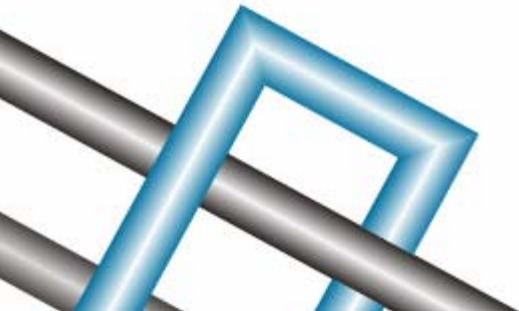


design and
implementation
of strategic
technology
solutions



34736 Moffat Ave., Mission, BC V2V 6R6
Tel: 604.820.1619 Cel: 604.996.6331
gower.mike@shaw.ca **www.itblueprint.ca**

Implementing ISA 2004 Quarantine v.1.0.1



Implementing ISA 2004 Quarantine

Foreword

These instructions are meant to build upon an existing L2TP/IPSec certificate based VPN solution using ISA 2004 SP1. Before implementing this solution, ensure that your L2TP VPN solution is working correctly.

This document has been put together from a variety of sources as well as modified scripts. For more information, please see the references at the end of the document.

Introduction

The ISA Server 2004 VPN Quarantine feature allows you to pre-qualify VPN clients before those clients are allowed access to resources that are available to non-quarantined VPN client machines. VPN Quarantine allows you to control the “quality” of client connected to the network via a VPN connection by insuring that the VPN client machine meet specific requirements, such as service pack level and updated anti-virus signatures.

VPN Quarantine requires client and server-side pieces to work correctly. The VPN client is configured with a VPN Quarantine script that it runs after making the VPN connection. The script checks for installed software on the VPN client machine. If the machine meets all the requirements set forth in the VPN-Q script, then it sends a message to the server-side component indicating that the system check was successful. At this point, the VPN client machine is moved from the VPN Quarantine Network to the VPN Clients Network. If the client isn't able to meet the requirements, it stays on the VPN Quarantine Network.

The ISA Server 2004 VPN Quarantine feature allows you to create Access Policies based on the network on which the VPN clients are placed. For example, if the VPN client machine is not able to meet the requirements set forth in the VPN-Q script, it can still access resources that you configure as available to machines that remain in quarantine. Those resources may contain files that give information on how to be removed from quarantine, or may contain automated processes that configure the VPN client with the required software so the next time the VPN client dials into the network, it will pass the VPN-Q check.

Notes

- Please note that if you start these steps, any existing VPN solution through ISA may not work until the entire configuration has been completed.
- Quarantine builds on the previous VPN solution, however, it begins to make use of an additional network called the “Quarantine VPN clients” network.

Implementation Instructions

ISA Server Modifications

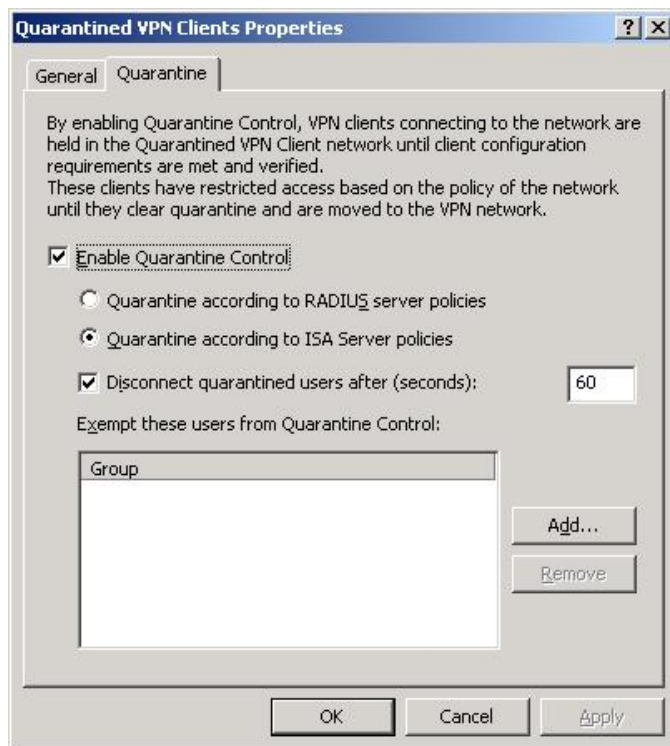
Access Rules

There are basically 3 rules that you need to configure on the ISA Server:

1. A rule that allows both Quarantined and non-quarantined VPN clients to connect to a DNS server on the internal network
2. A rule that allows quarantined VPN clients to access resources to help them remove quarantine (ie. this could be a web server with distributable code and binaries such as virus scanning software, updates, patches, etc). See some of the example documentation from Microsoft for more information on possibilities.
3. A rule that allows the VPN client network to access internal resources of your choosing (ie. Terminal Services server)

Enabling Quarantine Control

1. In the ISA management console, expand the server name and the **Configuration** node in the left pane of the console. Click the **networks** node
2. In the details pane, right click on the **Quarantined VPN clients** network entry on the **Networks** tab and click **Properties**
3. From the **Quarantine** tab, put a checkmark in the **Enable Quarantine Control** checkbox. Set a disconnect time if required. Click **Apply** and then click **OK**.



Install the Server 2003 Resource Kit Tools

The quarantine process uses several files that are included in the 2003 Resource Kit: rqc.exe and rqs.exe. Updates for these files for use with ISA 2004 are also available. The resource kit files can be accessed from the Microsoft downloads website at <http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en>

1. Run Rktools.exe from the ISA Server. This will install the required files into the C:\Program Files\Windows Resources Kits\Tools directory.

Install the Quarantine Service Listener on the ISA Server 2004 Firewall

The VPN Quarantine service listener will listen for the results of the script that the VPN client runs after it connects to the VPN server. The next step is to install the VPN Quarantine listener component.

