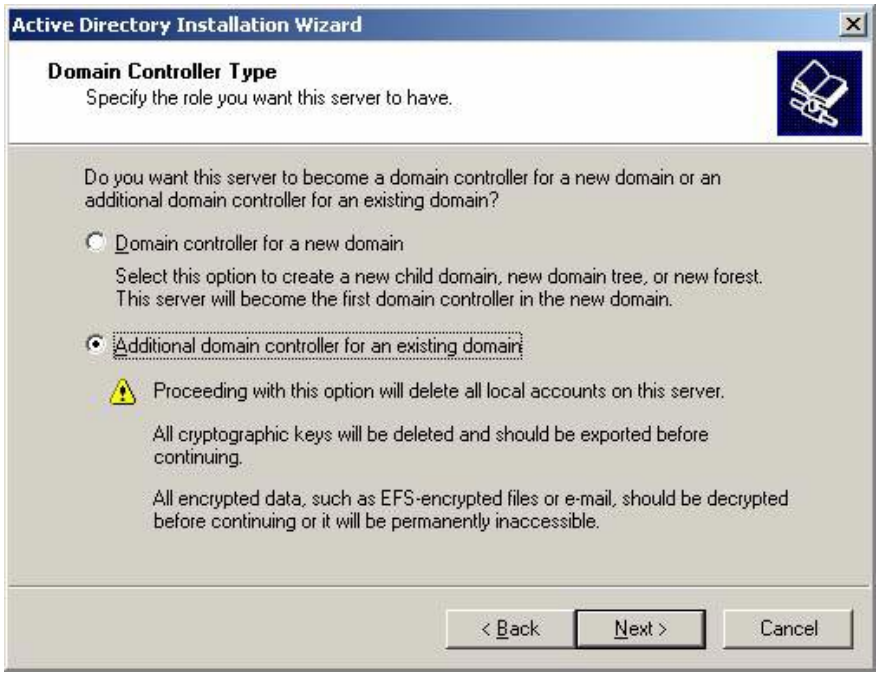


Figure 3

5. On the **Network Credentials** page, enter the credentials of users who have the right to install new Domain Controllers. Click **Next** .

Figure 4

6. On the **Additional Domain Controller** page, click the **Browse** button and click the domain name of the main office. In this example, the domain name is **msfirewall.org** . Enter the domain name in the list in the **Browse for Domain** dialog box. Click **OK** and click **Next** to continue.

