

Deploying Network Access Quarantine Control, Part 2

Jonathan Hassell 2004-08-30

In the [last article](#), I stepped through how the process of network access quarantine control (NAQC) works and offered detailed deployment instructions. In this second and final installment, I'll continue the procedure by finishing the deployment, then discuss how ISA Server 2004's entrance to the marketplace changes the field of NAQC and how quarantining is implemented within ISA Server itself.

Let's start where we left off.

Distributing the Profile to Remote Users

The profile you created in the [previous installment](#) of this article is made into an executable file that can be distributed to your remote users and run on their systems automatically, creating a profile without any additional intervention. There are several options for getting that executable file to your users.

You could transmit the executable file as an attachment to an e-mail message, or better yet, a link to the executable file hosted on a web server somewhere. In the e-mail message, you could include instructions to run the file and use that new connectoid for all future remote access. You could also have the executable run as part of a logon or logoff script, but to do that, you'd need to either have your users log on through a dial-up connection, or wait until the mobile users return to the home network and connect remotely to your corporate campus or network.

Regardless of which method you choose to initially transmit the profile installer to your users, you should always place the latest version of the profile installer on a quarantined resource somewhere, so client computers that don't pass your baseline script's compliancy checks can still surf to the required web site and download the latest version without compromising the integrity of your network further.