Download the following files from the Microsoft website to the ISA Server:

Remote Access Quarantine Agent (RQS.msi)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=d4ec94b2-1c9d-4e98-ba02-b18ab07fed4e&DisplayLang=en>

Remote Access Quarantine Tool for ISA Server 2004 (RQSUtils.exe)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=3396c852-717f-4b2e-ab4d-1c44356ce37a&DisplayLang=en>

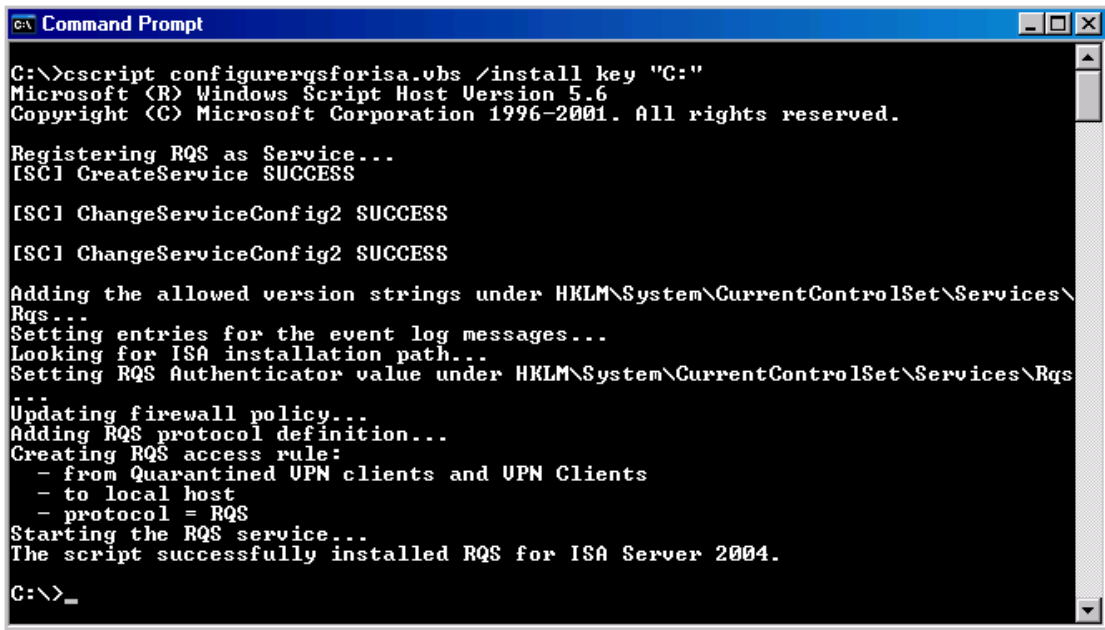
Steps:

1. Install the **RQS.msi** program on the ISA Server
2. Run the **RQSUtils.exe** program and extract the files to the root of C of the ISA Server.
3. Open the **command prompt** and change the focus to the root of the **C:** drive. Enter the following at the command prompt, replacing “**key**” with a unique string that will be passed to the listener on a successful health check and press ENTER:

```
Cscript ConfigureRQSForISA.vbs /install key "C:\Program Files\Windows Resource Kit\Tools"
```

Note: The path to the RQS.exe file must be included

4. You will see the following print out in the command prompt window.



```
Command Prompt
C:\>cscript configurerqsforisa.vbs /install key "C:"
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Registering RQS as Service...
[SC] CreateService SUCCESS

[SC] ChangeServiceConfig2 SUCCESS
[SC] ChangeServiceConfig2 SUCCESS

Adding the allowed version strings under HKLM\System\CurrentControlSet\Services\Rqs...
Setting entries for the event log messages...
Looking for ISA installation path...
Setting RQS Authenticator value under HKLM\System\CurrentControlSet\Services\Rqs...
Updating firewall policy...
Adding RQS protocol definition...
Creating RQS access rule:
- from Quarantined UPN clients and UPN Clients
- to local host
- protocol = RQS
Starting the RQS service...
The script successfully installed RQS for ISA Server 2004.

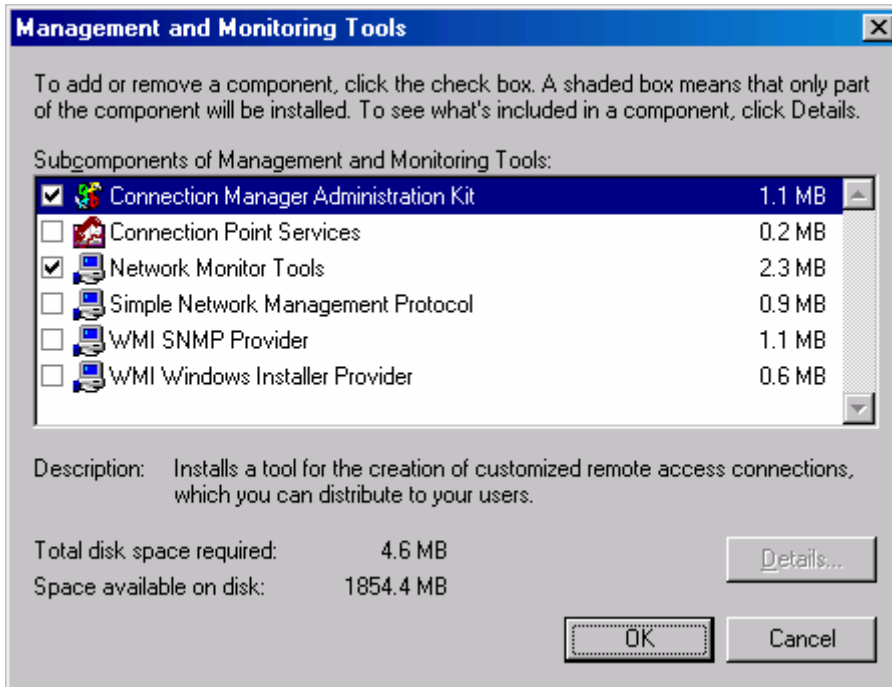
C:\>_
```

5. Restart the ISA Server 2004 firewall computer.

Install the Connection Manager Administration Kit on the ISA Server 2004 Firewall

Perform the following steps to install the Connection Manager Administration Kit onto the ISA Server 2004 firewall machine:

1. Click **Start** and point to **Control Panel**. Click **Add or Remove Programs**.
2. In the **Add or Remove Programs** window, click **Add/Remove Windows Components** on the left side of the window.
3. In the **Windows Components** page, select **Management and Monitoring Tools** from the **Components** list and click **Details**.
4. In the **Management and Monitoring Tools** dialog box, put a checkmark in the **Connection Manager Administration Kit** check box. Click **OK**.