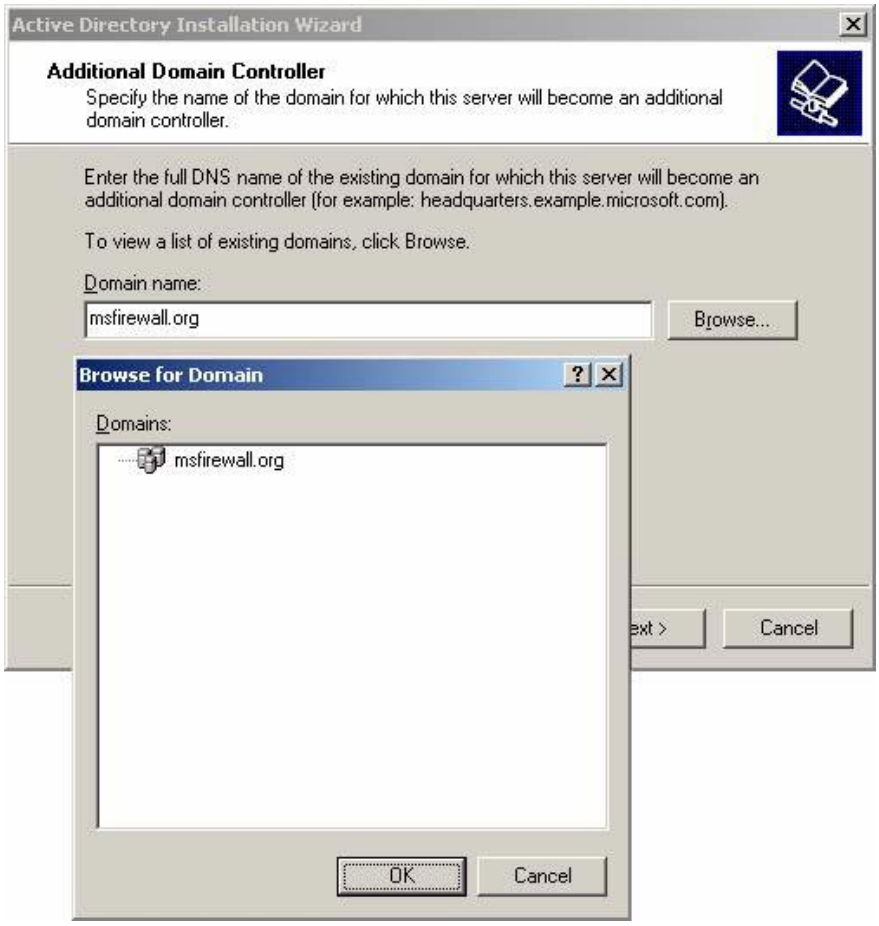


Figure 5

7. On the **Database and Log Folders page** , accept the default settings and click **Next** .
8. On the **Shared System Volume** page, accept the default area and click **Next** .
9. Enter the password and verify the password on the **Directory Services Restore Mode Administrator Password page** and click **Next** .
10. Click **Next** on the **Summary** page, click **Next** .
11. The **Installation Wizard** starts. Leave it until you see the completion page appear.

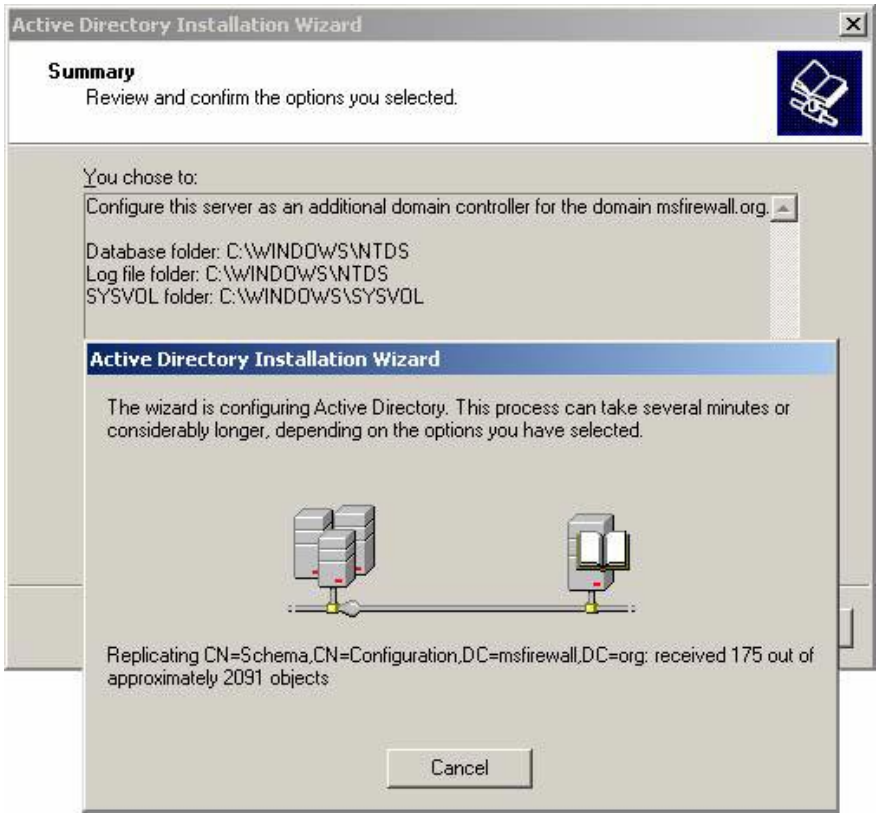


Figure 6

12. Click **Finish** on the **Completing the Active Directory Installation Wizard page** .

Figure 7

13. Click the **Restart Now** button in the **Active Directory Installation Wizard** dialog box.

The Dcpromo program works quite well. No errors occurred during installation. After restarting the machine, all components appear and operate stably. If you open the **Certificates** MMC, you will see the enterprise CA certificate automatically brought to the **Trusted Root Certification Authorities** certificate store as we want. You can see in the illustration below.