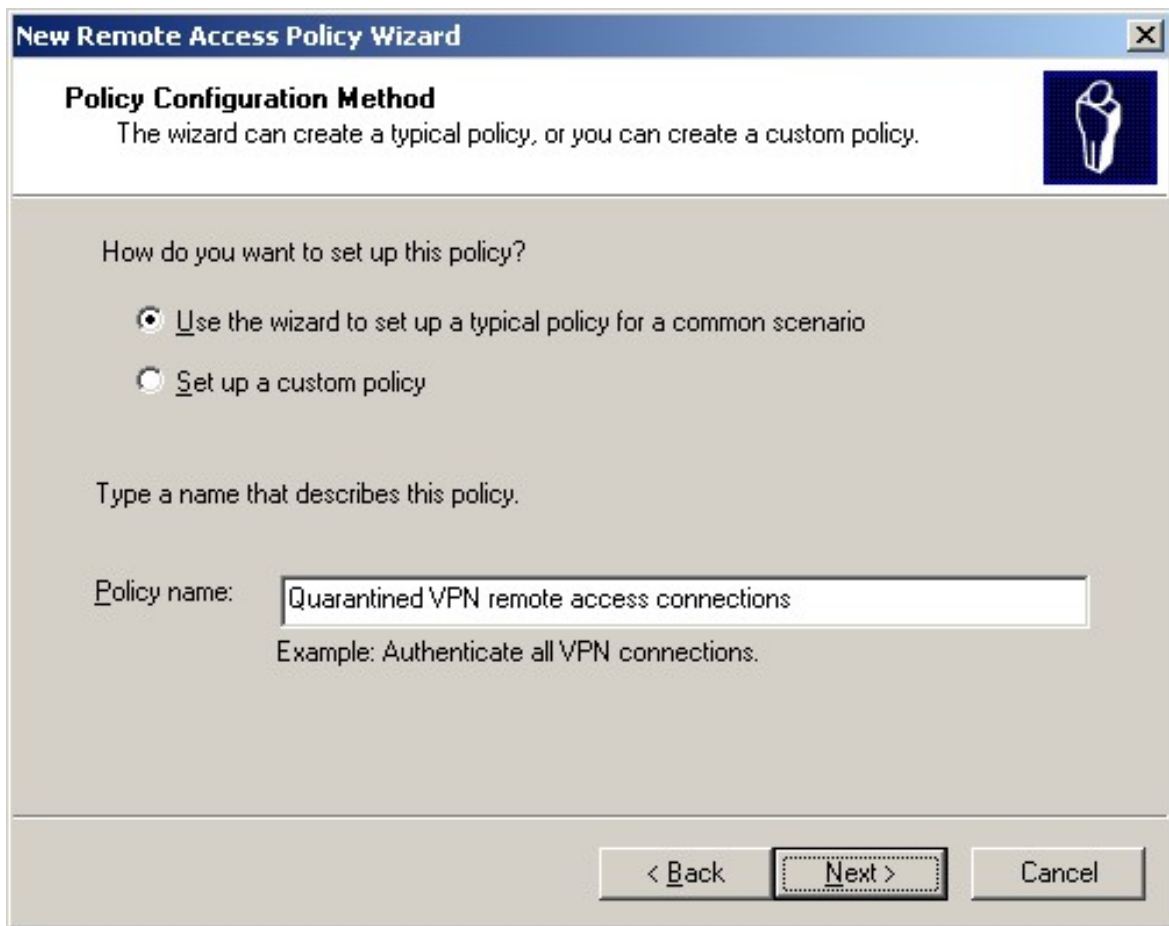
Configuring the Quarantine Policy

The final step in the deployment process is to configure the actual quarantine policy within RRAS. In this section, I'll create a quarantine policy within RRAS that assumes you've posted the profile installer on a web server that is functioning as a quarantined resource.

If RRAS is configured to use the Windows authentication provider, then RRAS uses Active Directory or an NT 4 domain (remember, the RRAS machine needs only to be running Windows Server 2003; it doesn't need to belong to an Active Directory-based domain) to authenticate users and look at their account properties. If RRAS is configured to use RADIUS, then the RADIUS server must be a Server 2003 machine running IAS. Incidentally, IAS also uses Active Directory or an NT domain to authenticate users and look at their account properties.

Configuring RRAS

1. Open the RRAS Manager.
2. In the left-pane, right-click Remote Access Policies, and then select New Remote Access Policy from the context menu. Click Next through the introductory pages.
3. The Policy Configuration Method page appears. Enter Quarantined VPN remote access connections for the name of this policy, as shown in Figure 4. Click Next when you're finished.



New Remote Access Policy Wizard

Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

< Back Next > Cancel

Figure 4: The Policy Configuration Method screen

4. The Access Method page appears. Select VPN, and then click Next.
5. On the User or Group Access page, select Group, and then click Add.
6. Type in the group names that should be allowed to VPN in to your network. If all domain users have this ability, enter Everyone or Authenticated Users. I'll assume there is a group called VPNUsers on this domain that should have access to VPN capabilities. Click OK.
7. You'll be returned to the User or Group Access page, and you'll see the group name you added appear in the list box, as shown in Figure 5. Click Next if it looks accurate.

