Ten things you should know about troubleshooting VPN connections

Version 1.0
August 31, 2005

By Deb Shinder and Dr. Thomas Shinder

Virtual private networking provides a secure and convenient way for users to connect remotely to their corporate networks, but plenty of things can go wrong. Here are some of the most common problems encountered with VPN connections and what you can do about them.

Table of contents

1 Users can't access file servers

If the user can access the file server using an IP address but not a name, then the most likely reason for failure to connect is a name resolution problem. Name resolution can fail for NetBIOS or DNS host names. If the client operating system is NetBIOS dependent, the VPN clients should be assigned a WINS server address by the VPN server. If the client operating system uses DNS preferentially, VPN clients should be assigned an internal DNS server that can resolve internal network host names.

When using DNS to resolve internal network host names for VPN clients, make sure that these clients are able to correctly resolve unqualified fully qualified domain names used on the corporate network. This problem is seen most often when non-domain computers attempt to use DNS to resolve server names on the internal network behind the VPN server.

2 Users can't access anything on the corporate network

Sometimes users will be able to connect to the remote access VPN server but are unable to connect to any resources on the corporate network. They are unable to resolve host names and unable to even ping resources on the corporate network.

The most common reason for this problem is that users are connected to a network on the same network ID as the corporate network located behind the VPN server. For example, the user is connected to a hotel broadband network and is assigned a private IP address on network ID 10.0.0.0/24. If the corporate network is also on network ID 10.0.0.0/24, they won't able to connect because the VPN client machine sees the destination as being on the local network and will not send the connection to the remote network through the VPN interface.

Another common reason for communications failures is that the VPN clients are not allowed access to resources on the corporate network due to firewall rules on the colocated VPN server/firewall device to which they are connected. The solution is to configure the firewall to allow the VPN clients access to the appropriate network resources.

3 Users can't connect to VPN server from behind NAT devices

Most firewalls and NAT routers support the PPTP VPN protocol from behind a NAT. However, some high profile network equipment vendors don't include a NAT editor for the PPTP VPN protocol. If the user is located behind such a device, the VPN connection will fail for PPTP attempts but may work for alternate VPN protocols.

All NAT devices and firewalls support IPSec passthrough for IPSec-based VPN protocols. These VPN protocols include proprietary implementations of IPSec tunnel mode and RFC compliant L2TP/IPSec. These VPN protocols can support NAT traversal by encapsulating the IPSec communications in a UDP header.

If your VPN client and server support NAT traversal and the client attempts to use L2TP/IPSec to connect to a NAT-T compliant VPN server from across a NAT, the most likely reason for this failure is that the client is running Windows XP Service Pack 2. Service Pack 2 “broke” NAT traversal for L2TP/IPSec VPN clients. You can solve this problem with a Registry entry on the VPN client computer, as described in a KB article at http://support.microsoft.com/default.aspx?scid=kb;en-us;885407.

4 Users complain of slow performance

Slow performance is one of the most difficult problems to troubleshoot. There are a number of reasons for why VPN clients appear to perform poorly and its critical to have the users describe exactly what they are doing when they experience poor performance.

One of the more common reasons for poor performance for VPN clients is when those clients are located behind DSL networks employing PPPoE. These network connections often encounter MTU problems that can cause both connectivity and performance issues. For more information on MTU issues for Windows clients, check out http://support.microsoft.com/default.aspx?scid=kb;en-us;283165

5 Users can connect via PPTP but not L2TP/IPSec

PPTP is a simple protocol to set up on both the VPN server and client. All the user requires is the built-in VPN client software included with all versions of Microsoft operating system and a valid user name and password for an account that has remote access permissions. The VPN server component, if based on Windows Routing and Remote Access Service (and just about any other VPN server supporting PPTP remote access VPN client connections) is easy to set up and usually works automatically after running a short configuration wizard.