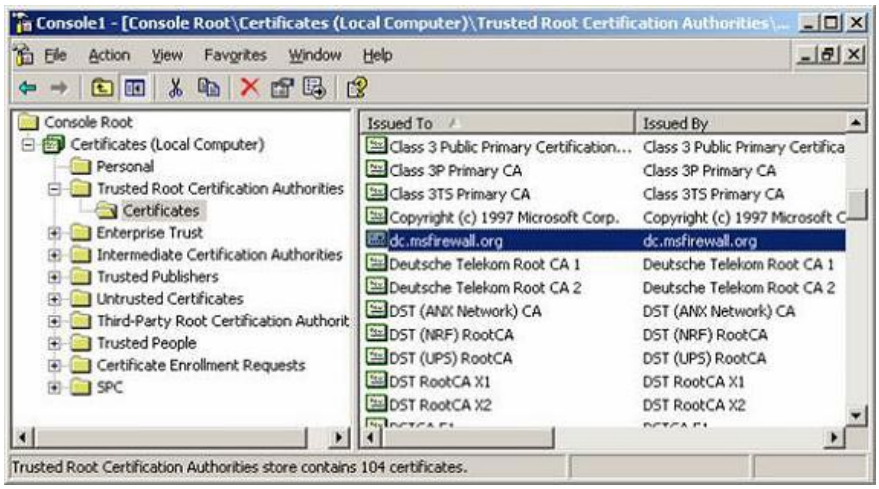


Figure 8

However, if you open the Event Viewer, you will see some errors with real problems appearing. The figure below shows that the autoenrollment function does not work and the branch office Domain Controller does not receive a DC certificate. Is that a real error, a real problem, a problem related to the ISA Firewall?

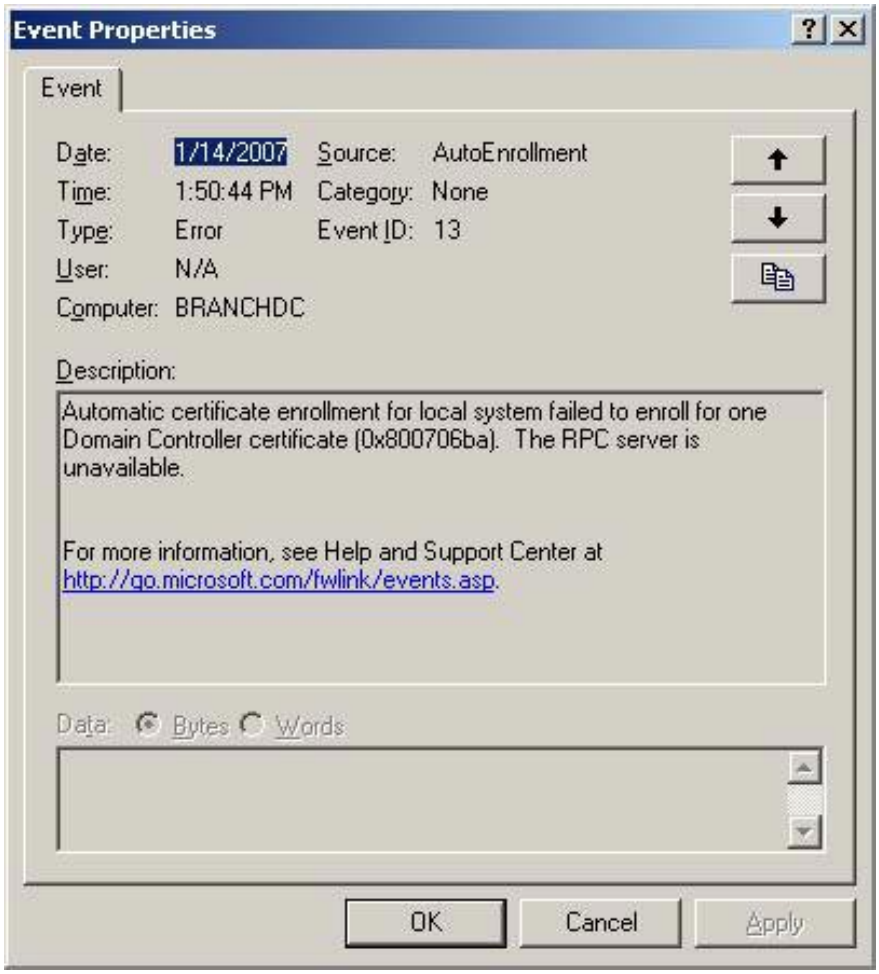


Figure 9

The figure below shows another error, probably significant. This error indicates that the branch office Domain Controller cannot query the list of policy object groups. Sounds like a big problem, but is that really the case, is it a problem with the ISA Firewall or other problem?