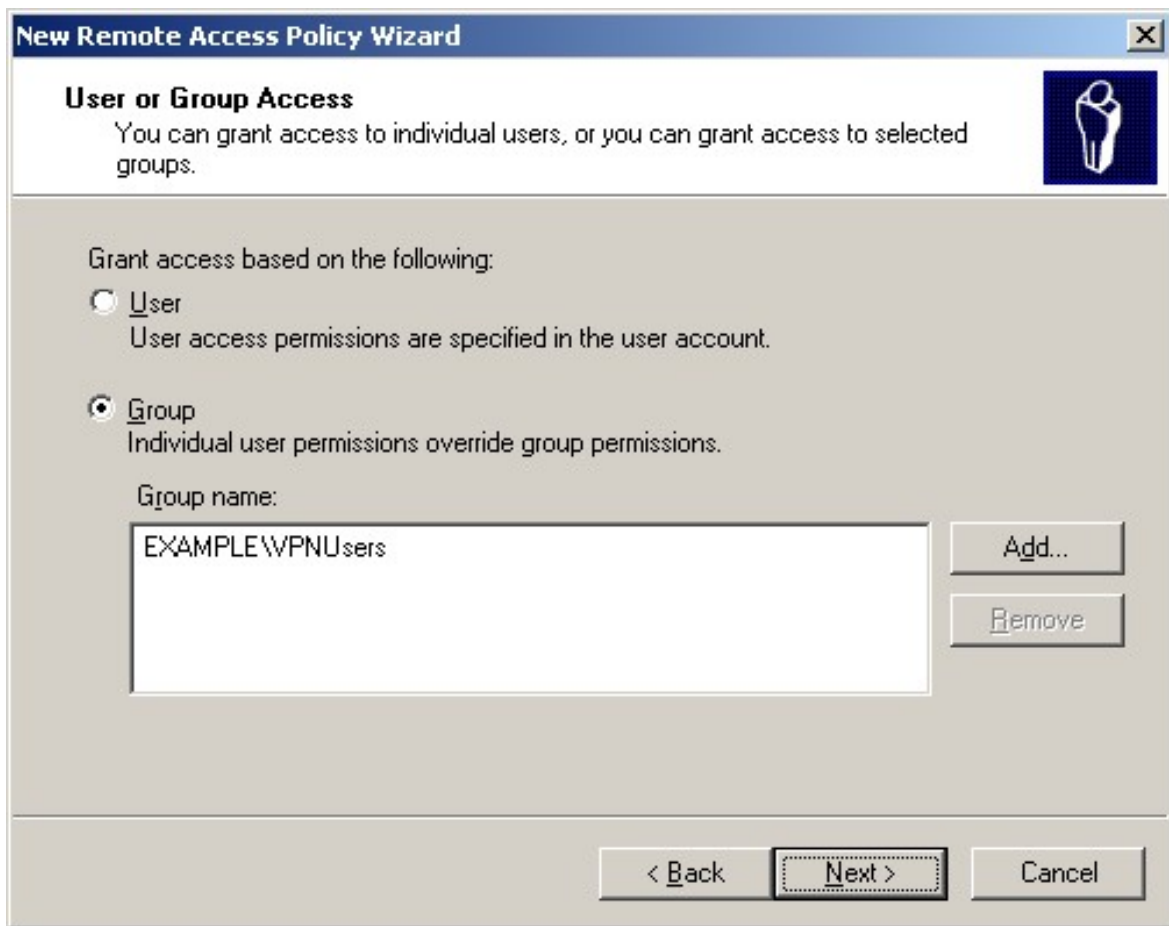


Figure 5: the User or Group Access screen.

8. The Authentication Methods page appears. To keep this example simple, use the MS-CHAP v2 authentication protocol, which is selected by default. Click Next.
9. On the Policy Encryption Level page, make sure the Strongest Encryption setting is the only option checked. This is shown in Figure 6. Then, click Next.

