



Winfrasoft VPN-Q 2006

Solution

What is your weakest link...?

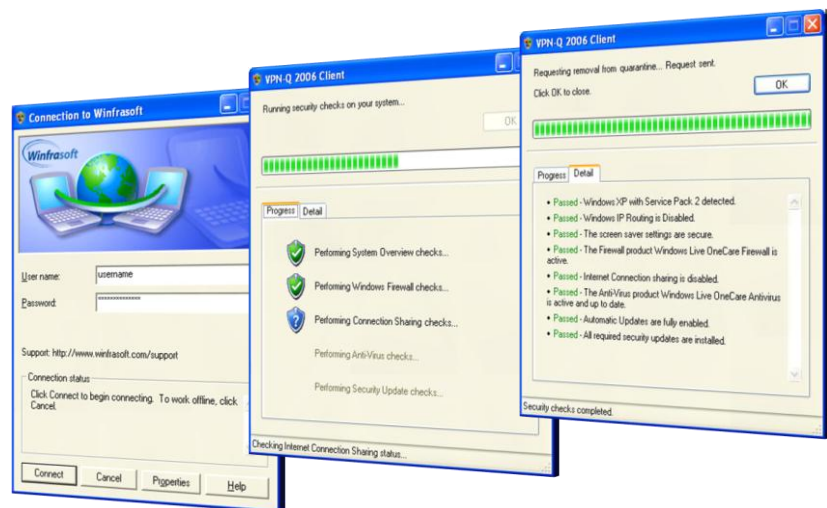
- ✗ Do you have an up-to-date and enforced antivirus and patch management system in place for your corporate network, only to find that your remote clients don't comply and may compromise your internal network...?
- ✗ Do you have employees who spend most of their time out of the office resulting in them connecting to the network with unpatched or infected machines...?
- ✗ Do you entrust your employees with keeping their laptops or remote computers up-to-date with the latest security updates...do they? ...are you sure?
- ✗ How do you enforce the rules by which your remote users connect to the corporate network...?
- ✗ Is your remote access solution so complex to use it hinders business productivity?

VPN Compliance

The ability to access your corporate network regardless of where you are in the world is a necessity in modern times where mobility and remote access are key factors in a business' ability to out-deliver its competitors.

Traditional IP based VPN's have been widely used throughout the world for remote connectivity but they are typically hampered by complex client software and difficulties in managing the health status of remote clients. Many viruses and worms (Nimda, Code red, slammer etc) propagate via these unmanaged VPN endpoints resulting in breaches of the internal networks' security.

Risk and costs associated with VPN's have been difficult to balance with the business benefits they bring...until now! Winfrasoft VPN-Q 2006 leverages the benefits of traditional IP based VPN's whilst addressing their weaknesses in a cost effective way. This allows you to significantly reduce the costs and risks associated with remote clients connecting to the network.



Winfrasoft VPN-Q 2006 works by delaying full connectivity to the corporate network until pre-defined security checks have been carried out on the configuration of the remote computer. If the remote computer attempting to connect to the corporate network does not pass these checks and is determined to be non-compliant with the security policy, their connection can be terminated or kept in quarantine with limited connectivity.

The Winfrasoft VPN-Q 2006 solution is built upon the security and reliability of Windows Server 2003 and Microsoft .NET, and can easily integrate into almost any network environment.

Winfrasoft VPN-Q 2006 is a complete client and server solution for deploying and managing VPN Quarantine services with Microsoft ISA Server 2004/2006 or Windows Server 2003 RRAS to meet compliance requirements - no scripting or coding required!

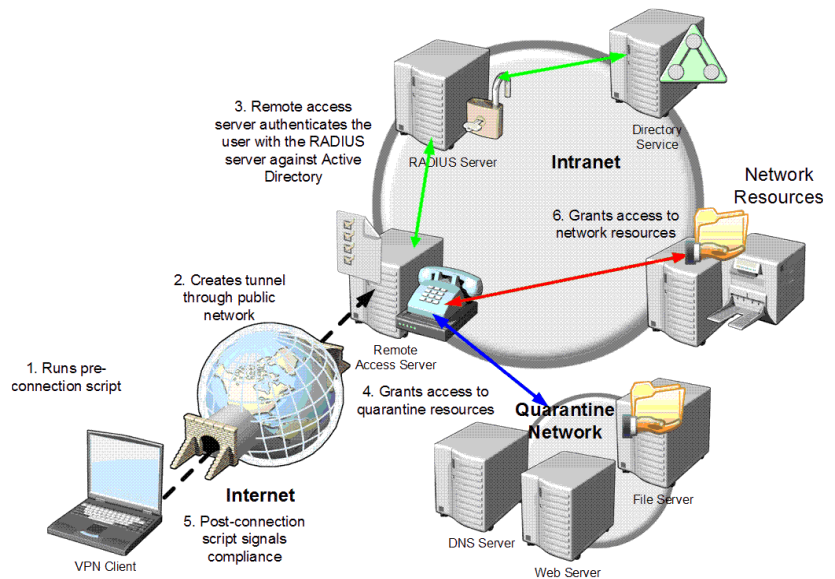


Highlights

- ✓ Separates remote clients from the corporate network unless they conform to your policy.
- ✓ Security check overview:
 - ✓ Supported operating systems and service packs?
 - ✓ Antivirus software installed, running and up-to-date?
 - ✓ Windows / 3rd party Firewall enabled on network interfaces?
 - ✓ Required security updates / patches installed?
- ✓ Custom remediation capabilities.
- ✓ Active Directory group policy based central management.
- ✓ Self updating VPN client built on the native Windows connections.
- ✓ Central logging of remote PC security profile.
- ✓ Least privilege access – no admin rights required for the user.
- ✓ FIPS 197 compliant cryptography.
- ✓ VeriTest approved for ISA Server 2004.

The VPN Quarantine Process

The connection process has been designed to be secure whilst maintaining ease of use for a user. The process is as follows:



1. The client computer performs a pre-connection check to ensure that the computer meets pre-defined requirements. This includes checking for updates to the Winfrasoft VPN-Q 2006 client software.
2. After the pre-connection checks have completed, the computer connects to the remote access server (ISA Server or RRAS) using an L2TP/IPSec or PPTP VPN.
3. The remote access server authenticates the user against any directory service via RADIUS or directly against Active Directory via domain membership.
4. The remote access server places the client in quarantine and runs detailed security checks. These checks include checking for missing security updates, virus signatures and personal firewall settings. While in quarantine, the client only has access to limited resources, which may include remediation services, to enable it to comply with the prescribed security requirements, or an Intranet site.
5. Once the checks have completed and the checks are successful, the client computes an encrypted signal and sends it to the remote access server to signify compliance to the policy. If the connection does not meet the requirements within the specified time-out period, VPN-Q 2006 notifies the user and the remote access server. The connection then remains active until the timeout expires or policy settings disconnect the connection.
6. Provided the remote access server received a valid encrypted signal from the client, it grants appropriate access to internal network resources. If ISA Server is used the access granted, once quarantine has been lifted, can be further restricted by user name or group for granular security control.

Microsoft
GOLD CERTIFIED
Partner

ISV/Software Solutions
Networking Infrastructure Solutions

Winfrasoft