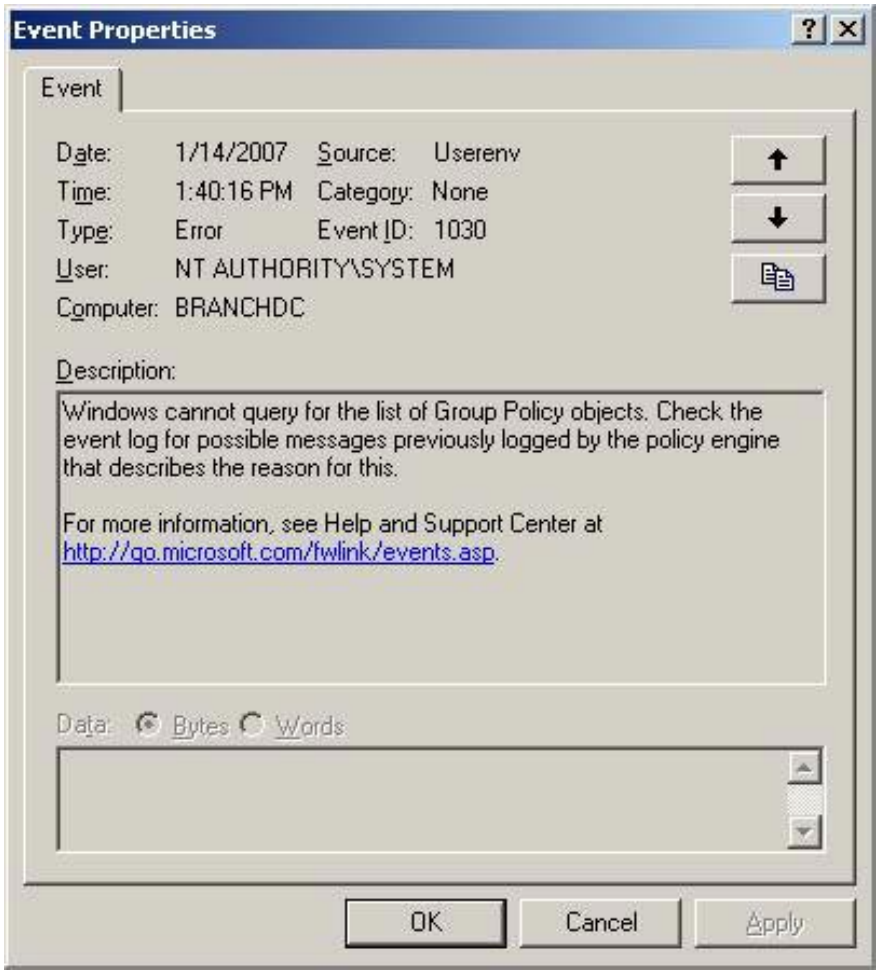


Figure 10

The figure below shows the DCOM error that could not contact the Domain Controller at the main office (Domain Controller.msfriewall.org). Is this an error related to the ISA Firewall? Or what else?