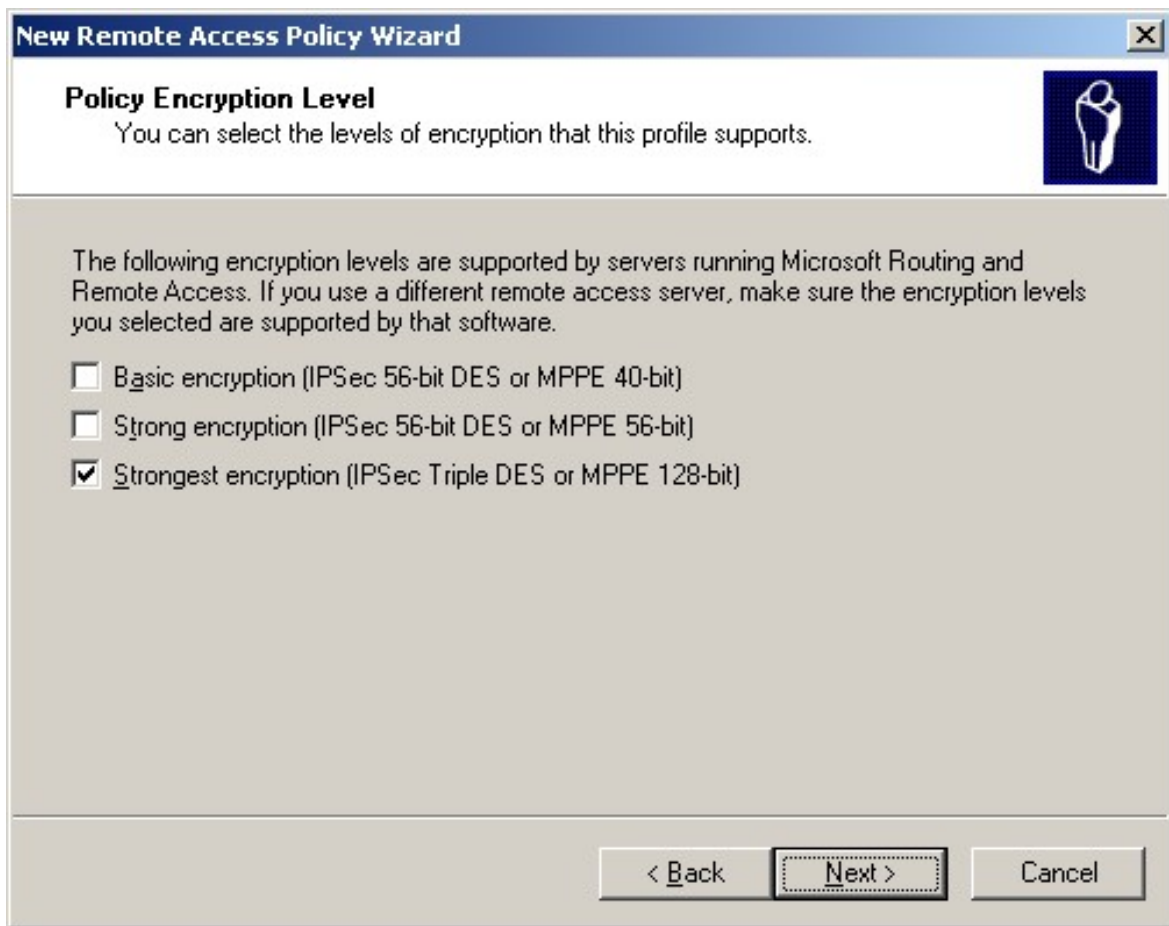


Figure 6: the Policy Encryption Level screen

10. Finish out the wizard by clicking Finish.

Configure attributes to be quarantined

Now, you need to actually configure the attributes that will be assigned to the quarantined session.

1. Back in RRAS Manager, right-click on the new Quarantined VPN remote access connections policy, and select Properties from the context menu.
2. Navigate to the Advanced tab, and click Add to include another attribute in the list.
3. The Add Attribute dialog box is displayed, as depicted in Figure 7.