5. Click **Next** on the **Windows Components** page.
6. Click **OK** in the **Insert Disk** dialog box. In the **Files Needed** dialog box, enter the path to the Windows Server 2003 **i386** folder in the **Copy files from** text box. Click **OK**.
7. Click **Finish** on the **Completing the Windows Components Wizard** page.

Create a Quarantine Script and Save it on the ISA Server Firewall

The quarantine script contains instructions that are run on the VPN client machine after the client establishes a VPN link with the ISA Server 2004 firewall/VPN server. This script and its supporting files are included with the CMAK connection profile that is created and then installed on the VPN client machine. You can create your own scripts using some of the various examples provided by Microsoft or try the modified scripts I have created.

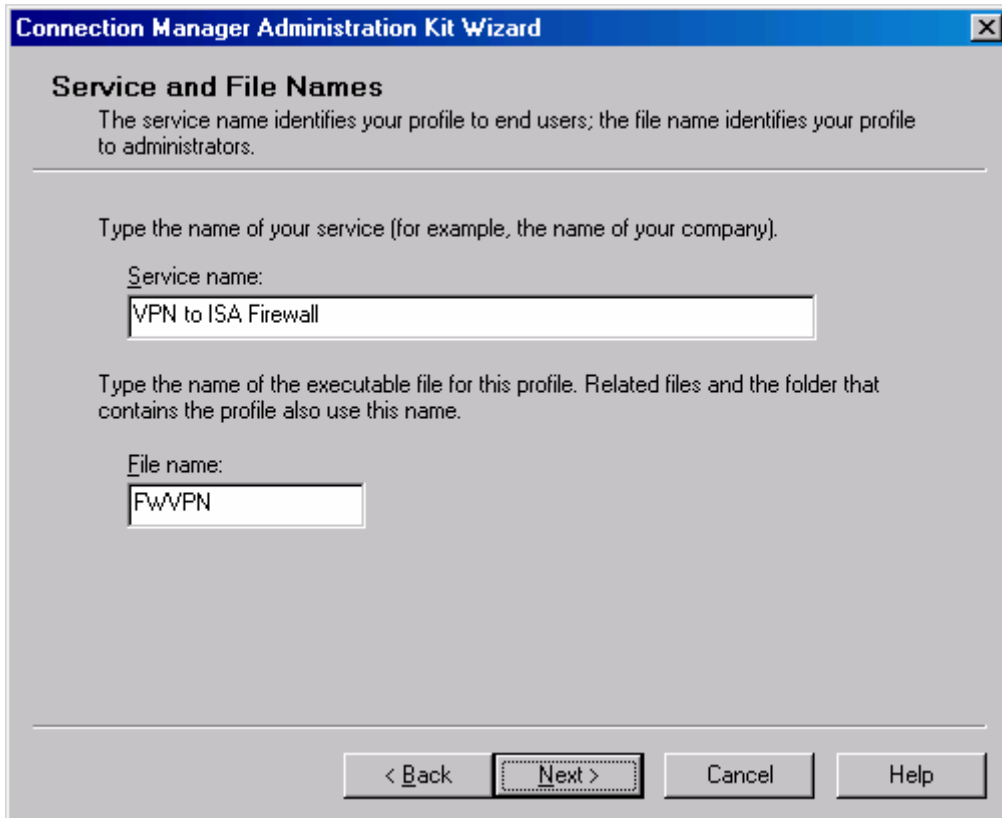
<http://www.itblueprint.ca/docs/isa2004/quarantine/scripts.zip>

Create the Connection Manager Profile

Now that we have the quarantine script configured, we're ready to create the CMAK profile. This profile will be used to install the VPN client software onto the VPN client machine. The quarantine script will be included with the VPN client software. The CMAK profile is very simple for the end-user to install: he only needs to double click on the CMAK package and the installation takes place automatically.

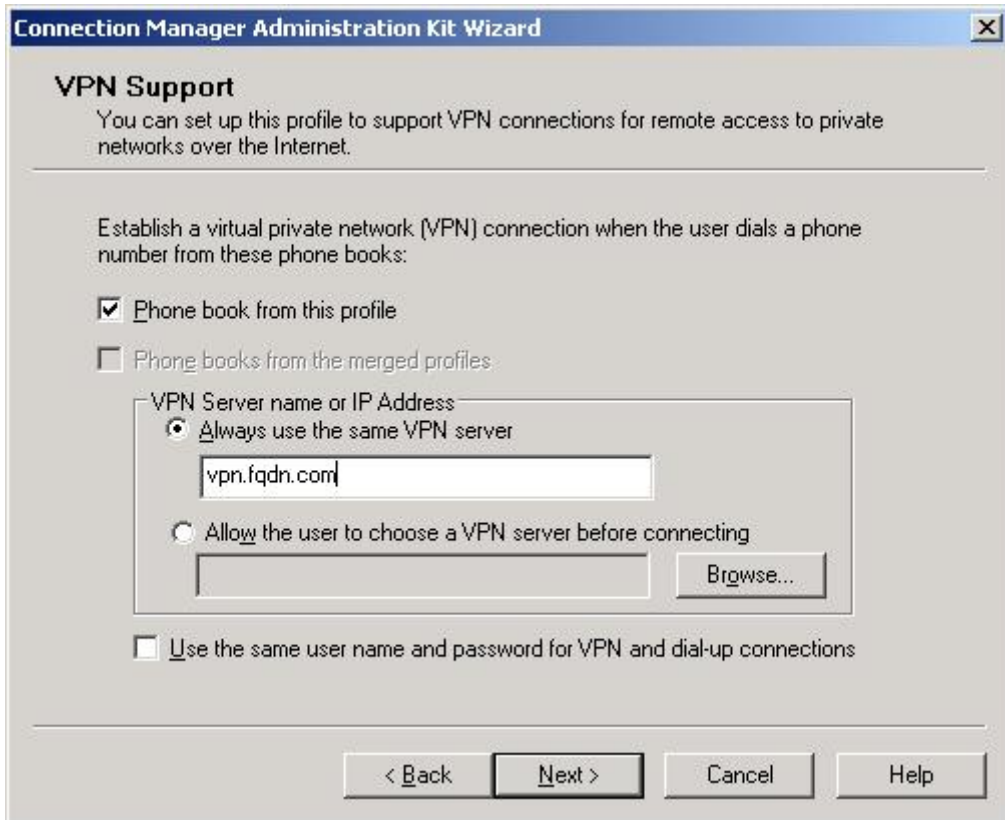
Perform the following steps to create the CMAK package:

1. Click **Start**, point to **Administrative Tools**, and click **Connection Manager Administration Kit**.
2. On the **Welcome to the Connection Manager Administration Kit Wizard** page, click **Next**.
3. On the **Service Profile Selection** page, ensure that **New profile** is checked and then click **Next**.
4. On the **Service and File Names** page, enter **VPN to ISA Firewall** in **Service name** and **FWVPN** in **File name**, and click **Next**.

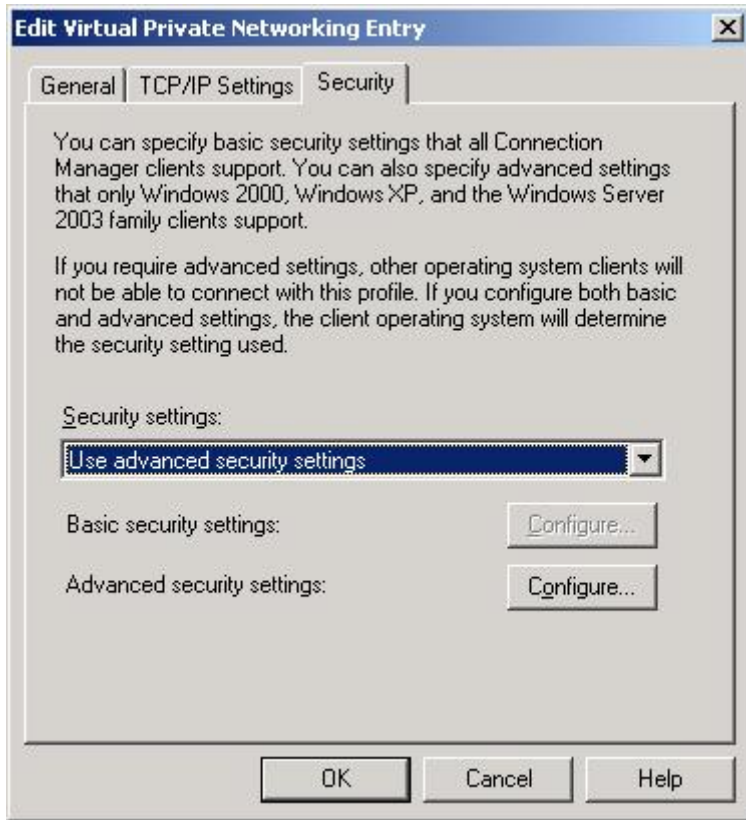


The screenshot shows a window titled "Connection Manager Administration Kit Wizard" with a close button in the top right corner. The main title is "Service and File Names". Below the title is a descriptive text: "The service name identifies your profile to end users; the file name identifies your profile to administrators." There are two input fields. The first is labeled "Service name:" and contains the text "VPN to ISA Firewall". The second is labeled "File name:" and contains the text "FWVPN". At the bottom of the window, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a dashed border.

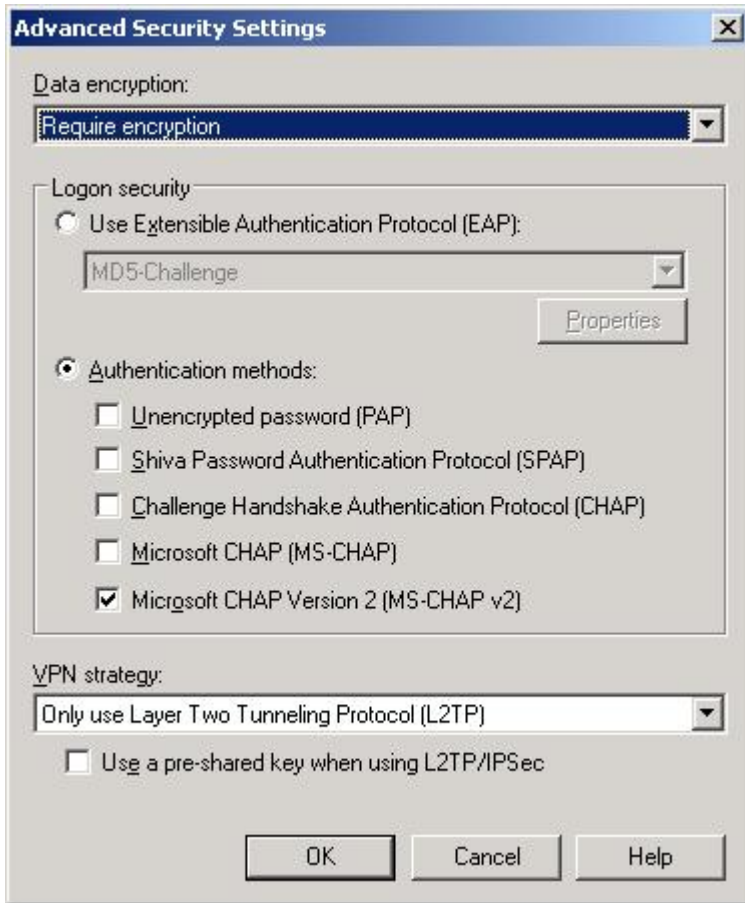
5. On the **Realm Name** page, click **Next**.
6. On the **Merging Profile Information** page, click **Next**.
7. On the **VPN Support** page, select the **Phone book from this profile** check box. In **VPN Server name or IP Address**, click **Always use the same VPN server**, type **vpn.fqdn.com** (or whatever you are using for a fqdn (as shown in the following figure), and click **Next**.



