

Releasing VPN Quarantine Users with VPN-Q 2006

- Author: **Thomas Shinder**
- Section: **Tutorials :: Configuration - Security**
- Published: **Mar 06, 2007**
- Updated: **Mar 09, 2007**



How VPN-Q 2006 fills an important gap in the ISA Server 2004/2006 Quarantine space.

Ever since the release of the ISA 2004 Firewall, ISA Firewall VPN admins who want to leverage all the benefits that the Quarantine solution has to offer have been frustrated with trying to manipulate and secure batch scripts to perform the required tasks. Utilizing a Quarantined Area for non-trusted clients and systems whose integrity cannot be guaranteed, is a sound practice. However, it is in verifying the end point's integrity and releasing the client from Quarantine where all the problems arise.



Microsoft has published some simplistic sample script templates designed to highlight how one can go about performing some rudimentary end point integrity checks, that when passed, releases the client from quarantine. Unfortunately, to really make this a workable solution, ISA Firewall admins need to do intense system development to turn these samples into a useable system checking utility. Following that you have to run through the process of manually building a Connection Manager Profile and make sure you have all those settings just right.

Finally, if by some miracle, you actually manage to develop and deploy the solution, one final and all too painful issue still remains: To release a client from quarantine, the releasing mechanism is embedded in plain sight within the unsecure batch file script. All a remote user needs to do (on his not so trustworthy system) is run the RQC.EXE command with a few parameters and the shared secret (found in plain sight within the script) and full access to the network is granted without ever having to run any of the checks!

Yep, what the ISA Firewall admin needs is fulfillment of the promise of remote access VPN quarantine. As it stands now, the VPN-Q feature is about to be relegated into the ISA Firewall's dustbin of history, along with active caching, the H.323 gatekeeper, and bandwidth controls. VPN-Q, like the rest of the technologies, is a great idea but Microsoft didn't finish the job. The features were left half-finished and they threw them against the wall to see if they'd stick. They didn't.

However, perhaps not all hope is lost for remote access VPN quarantine? Is there a solution that allows us to fulfill the promise of VPN-Q without us having to go broke in hiring expensive consultants for one-off solutions that will continue to cost us as we update our requirements in the future?

One solution is Winfrasoft's VPN-Q 2006. Compiled into a managed .NET application, VPN-Q performs a series of comprehensive security checks on the client's workstation and only when these checks are passed will the client gain full VPN access. Key checks that every organization needs are that all patches and updates have been applied and that the remote system has an up-to-date anti-virus package.

VPN-Q works with dozens of the most popular anti-virus and personal firewall packages available, and plugs into both Internet hosted Microsoft Update servers or internal WSUS servers so that you can ensure your remote users comply with the internal patch update policies. Central administration via GPOs gives administrators the power to determine which checks must be passed on the client's device before release from the quarantine network is allowed.

Most importantly, all this is done without the need for scripting or coding. That's right – NONE, not any. It also solves the security flaw with manually running the RQC.EXE process.

VPN-Q 2006 Security Feature Set

So what else can VPN-Q do apart from just AV, firewall and patch checking? Well it also extends standard quarantine services into the compliance arena by providing detailed central logs and including features like legal notices. Here is the full feature list from the web site:

Security Check \ Edition	Free	Standard	Enterprise
Minimum operating system and service pack level	Yes	Yes	Yes
Windows IP Routing status	No	Yes	Yes
Screen Saver Security settings	No	Yes	Yes
Windows Firewall status	No	Yes	Yes
3rd Party Personal Firewall status	No	Yes	Yes
Windows Firewall F&P Sharing exception status	No	Yes	Yes
Internet Connection Sharing status	No	Yes	Yes
Anti-Virus Scanner status	Yes	Yes	Yes
Anti-Virus Scanner up to date check	Yes	Yes	Yes
Automatic Updates status (Patch settings)	No	Yes	Yes
Security Update status (Missing patches)	No	Yes	Yes
Windows Software Update Services (WSUS) Integration	No	Yes	Yes

Other Feature \ Edition	Free	Standard	Enterprise
Runs on Windows Vista! (SP2)	Yes	Yes	Yes
Client and server runs on multi-lingual platforms (SP2)	Yes	Yes	Yes
Manual and Auto pre-shared keys for IPSec (SP2)	No	Yes	Yes
Central Logging	No	No	Yes
Central Management of policy (GPO)	No	No	Yes
Legal Notices and policy notification	No	No	Yes
Remediation capabilities	No	Limited	Yes
AES Encryption (Client <-> Server health state data)	56 bit	128 bit	256 bit

Installation

The installation of both the server and client components is brain-dead simple. On the server side the VPN-Q server installation will install the necessary Windows services for you, create the required access rules via a wizard and also enable the Quarantine network. The only thing you have to do before installing is enable normal VPN access to the ISA Server in the usual way. For details on how to accomplish this see my article [Enabling the ISA Server 2004 VPN Server](#).



Server Administration Wizard

The configuration wizard does the heavy lifting by allowing access to resources from the quarantine network. It handles things like accessing infrastructure services such as DNS to resolve internal server names and Active Directory to allow for group policy processing and WSUS servers to check the patch policy. The rules the wizard creates are pretty tight, for example, the WSUS rule only allows the specific WSUS related URL's out of the quarantine network based on the server name you specify, it's not a blanket allow all rule to the server.