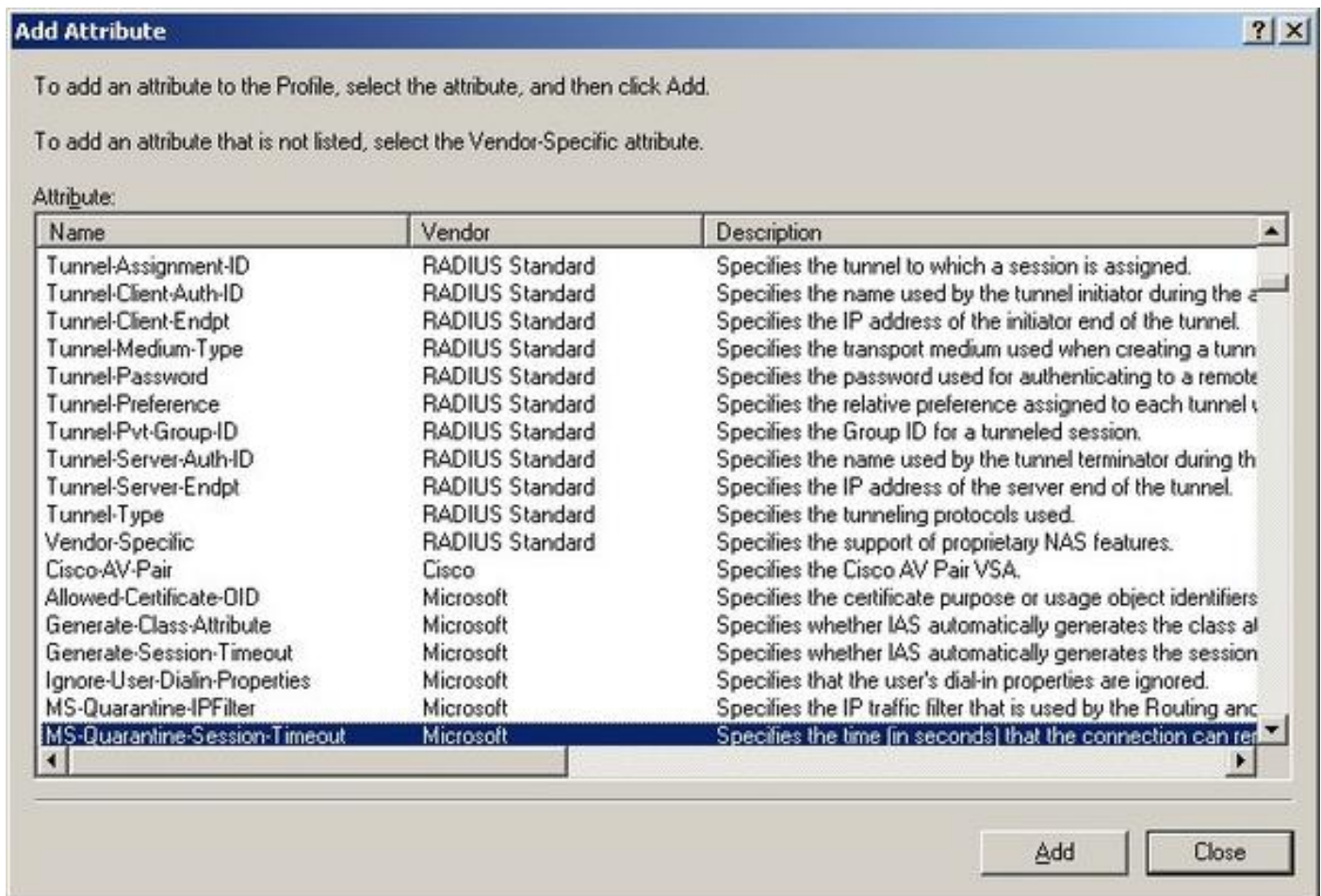


Figure 7: The Add Attribute dialog box

- Click MS-Quarantine-Session-Timeout, and then click Add.
- In the Attribute Information dialog box, type the quarantine session time in Attribute value. Use a sample value of 60, which will be measured in seconds, for the purposes of this demonstration. Click OK, and then OK again to return to the Advanced tab.
- Click Add. In the Attribute list, click MS-Quarantine-IPFilter, and then click Add again. You'll see the IP Filter Attribute Information screen, as shown in Figure 8.

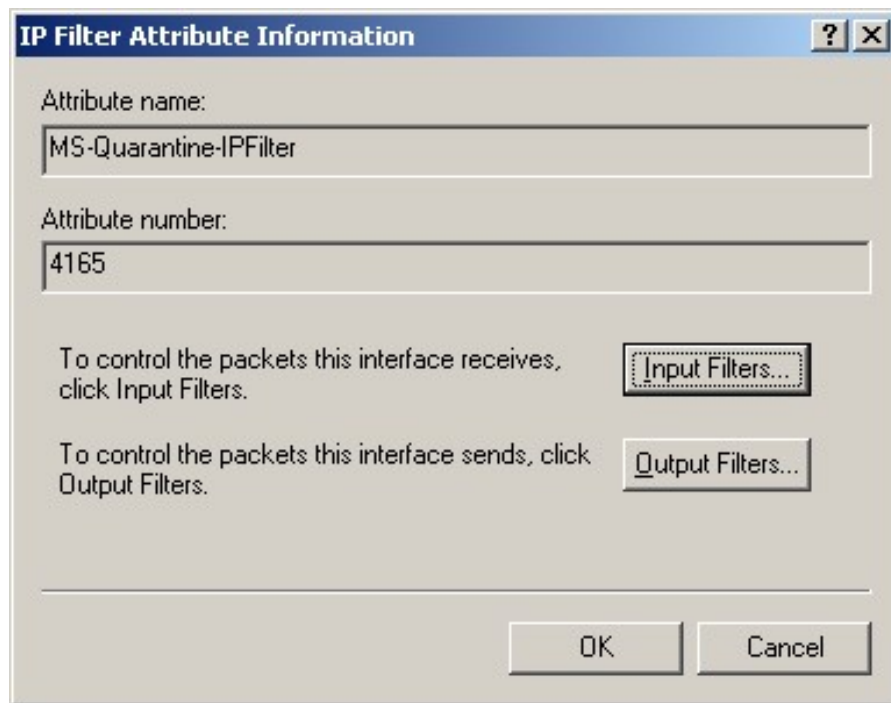


Figure 8: the IP Filter Attribute Information dialog box

7. Click the Input Filters button, which displays the Inbound Filters dialog box.
8. Click New to add the first filter. The Add IP Filter dialog box is displayed. In the Protocol field, select TCP. In the Destination port field, enter 7250. Click OK.
9. Now, back on the Inbound Filters screen, select the Permit only the packets listed below radio button. Your screen should look like Figure 9.