8. On the **VPN Entries** page, click the default entry, and click **Edit**.
9. Click the **Security** tab. In **Security settings** section, click **Use advanced security settings** (as shown in the following figure), and then click **Configure**.

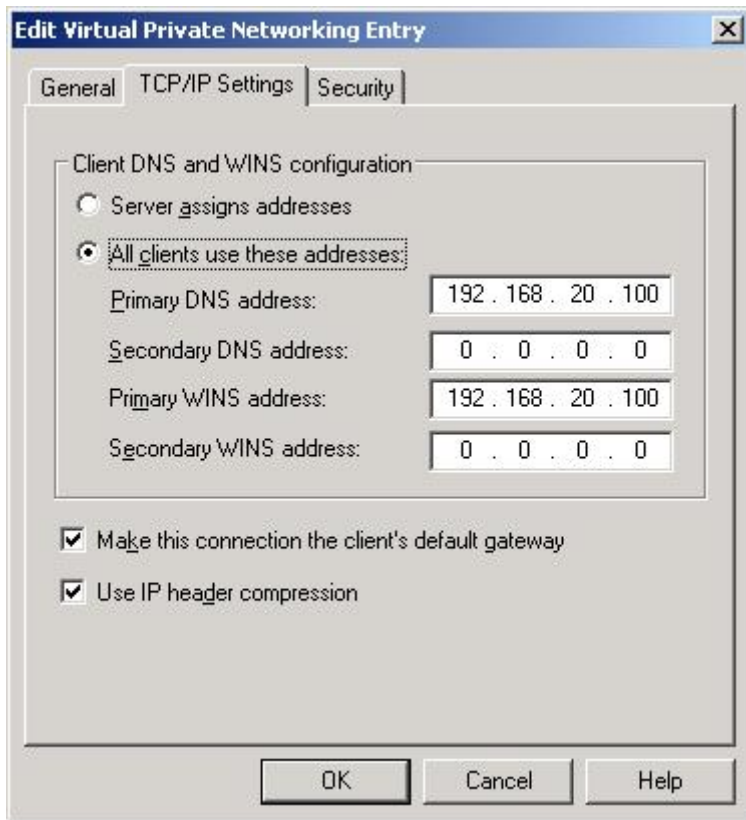


10. Under **Authentication methods**, clear the **Microsoft CHAP (MS-CHAP)** check box. In the **VPN strategy** list, select **Only use layer 2 Tunneling Protocol**. Click **OK** once and click on the **TCP/IP Settings**



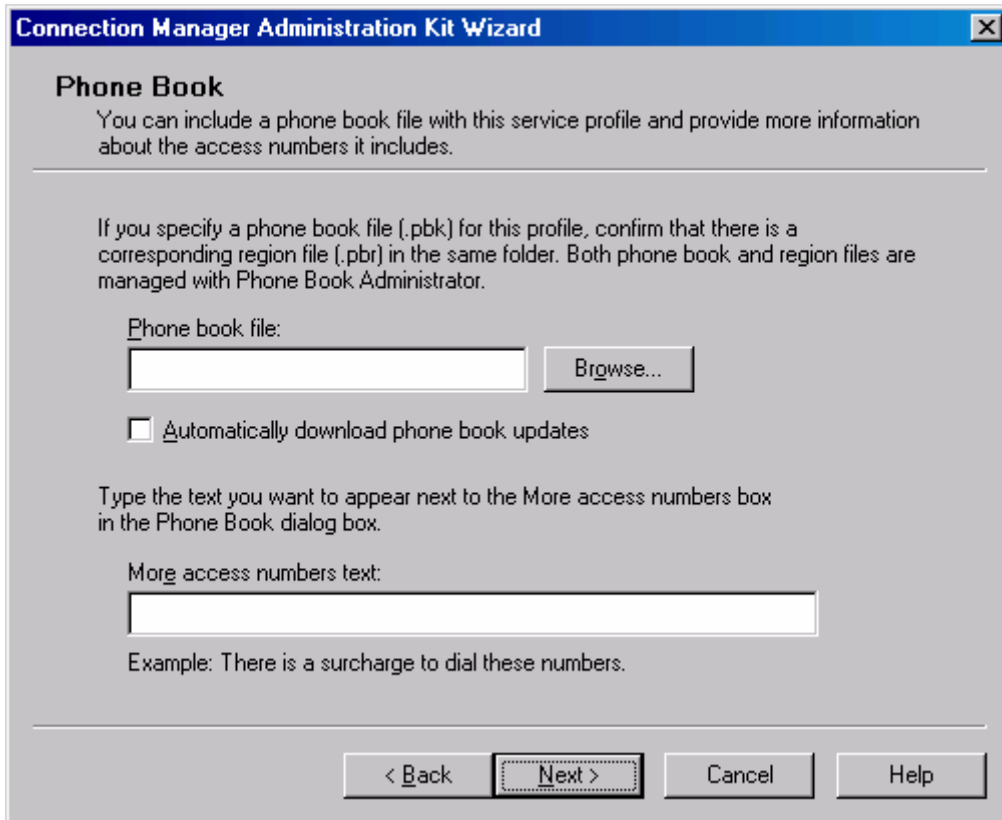
11. Enter in the IP address of the DNS and WINS servers that you wish Quarantined and VPN clients to be able to access. (WINS may not be necessary).

Note: You can also do this through DHCP, however, you would then need to install the DHCP relay agent on the ISA server.



12. Click OK once to return to the **VPN Entries** page, and then click **Next**.

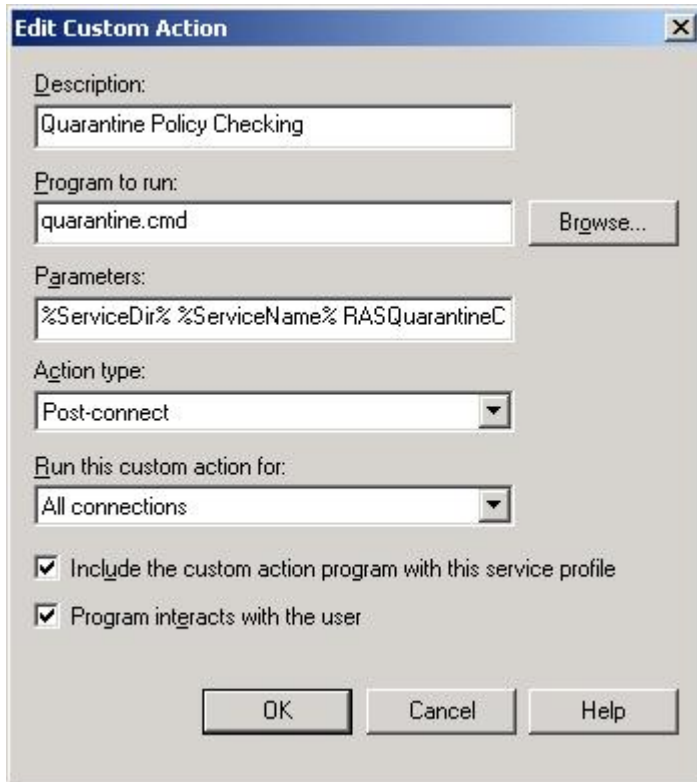
13. On the **Phone Book** page, clear the **Automatically download phone book updates** check box, and click **Next**.



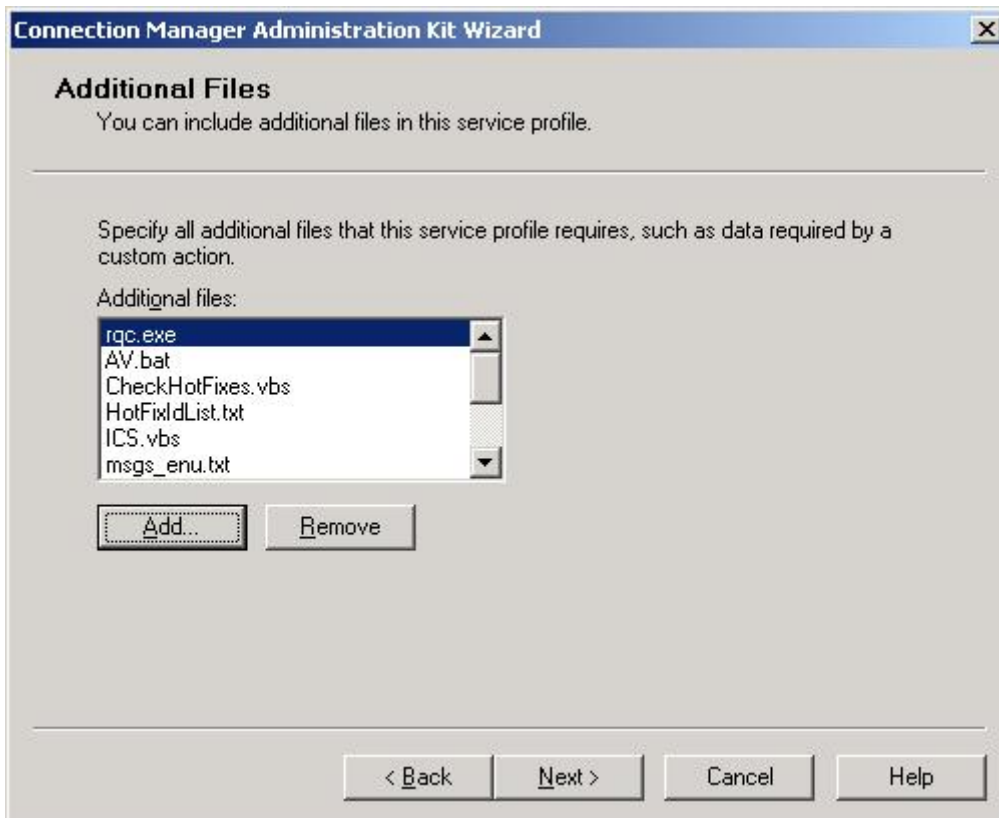
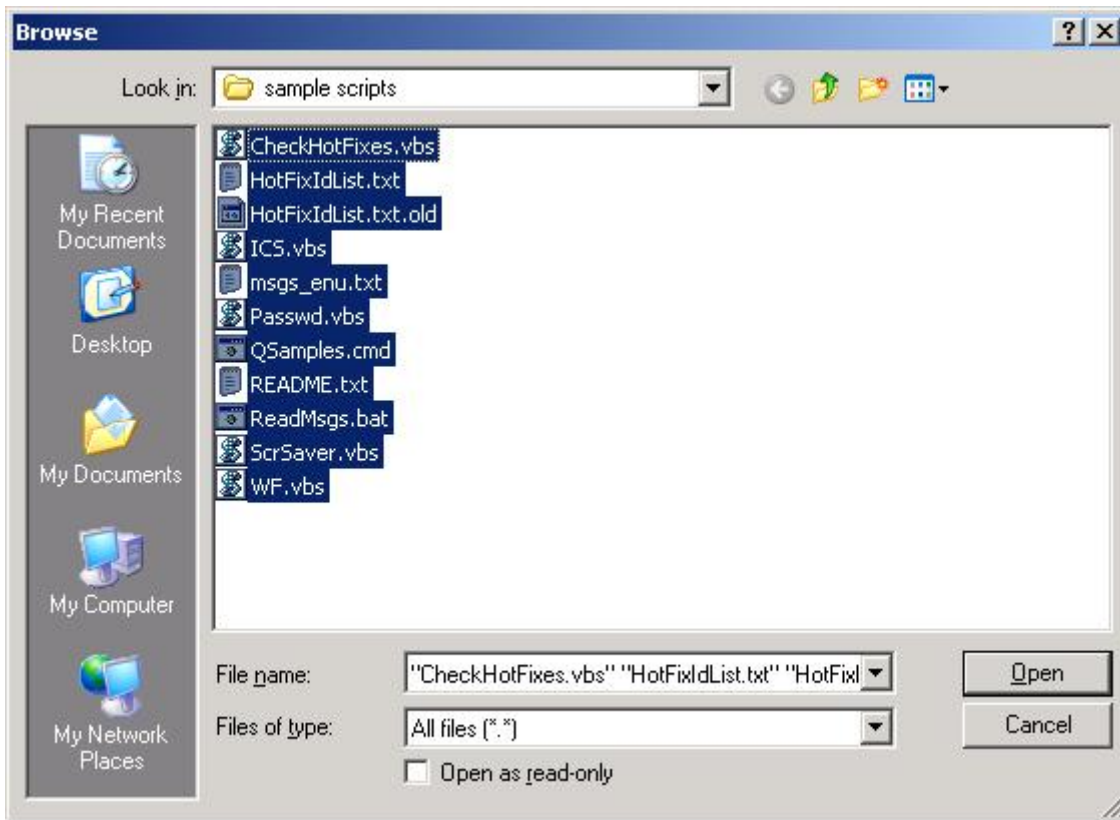
14. On the **Dial-up Networking Entries** page, click **Next**.
15. On the **Routing Table Update** page, click **Next**.
16. On the **Automatic Proxy Configuration** page, click **Next**.
17. On the **Custom Actions** page, click **New**.
18. In the **New Custom Action** dialog box, type **Quarantine policy checking** in **Description**. In **Program to run**, click **Browse** and find the **quarantine.cmd** file. In **Parameters**, enter
`%ServiceDir% %ServiceName% RASQuarantineConfigPassed %Domain%
%Username% 7250 %DialRasEntry% %TunnelRasEntry%`
In **Action type**, click **Post-connect**. In **Run this custom action for**, click **All connections**. Leave both check boxes selected, and click **OK**.

Note: The **quarantine.cmd** file is a modified Qsample.cmd that was provided by Microsoft. At this time I have shared the source at the following location:

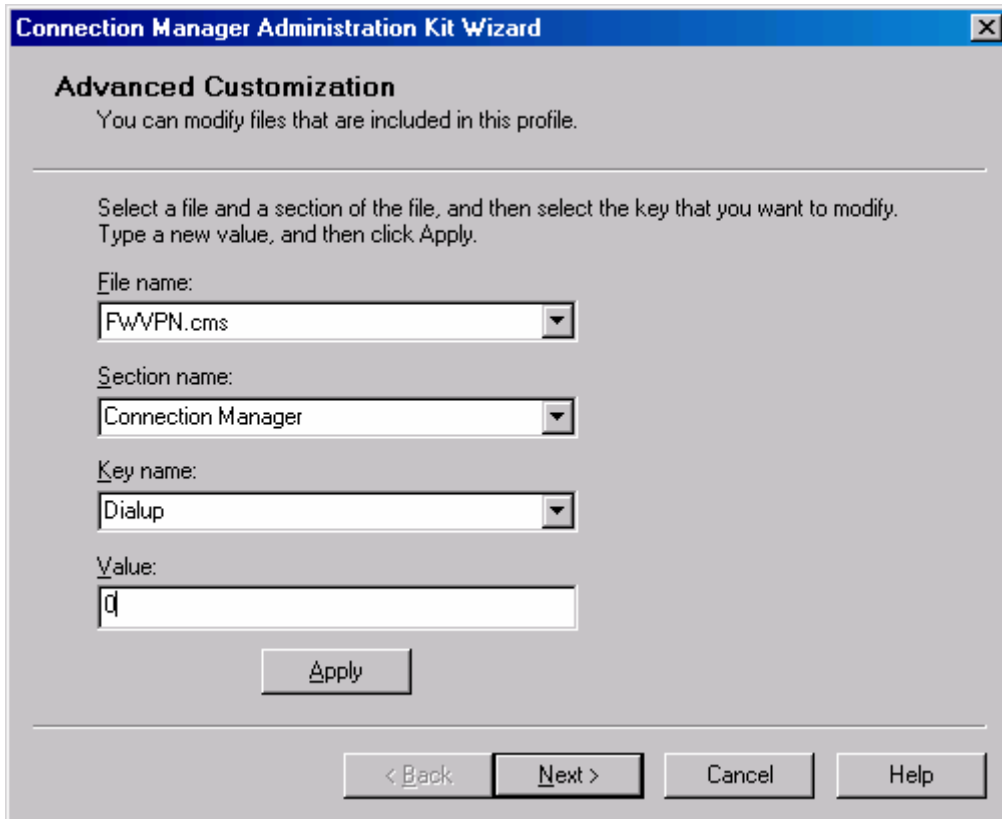
<http://www.itblueprint.ca/docs/isa2004/quarantine/scripts.zip>



19. On the **Logon Bitmap** page, click **Next**.
20. On the **Phone Book Bitmap** page, click **Next**.
21. On the **Icons** page, click **Next**.
22. On the **Notification Area Shortcut Menu** page, click **Next**.
23. On the **Help File** page, click **Next**.
24. On the **Support Information** page, click **Next**. (or fill in relative info)
25. On the **Connection Manager Software** page, click **Next**.
26. On the **License Agreement** page, click **Next**.
27. On the **Additional Files** page, click **Add**.
28. Browse to the **rqc.exe**, and click **Open**. (This is found in the C:\Program Files\Windows Resource Kits\Tools directory)
29. On the **Additional Files** page, click **Add**. Highlight all of the following files needed and click **Open**. Note: In this example, I included all files called by the **quarantine.cmd** script.



30. On the **Ready to Build the Service Profile** page, select the **Advanced customization** check box and then click **Next**.
31. On the **Advanced Customization** page, click **Connection Manager** in **Section name**, type **Dialup** in **Key name**, and type **0** in **Value**, as shown in the following figure. Click **Apply**, and then click **Next**.