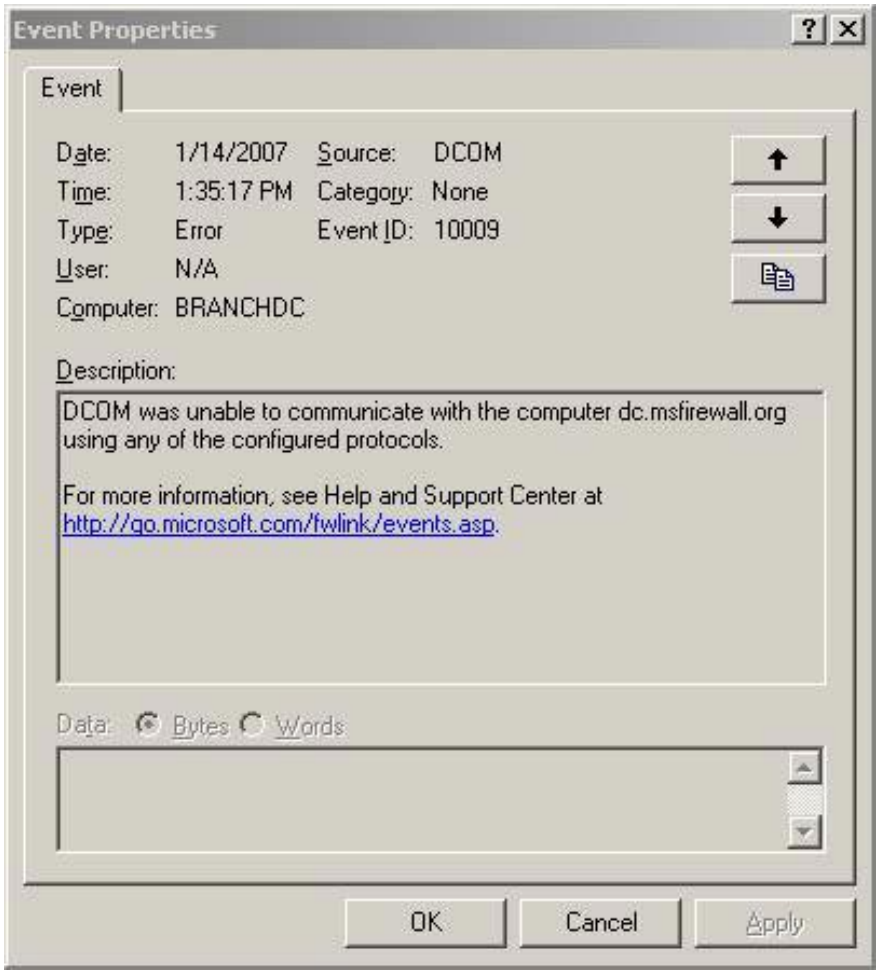


Figure 11

Are these errors real? Are they created during startup before the Site-to-Site VPN is activated? Verifying this is not correct.

Are you sure the auto-recovery function does not work? We saw that the CA certificate is automatically included in the Trusted Root Certification Authorities certificate store. Should I automatically assign a DC certificate? Or do we need to create a policy for this?

Are you sure Group Policy is actually executing your process?

To test, make a small change to Domain Group Policy at the main office Domain Controller. For example, go to the **Desktop** button in **Administrative Templates** at **User Configuration** , as shown below.