L2TP/IPSec is more complex. Both the user and the user's machine must be able to authenticate with the VPN server. Machine authentication can use either a pre-shared key or machine certificate. If you use pre-shared keys (not recommended for security reasons), check that the VPN client is configured to use the same pre-shared key as the server. If you use machine certificates, confirm that the VPN client machine has a machine certificate and that is also trusts the certificate authority that issued the VPN server's machine certificate.

6 Site-to-site VPNs connect but no traffic passes between the VPN gateways

When creating site-to-site VPN connections between Windows RRAS servers, you may find that the VPN connection seems to be established, but traffic does not move between the connected networks. Name resolution fails between the networks and hosts are unable to even ping hosts on the remote site network.

The most common reason for this failure is that both sides of the site-to-site network connection are on the same network ID. The solution is to change the IP addressing scheme on one or more networks so that all networks joined by the site-to-site VPN are on different network IDs.

7 Users can't establish IPSec tunnel mode connections from behind some firewalls

Often, the VPN server and clients are correctly configured to use IPSec tunnel mode or L2TP/IPSec NAT-T connection to connect to a remote VPN server and the connection fails. Sometimes, you'll see this happen after a first client makes a successful connection, but subsequent clients from behind the same NAT device fail.

The reason for this problem is that not all IPSec NAT-T VPN servers are RFC compliant. RFC compliance requires that the destination NAT-T VPN server support IKE negotiations from source port UDP 500 and that they be able to multiplex connections from multiple clients behind the same VPN gateway.

The solution to this problem is to contact your VPN server vendor and confirm that their implementation of VPN IPSec NAT-T is RFC compliant. If not, ask if there is a firmware update.

8 Users can't reach some network IDs on the corporate network

Users sometimes report that they can connect to some servers after establishing the VPN connection but not to other servers to which they should have access. When they test the connection, they can't ping the destination server using either a name or IP address.

A common reason for this problem is that the VPN server does not have routing table entries for all network IDs that the VPN clients need to connect to. Users are able to connect to servers that are on-subnet with the VPN server but are unable to connect to network IDs remote from the VPN server. The solution to this problem is to populate the routing table on the VPN server so that it has a gateway address for all network IDs that VPN must be able to connect.

9 Users can't connect to the Internet when connected to the VPN server

Sometimes, users are unable to connect to the Internet after the VPN link is established. Once the VPN link is disconnected, the users have no problem connecting to the Internet.

This problem arises when the VPN client software is configured to use the VPN server as its default gateway. This is the default setting for the Microsoft VPN client software. Since all Internet hosts are remote from the VPN client's location, Internet connections are routed to the VPN server. If the VPN server is not configured to allow Internet connections from VPN clients, the Internet connection attempts fail.

The solution to this problem is to configure the VPN server to allow VPN clients access to the Internet. The Windows RRAS server supports this configuration, and so do many firewalls. Resist the urge to disable the setting configuring the VPN client to use the VPN server as its default gateway, as this enables split tunneling, which is a well-known VPN client security risk.

10 Multiple users connect to the VPN server using the same PPP authentication credentials

A risk for all organizations implementing remote access VPN servers is that users will share username and password information with one another. Most VPN server implementations enable you to not only authenticate users before allowing a VPN connection, but also to authorize a VPN connection. A user might be able to successfully authenticate, but if that user is not authorized to access the network via VPN, the connection request is dropped. If users share credentials, this creates a situation where an unauthorized user can access the network with an authorized user's credentials.

A solution to this problem is to use an extended authentication scheme. For example, you can assign users client (user) certificates for authentication, so that user credentials are never entered by the user. Other schemes include smart card authentication, biometric authentication, and other forms of two-factor authentication.

Additional resources

- TechRepublic's **Downloads RSS Feed** XML
- Sign up for our Downloads Weekly Update newsletter
- Sign up for our Network Administration NetNote
- Check out all of TechRepublic's free newsletters
- "Get connected to a Windows Server 2003 VPN with this step-by-step guide" (TechRepublic article)
- "Join a domain during Windows logon using a VPN client" (TechRepublic download)
- "Support and Configuration Checklists for Small/Midsize Networks" (TechRepublic Download)

Version history

Version: 1.0
Published: August 31, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team