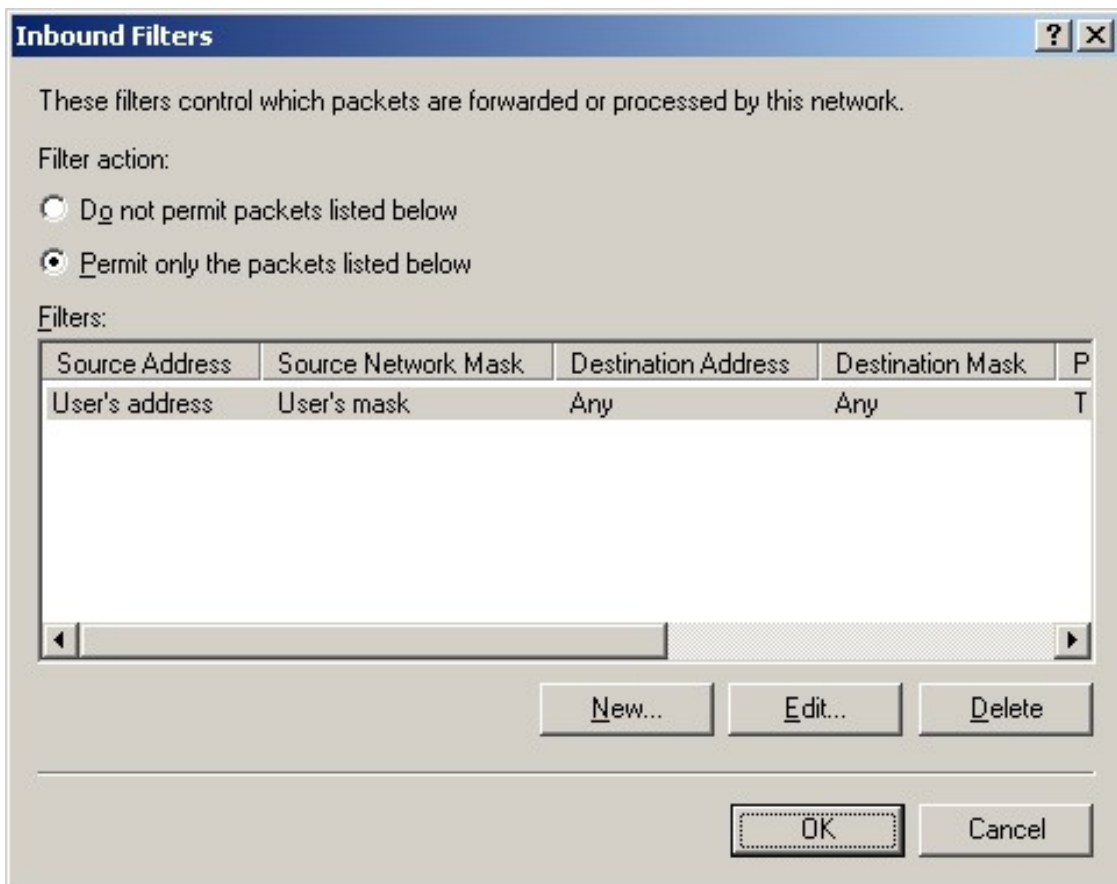


Figure 9: the completed Inbound Filters screen

10. Click New and add the input filters for DHCP, DNS, and WINS traffic, repeating the steps above and including the appropriate port number and type.
11. Click New and add an input filter for a quarantine resource, such as a Web server, where your profile installer is located. Specify the appropriate IP address for the resource in the Destination Network part of the Add IP Filter screen, as shown in Figure 10.

The screenshot shows a dialog box titled "Add IP Filter". It has a blue header bar with a question mark and a close button. The dialog is divided into two sections: "Source network" and "Destination network".

- Source network:** This section is unchecked. It contains two empty text boxes for "IP address" and "Subnet mask".
- Destination network:** This section is checked. It contains:
 - "IP address": 131 . 107 . 47 . 91
 - "Subnet mask": 255 . 255 . 255 . 255
 - "Protocol": A dropdown menu set to "TCP".
 - "Source port": An empty text box.
 - "Destination port": 80

At the bottom right, there are "OK" and "Cancel" buttons.