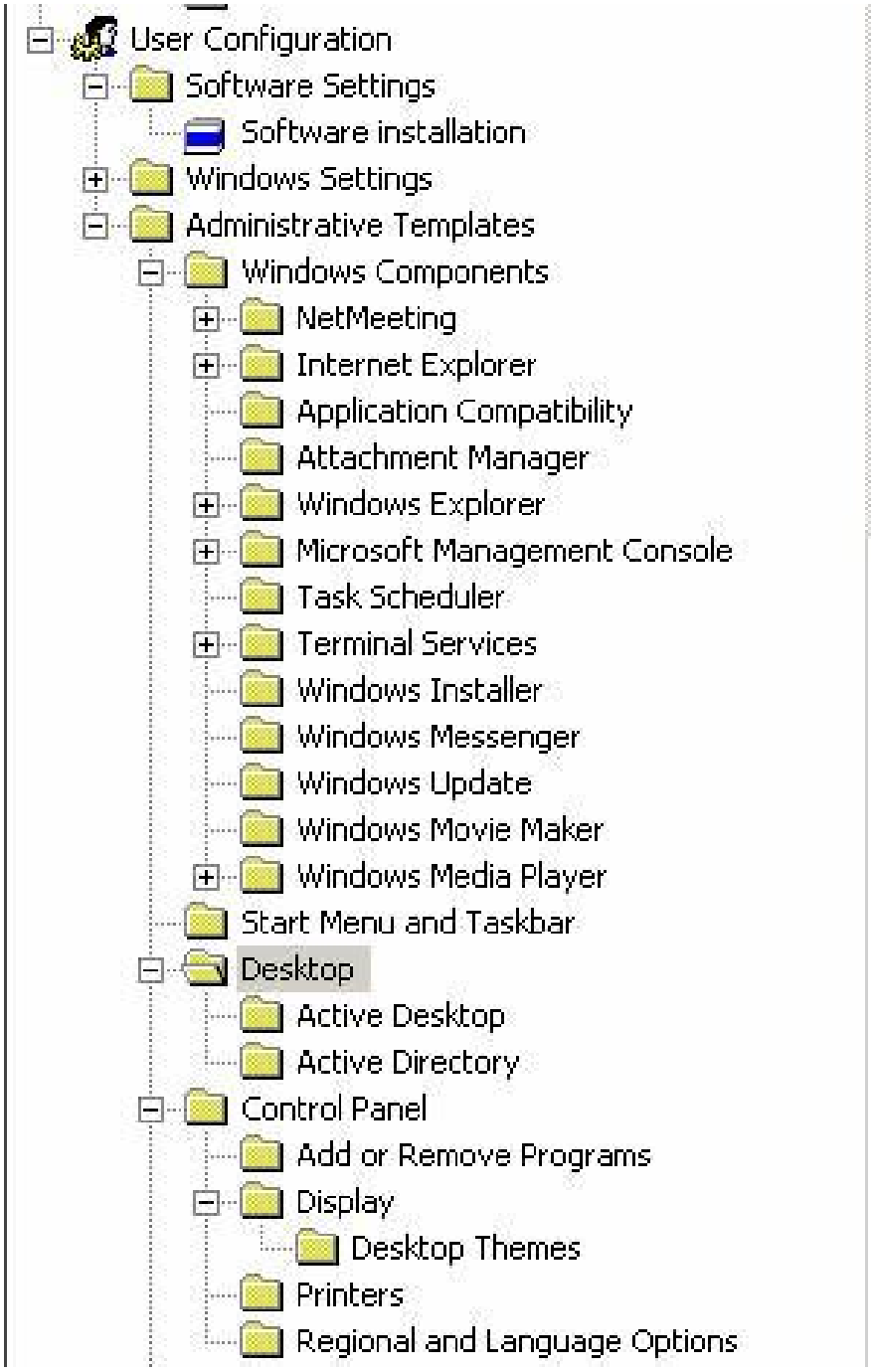


Figure 12

Next, double-click **Remove Recycle Bin icon from desktop** in the right pane and click the **Enable** area. Click **OK** and then run **gpupdate / force** on the main office Domain Controller. Once completed, run the **gpupdate / force** command at the branch office. What happened?

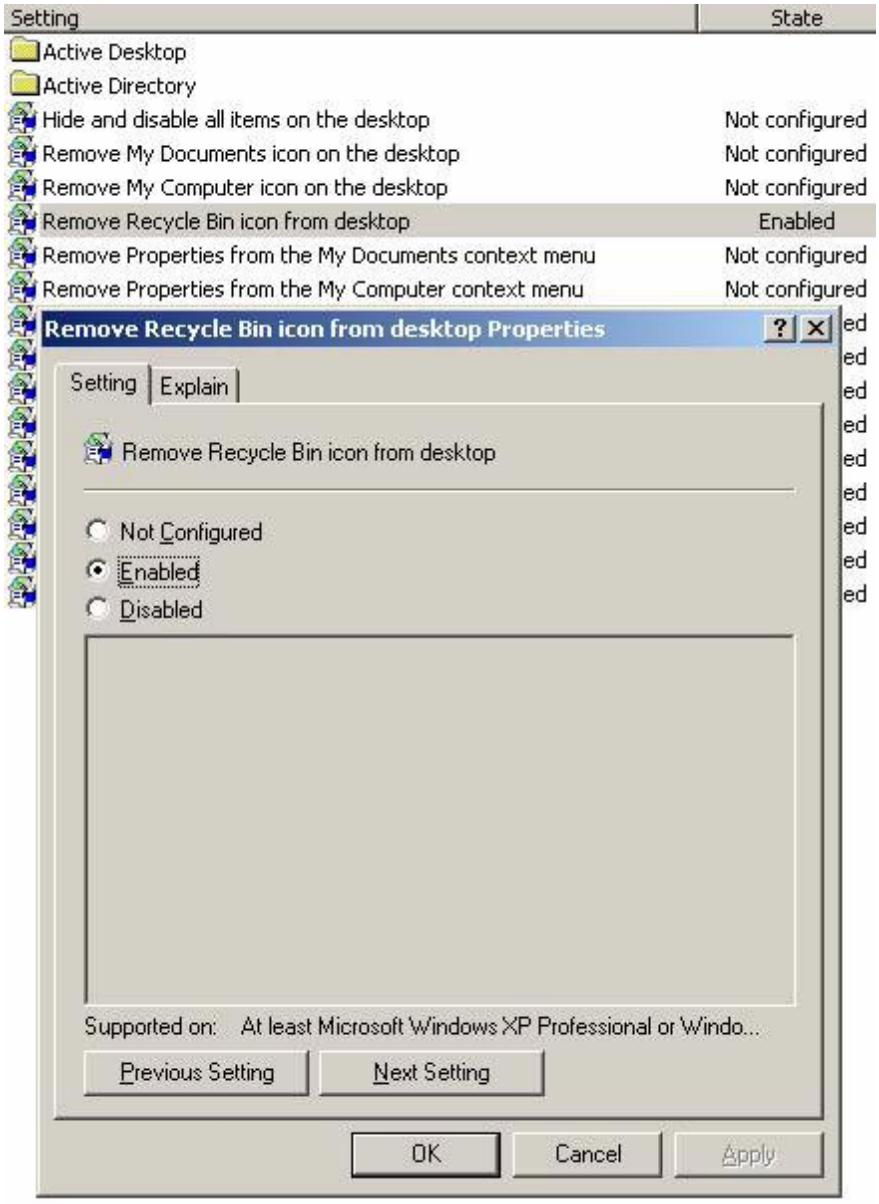


Figure 13

You can see, Group Policy is applied in both branch offices and headquarters. The Recycle Bin object is removed on the desktop (you may have to refresh the desktop to see this change). Therefore, it is not always possible to trust what is seen in Event Viewer.

What about the **Certificates** MMC? Unfortunately, the Certificates MMC doesn't work. However, it is possible that we do not configure the ISA Firewall to meet some specific details. Here are some notable reference guides:

'To request a certificate for the ISA Server computer, clear the **Enforce strict RPC compliance check** box in the **System Policy Editor** dialog box. To request a certificate for the client computer when the Certification Authority is *on another network* , you do not have to correct the system policy on the ISA Firewall machine. In this case, you need to change strict RPC-compliance rule settings or rules that allow traffic to be converted between the two networks. To do this, follow these steps:

1. Start the ISA Server Management function.
2. Expand the ***ServerName*** button, click **Firewall Policy** .
3. Right-click the rule that allows traffic to be performed between the network with the Certification Authority mode and the client computer network on it.
4. Click the **Configure RPC Protocol button** .
5. Remove the **Enforce strict RPC compliance check box** and click **OK** .
6. *Repeat steps 3 through 5 to change system policy rules and allow DCOM communications between any two different rules that fall within two specific networks.*
7. After changing the policy rules (policy), click **Apply** .

Notice step 6. What will System Policy look like with *any two different rules that fall into two specific networks* ? What does this mean? Does it mean that System Policy rules apply to communications between two ISA Firewall Network networks? How can this happen? System Policy only controls traffic that is either from or from the ISA Firewall, or is directed to the ISA Firewall. Why can the System Policy Rule control traffic *between two networks* ?

Is this a small secret for the ISA development team? To check, let's see what happens if we stop using strict RPC compliance at the System Policy level. The only way to do this is to open the System Policy editor for the array level.

Click on the **Firewall Policy** in the left pane of the ISA Firewall console and select the **Tasks** tab on the Task Pane. In the Task Pane, click the **Edit System Policy link** . Click on Group Policy **Authentication Services** in the right pane and uncheck the **Enforce strict RPC compliance check box** . Click **OK** . Perform this operation on both ISA Firewalls.