The screenshot shows a dialog box titled "Connection Manager Administration Kit Wizard" with a close button (X) in the top right corner. The main heading is "Advanced Customization" with a subtitle "You can modify files that are included in this profile." Below this, there is a horizontal line and a paragraph of instructions: "Select a file and a section of the file, and then select the key that you want to modify. Type a new value, and then click Apply." There are four input fields, each with a label and a dropdown arrow: "File name:" with "FWVPN.cms", "Section name:" with "Connection Manager", "Key name:" with "Dialup", and "Value:" with "0". Below these fields is an "Apply" button. At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

32. A command prompt window will open and close as the profile is created. When the **Completing the Connection Manager Administration Kit Wizard** page appears, click **Finish**.



33. Copy the **FWVPN.exe** file to a floppy or network share point available to the VPN client machine. This file will have all other required files.

Install the Connection Manager Profile on the VPN Client Machine

Installing the Connection Manager Profile is simple. Just copy the profile you created with the Connection Manager to the VPN Client machine and then perform the following steps:

1. Insert the floppy disk on which you saved the **FWVPN.exe** into the floppy disk drive of the client, or copy the file to the VPN client machine from the network share point.
2. Open **Windows Explorer**, and browse to **FWVPN.exe**.
3. Double-click **FWVPN.exe**. When prompted to install the profile (as shown in the following figure), click **Yes**.



4. When prompted for whom to make this connection available, ensure that **My use only** is selected and then click **OK**.



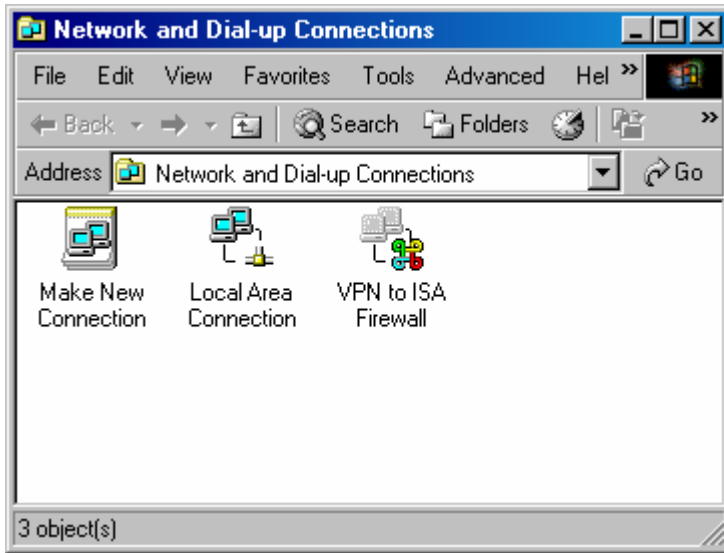
Note: The installation of this connection does **not include** any certificates that may be required for the actual L2TP/IPSec connection. It is assumed that the client already has these certificates installed and can already make an L2TP/IPSec connection.

Test the Connection

We're now ready to test the connection. The VPN client will first connect to the ISA Server 2004 VPN server and be placed on the VPN Quarantine Network. The client will be initially placed on the VPN Quarantine network, and then the client-side script will determine if it has met the pre-requisites. The RQC.exe component will inform the RQS.exe component on the VPN server that the script ran successfully and the client meets Quarantine requirements. At this point, the VPN client will be moved from the VPN Quarantine Network to the VPN Clients Network.

Perform the following steps to test the VPN Quarantine functionality:

1. Right click **My Network Places** on the desktop, and click **Properties**.
2. Double click on the **VPN to ISA Firewall** icon.










3. Enter your **user name band** and **Password** in the **VPN to ISA Firewall** dialog box. Click **Connect**.











The process can be monitored from the ISA Server's monitoring **Sessions** tab and you can see the switch between a Quarantined VPN client and after the rqc process runs and validates the client, causing the network to change from Quarantined to VPN Clients.

First connection:

	5/4/2005 6:50:10 AM	SecureNAT	192.168.254.101	External		192.168.254.101
	5/4/2005 6:50:12 AM	SecureNAT	192.168.254.3	Local Host		192.168.254.3
	5/4/2005 6:50:48 AM	Web Proxy	192.168.20.1	Local Host	anonymous	
	5/4/2005 6:50:12 AM	SecureNAT	192.168.1.1	Local Host		192.168.1.1
	5/4/2005 6:51:20 AM	Web Proxy	192.168.254.3	Local Host	anonymous	
	5/4/2005 6:52:56 AM	SecureNAT	192.168.20.110	Internal		192.168.20.110
	5/4/2005 6:56:48 AM	VPN Client	192.168.50.106	Quarantined VPN ...	mgower (?)	192.168.50.106

After validation:

	5/4/2005 6:50:10 AM	SecureNAT	192.168.254.101	External		192.168.254.101
	5/4/2005 6:50:12 AM	SecureNAT	192.168.254.3	Local Host		192.168.254.3
	5/4/2005 6:50:48 AM	Web Proxy	192.168.20.1	Local Host	anonymous	
	5/4/2005 6:50:12 AM	SecureNAT	192.168.1.1	Local Host		192.168.1.1
	5/4/2005 6:51:20 AM	Web Proxy	192.168.254.3	Local Host	anonymous	
	5/4/2005 6:52:56 AM	SecureNAT	192.168.20.110	Internal		192.168.20.110
	5/4/2005 6:56:48 AM	VPN Client	192.168.50.106	VPN Clients	mgower	192.168.50.106
	5/4/2005 6:56:51 AM	SecureNAT	192.168.20.100	Internal		192.168.20.100

References:

This document has been put together from a variety of sources as well as modified scripts. For more information, please see the following references below.

ISA Server 2004 VPN Deployment Kit: ISA2004SE_vpnkit-Rev 1 04.doc : Chapter 14

Step by Step guide for implementing Quarantine in a test lab

<http://www.microsoft.com/downloads/details.aspx?FamilyID=fe902704-52dd-4bbe-8a75-f8fbb76cd28a&DisplayLang=en>

VPN Quarantine Sample scripts for verifying client health configurations

<http://www.microsoft.com/downloads/details.aspx?FamilyID=a290f2ee-0b55-491e-bc4c-8161671b2462&DisplayLang=en>