You may still need to create your own extra rules if you want to allow other access to the network while the users are in quarantine. For example, to allow access to an internal Anti Virus update server.

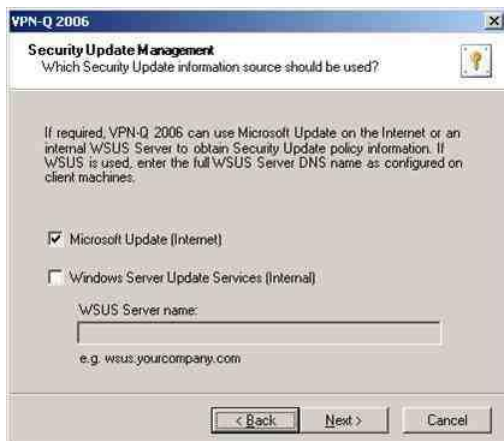


Figure 1

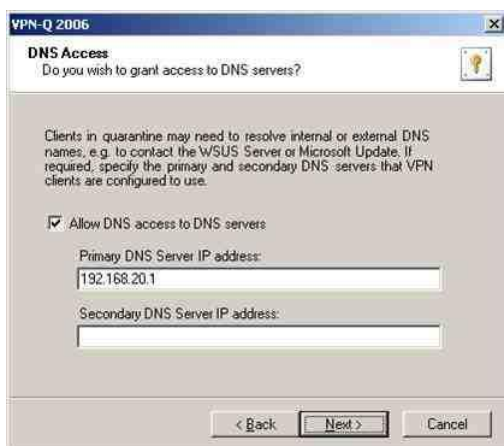


Figure 2

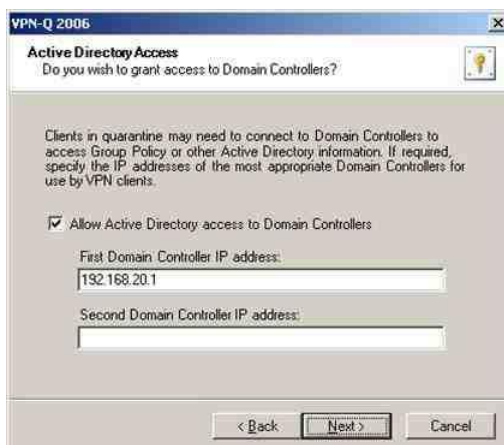


Figure 3

The VPN Client

The VPN client is created from the Server Administration console. When I say that the VPN client is created, I mean a custom Connection Manager (CMAC) package is built into a client installation .EXE containing all the quarantine bits and your specific settings. Installing the client is insanely easy, all the user needs to do is accept the license agreement and the connection to the VPN is complete, it's that simple. There is no alien 3rd-party dial-up software here, it's all using a standard Windows

CMAK connection. And best of all, you don't have to be a local administrator to install or run it either!

Other neat little enhancements include things like, having the quarantine logo associated with the connection and your organization name in the connection name. From what I hear, future versions will allow for further branding customization.



Figure 4

Client Device Security Check UI

What I really like about the product is the look and feel and how tightly it integrates with Windows. The security checks are clear with an easy to follow "traffic light" system. Should a client computer fail some checks, then remediation facilities can explain what a user needs to do to ensure that the system passes future tests. The Enterprise Edition VPN-Q 2006 allows you to direct users to custom URL for remediation such as an internal help desk page.



Figure 5

For those that really want to know what's going on there is a details tab too.

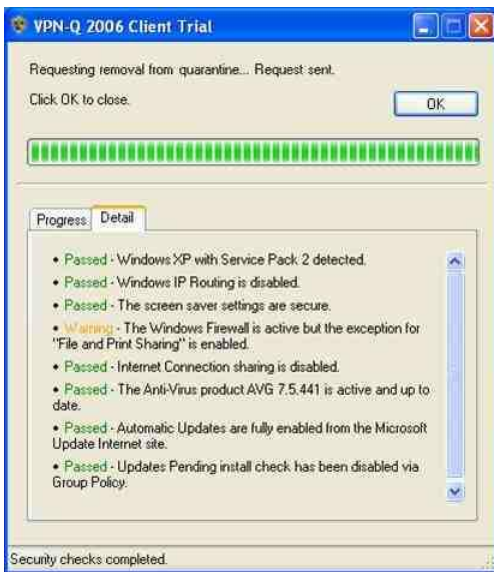


Figure 6

Again with the VPN-Q 2006 Enterprise Edition, you are able to completely customize the desired policy for your needs via Group Policy. You can disable certain checks if you don't want to run them, or you can change the outcome of a check. You can even drill down into how to behave for each severity level of updates from Microsoft if you so wish, although the defaults will be fine for most installations.



Summary

VPN-Q 2006 fills an important gap in the ISA Server 2004/2006 Quarantine space. VPN-Q 2006 finally provides some comfort to ISA Firewall admins who are concerned about the level of security on remote user's systems and will also help keep the compliance police at bay. No longer do we have to try and manipulate sample scripts only to be left with a useless and flawed solution that can't be realistically deployed in a production environment. Winfrasoft has managed to find the balance between an easy to use system for the users and a technically powerful enough solution for the administrators.

For more information on Winfrasoft's VPN-Q 2006, please visit the Winfrasoft Web site at <http://www.winfrasoft.com/vpnq.htm>

Original article available at:

<http://www.isaserver.org/tutorials/Releasing-VPN-Quarantine-Users-VPN-Q-2006.html>