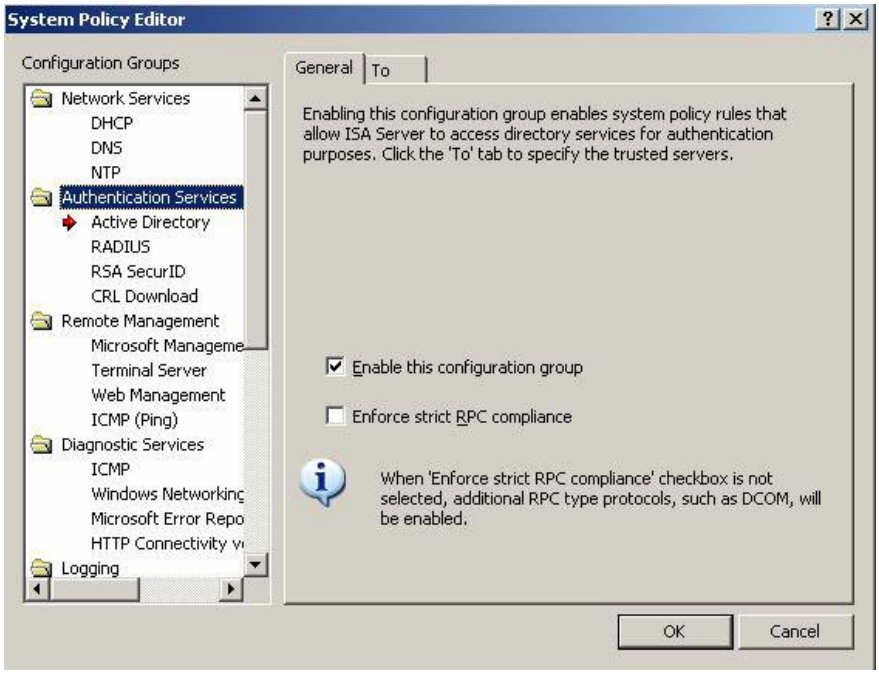
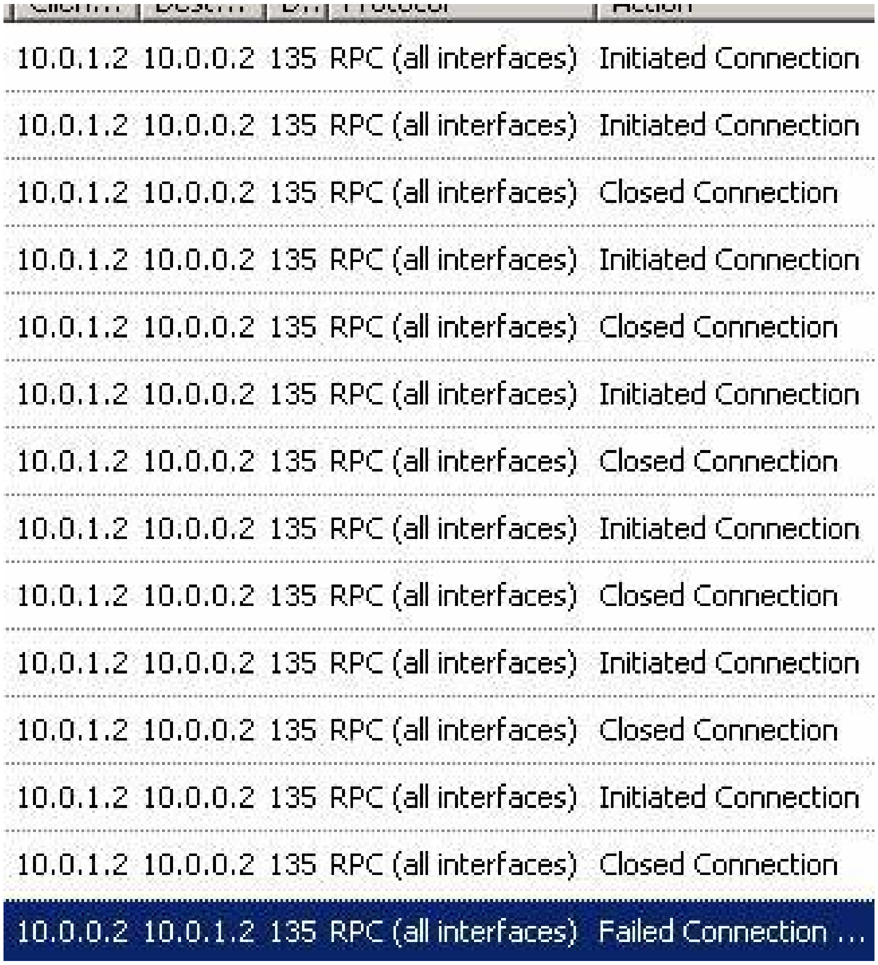


Figure 14

To test, restart both ISA Firewalls, review the RPC state table to make sure entries are removed. I don't know if this is necessary, but it is the most reliable way to make sure the tables are cleared. Restart the branch office Domain Controller, but the **Certificates** MMC fails with the enterprise CA. You will see an error like the one below:

Figure 15

Both reasons given in the error message are incorrect. The CA is active online and the user account logged in is enterprise administrator. Some of the real reasons are:



10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Initiated Connection
10.0.1.2	10.0.0.2	135	RPC (all interfaces)	Closed Connection
10.0.0.2	10.0.1.2	135	RPC (all interfaces)	Failed Connection ...

Figure 16

This log file entry information is recorded when the certificate request is sent from the branch office Domain Controller to the main office Domain Controller, also an enterprise CA.

Summary

In this article we have reviewed some of the activities that took place after installing the domain controller at the branch office. Unfortunately, the number of questions is more than the answers received. Some instructions from Microsoft suggest that all problems encountered here should be resolved by strict strict RPC compliance, but we still see some communication related RPC errors that appear in Event Viewer. Should all the event messages be trusted in Event Viewer? This event viewer reports that Group Policy process is not active, but actually Group Policy has been applied. What about automatic recovery mechanism (autoenrollment)? Perhaps we need to create a policy first. Then there is the **Certificates** MMC.

There are now more questions than answers. But it can be said that, for the most part, the Domain Controller is quite stable. We will continue to meet again in the configuration of the Active Directory class for the branch office and configure the link layer. We will also create the DNS server on the branch office DC and change the DNS settings on the ISA Firewall in the next article.

(*Also*)