Figure 10: The Add IP Filter box, adding a quarantined Web resource

12. Finally, click OK on the Inbound Filters dialog box to save the filter list.
13. On the Edit Dial-in Profile dialog box, click OK to save the changes to the profile settings.
14. Then, to save the changes to the policy, click OK once more.

Creating Exceptions to the Rule

While it is certainly advantageous to have all users connected through a quarantined session until their configurations can be verified, there may be logistical or political problems within your organization that mitigate this requirement. If so, the simplest way to excuse a user or group of users from participating in the quarantine is to create an exception security group with Active Directory. The members of this group should be the ones that need not participate in the quarantining procedure.

Using that group, create another policy that applies to the exceptions group that's configured with the same settings as the quarantine remote access policy you created earlier. This time, though, don't add or configure either the MS-Quarantine-IPFilter or the MS-Quarantine-Session-Timeout attributes. Once the policy has been created, move the policy that applies to the exceptions group so that it is evaluated before the policy that quarantines everyone else.

Extending Functionality with ISA Server 2004

Quarantine Control for ISA Server 2004 works with the Routing and Remote Access service, as described

earlier in this article. The main difference lies in the fact that with ISA Server, you can require that a client attempting to log in is assigned to the Quarantined VPN Clients network in ISA, with an associated firewall policy that is very stringent, until the Connection Manager running on the desktop passes a message to ISA indicating the client passed the integrity check. Like the plain vanilla NAQC technique, ISA quarantining does rely on Connection Manager profiles and requires a baseline script to be developed that is custom to your environment.

Within ISA Server 2004, you have two options with regard to configuring quarantine functionality: you can enable quarantining using the Routing and Remote Access Service, which does require Windows Server 2003. Using this method, the quarantined clients go through the normal authentication and integrity check policies and ISA Server lets them join the regular VPN Clients network, as seen within the ISA Server interface, only when they've passed the check. You can also enable quarantining through ISA Server itself, and clients can make use of the integrated Quarantined VPN Clients network and any firewall policies associated therewith. The main strength of this method is that you can use quarantining on any ISA Server computer, not just those with Windows Server 2003 installed.

ISA Server quarantining supports a more robust timeout feature, allowing clients to remain in the Quarantined VPN Clients network for a specific number of seconds before being disconnected, and it also supports an exception list, which allows you to identify users (via either Active Directory or a RADIUS server) that should not be quarantined no matter what.

The listening components for quarantining have been upgraded specifically for ISA Server support and are available in the ISA Server 2004 Resource Kit, which can be [obtained](#) from the Microsoft site.

To enable quarantining with ISA Server:

1. Open ISA Server Management.
2. On the left pane, expand the node that corresponds to your computer, and then click Virtual Private Networks (VPN).
3. In the right pane, navigate to the Tasks tab, and then click Enable VPN Client Access.
4. Now, expand the Configuration node and select Networks.
5. In the middle pane, click the Networks tab.
6. Double-click on the Quarantined VPN Clients network to open the properties box for the network.
7. Navigate to the Quarantine tab. This is shown in Figure 11.
8. Click the 'Enable quarantine control' checkbox to allow quarantining to take place. A warning will appear to make sure you understand that the effect is immediate, and without proper configuration, clients will be indefinitely quarantined.
9. Choose whether to quarantine by RADIUS server policies (the first option) or ISA Server policies (the second option).
10. Enter a time-out for clients in the quarantined network in the Disconnect quarantined users after

box.

11. Enter any exceptions to quarantining in the 'Exempt these users from Quarantine Control' box.
12. Click OK, and then Apply in the ISA Server Management console, to apply the changes.

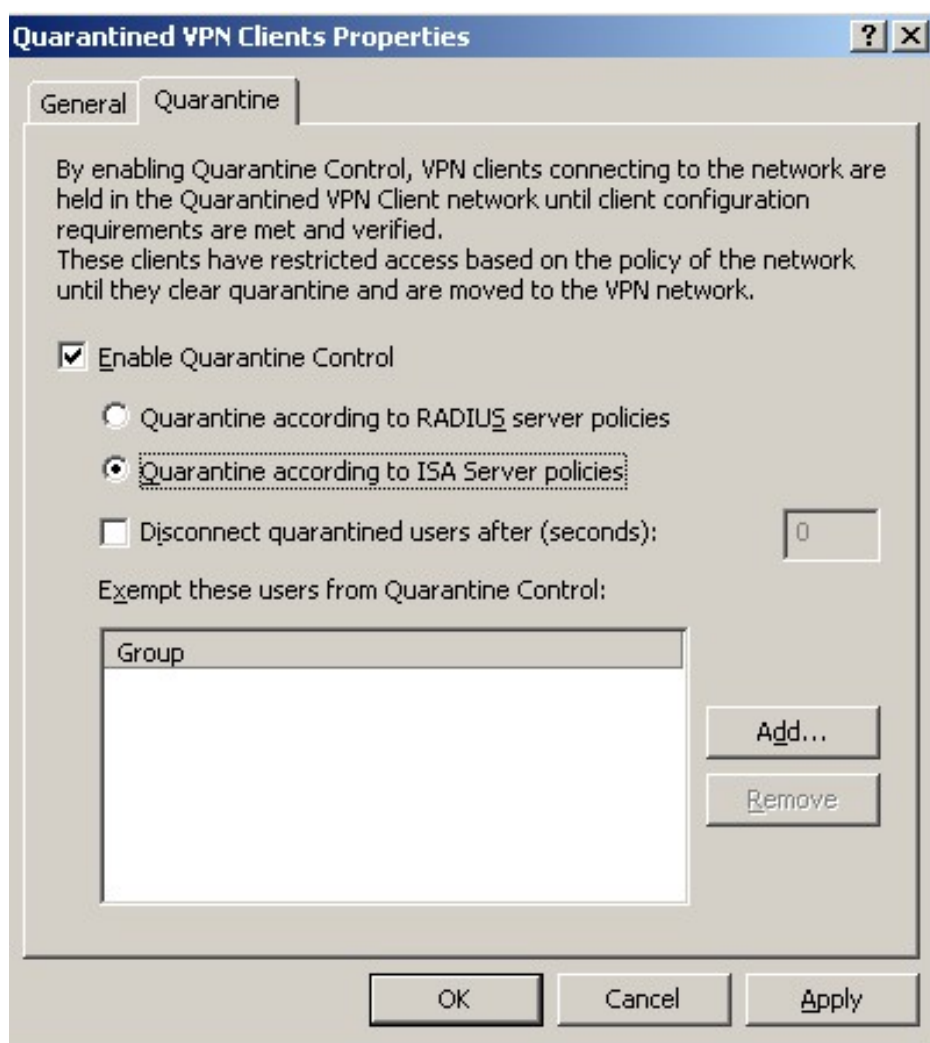


Figure 11: Quarantined VPN Clients in ISA Server 2004

Once you have completed these steps, from the ISA Server 2004 Resource Kit find the ConfigureRQSforISA.vbs script and run it. This will automatically create an access rule within ISA that will allow traffic to pass on port 7250 from both the VPN Clients and the Quarantined VPN Clients networks to the Local Host network. This is crucial traffic, because notifications from client computers that they have passed the integrity checks and are eligible to move to the regular network are sent on this port.

You might also consider establishing access rules for the Quarantined VPN Clients network that do the following:

- Allow transmissions to any LDAP servers on the internal network.
- Allow traffic to be passed to domain controllers.
- Allow DNS, DHCP, and WINS traffic to be passed to a hardened set of DNS servers, perhaps on a perimeter network.

- Allow traffic to a hardened, isolated web server that contains antivirus software, signature and detection engine updates.

Conclusion

In this article, I've discussed quarantining using services included in Windows Server 2003 and its associated resource kits and feature packs, and I've also touched on extended quarantine functionality within ISA Server. Your use of these techniques will help prevent or minimize the impact compromised remote hosts pose to your network when they attempt to connect.

About the author

[Jonathan Hassell](#) is an author and consultant specializing in Windows administration and security. He is the author of *Managing Windows Server 2003* and *RADIUS*, both published by O'Reilly & Associates, and *Hardening Windows*, published by Apress. He also holds periodic public seminars; see www.hardeningwin.com for details. He has written for *Windows & .NET Magazine* and *WindowsITSecurity.COM* and is a contributor to *PC Pro*, a leading computer magazine in the United Kingdom.

View [more articles](#) by Jonathan Hassell on SecurityFocus.

Comments or reprint requests can be sent to the [editor](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus