REMOTE ACCESS PROCEDURES

VPN TROUBLESHOOTING GUIDE

Date: 3/20/07/Updated: 02/06/2012
Author: Bruce R. VanTassel

Contents:

Purpose 2
Operating Systems Support: 2
Web page to download VPN client and installation instructions: 2
VPN Support 2
Common Errors and Solutions: 2
Error: Login failed. Please consult the switch log for further information 2
Error: Checking for banner text from <a URL or IP address>" 3
Error: Login failure due to: Remote host not responding 4
Error: Unable to resolve the IP Address of the remote server 4
Error: The secure Contivity VPN connection has been lost. Click Connect to re-establish connection. 4
Error: Maximum number of sessions reached 4
VPN client will not install 5
General Issues and Questions: 5
Nortel VPN running on Windows 7 does not work over AT&T wireless 3G when connected to County APN's, mdc.org, mdcf.miamidade.gov, etc. 5
Experiencing Frequent Drops 5
User cannot access local network resources when VPN is connected. 5
Conflicts with other VPN software 6
Conflicts with file share software 6
Conflicts with other network software 6
Conflicts with malware 6
IPSEC Conflicts 6
Can't browse the internet after establishing a VPN connection 7
Issues related to LAN systems behind a company firewall 7
Cannot connect to devices in SAZ, ISZ, DMZ or another secure network segments after connecting to VPN 8
Outdated router/broadband modem firmware causes VPN problems 8
Remote Desktop/RDP Problems 8
Issues connecting to systems or devices by DNS or Netbios name 8
VPN client software corruption 8
TCP stack corruption 9
NAT traversal 9
General troubleshooting steps 9

Purpose

This document was published to assist users, depot technicians and VPN staff when troubleshooting VPN issues. Common errors are listed along with detailed resolutions.

Operating Systems Support:

Nortel VPN is currently supported only for Windows XP and Windows 2000. Vista support is anticipated in the near future.

Web page to download VPN client and installation instructions:

http://connect.miamidade.gov/NortelVPN.aspx

VPN Support

Tier 1 support is through Depot. Call 305-596-HELP and open up a help desk ticket.

Tier 2 support team is:

- Bruce VanTassel
- Robert Baril
- Keith Adams

Common Errors and Solutions:

Error: Login failed. Please consult the switch log for further information

This generally indicates a problem authenticating to the VPN device or Active Directory. Check the following:

- Verify the correct group ID and group password has been entered into the VPN client: (Menu->Options->Authentication Options).
- Validate that the login account and password is correct.
- Insure that the domain precedes the login account, ie. miamidade\login. *(Note: Ensure the user is using the backslash (\) above the Enter key. Often they use the front slash (/) on the ? key)*

- Fix the following conditions of the user's Active Directory account which will not allow VPN authentication:
  - Expired
  - Locked out
  - User must change password at next logon (should NOT be checked)
  - Disabled
- Insure the Active Directory account is part of a VPN group – *(Note: we have been having a problem with newer accounts using the (ETSD) VPN Access – Contractors, best to use (Remote) VPN Access – Contractors).*

This also could be a symptom of multiple concurrent connection attempts to a static IP VPN account through different VPN devices.

Error: Checking for banner text from <a URL or IP address>"

This error message, followed by a 15 second pause and then the message "The secure Contivity VPN connection has been lost. Click connect to re-establish connection."

One cause is UDP500 traffic is not getting back to the requesting client through a firewall and/or router. If your firewall/router supports IPSec passthrough you must enable IP50, IP51, UDP500 on both the source and destination in order for the client to establish the connection. Some firewalls/routers have a generic setting "Enable IPSec", "Enable IPSec Passthrough", "Allow VPN", or similar setting. Simply turning this on may solve the problem. If you do not have this setting then you will have to program this manually.

Also, make sure that your firewall/router is using the latest software/firmware if you are having further issues getting it to work.

Try turning off local system firewall and anti-virus to see if the OS firewall is trapping the traffic.

Some systems will experience this after resuming from standby or hibernate mode. In such a case a complete reboot has been found to resolve the issue.

LAN systems behind a company firewall using dynamic NAT may need a static NAT entry on the remote firewall to avoid VPN packet corruption.

Error: Login failure due to: Remote host not responding

The VPN Client destination may be incorrect. Verify that the VPN client destination reads vpn.miamidade.gov.

It could be that there is some kind of problem with the DNS settings on the client computer. Ping vpn.miamidade.gov to see if it resolves to a valid IP address. Note that ping will not respond as County security devices block ping responses.

This error could also result if the VPN server or County DNS server is down.

The root cause of this could also be conflicts with other software, (network, maleware, file share, etc), router issues, firewall or network problems. See other relevant sections of this document addressing these.

Error: Unable to resolve the IP Address of the remote server

See error "Login failure due to: Remote host not responding".

Error: The secure Contivity VPN connection has been lost. Click Connect to re-establish connection.

Resolution: Click 'Connect' to re-establish connection. If problem persists follow the following steps:

- Step 1: Check DSL Connection. Disconnect from VPN and attempt to access the Internet.
- Step 2: If you cannot connect to the Internet, contact your Internet Service Provider
- Step 3: Follow other troubleshooting steps in this document.

See also: "Experiencing Frequent Drops"

Error: Maximum number of sessions reached

The user may be attempting to establish more VPN connections than they are allowed.

There may be multiple concurrent connection attempts to a static IP VPN account.

This may indicate the user has been ungracefully disconnected. Wait a few minutes and try again. If this does not resolve the problem, have

the VPN team manually disconnect the user. Make sure keepalives are not disabled.

VPN client will not install

Remove all other VPN clients installed on the system, (see Conflicts with other VPN software).

General Issues and Questions:

Nortel VPN running on Windows 7 does not work over AT&T wireless 3G when connected to County APN's, mdc.org, mdcf.miamidade.gov, etc.

This is not a supported combination. Change the operating system to XP or connect to the public APN, (requires executive management and security office approval).

Experiencing Frequent Drops

Periodic drops are to be expected since VPN connections are established over Internet connections. Changing the status of Disable Keepalives, (Menu->Options->Disable Keepalives) helps in some cases. Sometimes spyware, malware, viruses and other rogue software causes this problem. Also, wireless issues, network driver problems and sporadic broadband connections can result in a poor quality connection, causing VPN disconnects.

User cannot access local network resources when VPN is connected.

Access to local network resources is not available when connected to VPN. This is an unfortunate side effect to VPN. An unsupported work-around is to install virtual PC on the client system, configure a virtual machine, install XP on the virtual machine, install the Nortel Contivity client into the virtual machine and established the VPN connection through the virtual machine. In this way the host client system can access the local network and the virtual machine can access the County network through VPN.

Conflicts with other VPN software

The Nortel Contivity client is incompatible with other VPN clients, including the Cisco VPN Client, Citrix SSL-VPN and others. To connect with the Nortel VPN client, conflicting VPN software must be removed from the system.

Conflicts with file share software

The Nortel Contivity client has been found to sometimes conflict with file share software, including: Limewire, Kazaa, eDonkey, Gnutella, BitTorrent. To connect with the Nortel VPN client, conflicting software must be removed from the system. *(Note: Filesharing software is NOT permitted on the County network. Scans are conducted and if found will quarantine the device until such time as it has been remove and rescanned).*

Conflicts with other network software

The Nortel Contivity client has been found to sometimes conflict with other low level network software, including: AOL software, Cisco VPN Client(s), SSH Sentinel, PGP, Netmotion. To connect with the Nortel VPN client, conflicting software must be removed from the system.

Conflicts with malware

The Nortel Contivity client has been found to sometimes conflict with spyware, viruses and other rogue software. To connect with the Nortel VPN client, conflicting software must be removed from the system.

IPSEC Conflicts

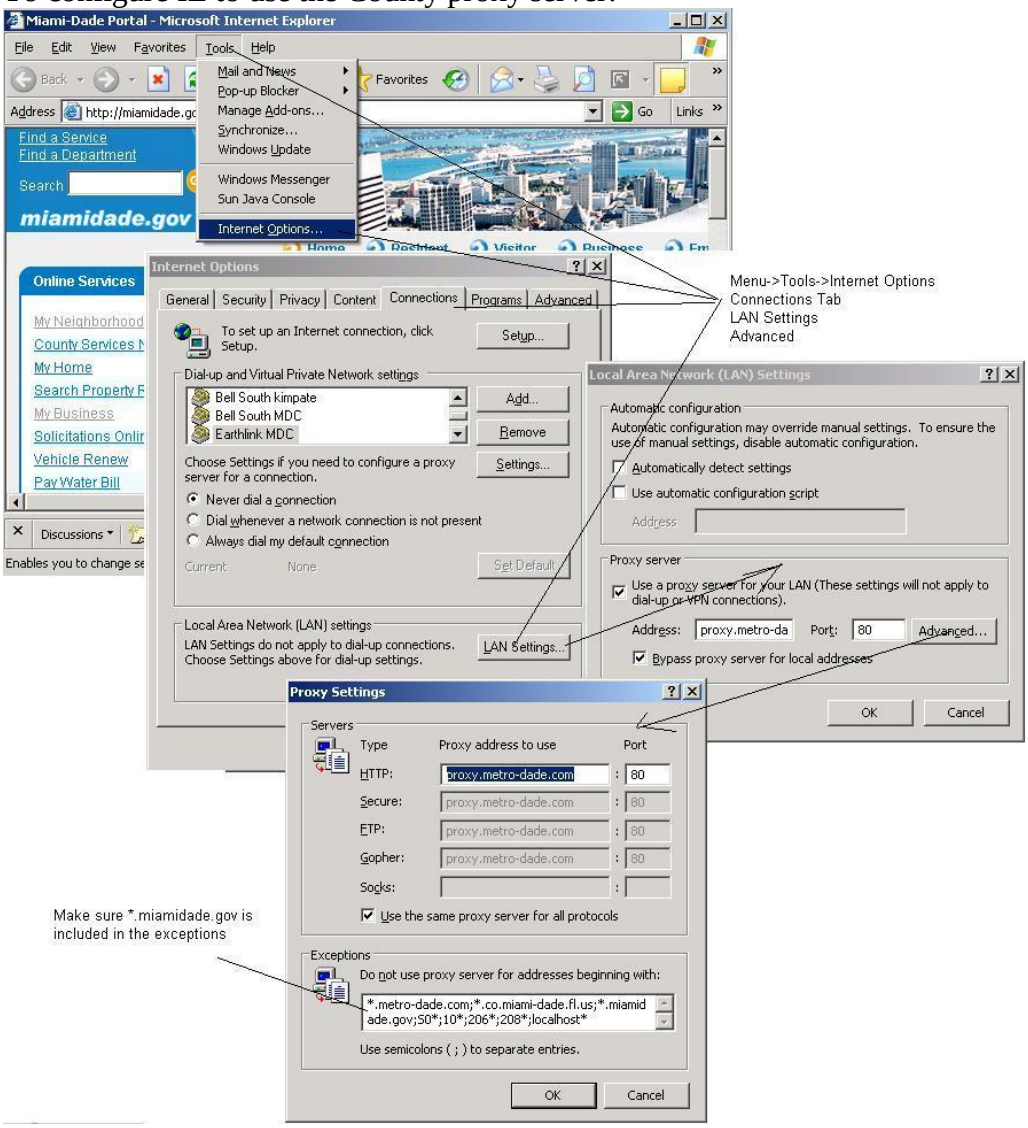
Make sure that the IPSEC service is disabled in your services list. To check this, do the following:

a) Right click My Computer -> Manage
b) Click the + beside 'Services and Applications'
c) Services
d) Look for IPSEC Policy Agent (on Windows 2000) or IPSEC Services (Windows XP)
e) Disable the service if it is not disabled already. (it should be disabled by default).

Can't browse the internet after establishing a VPN connection

Internal sites, (miamidade.gov, intra.miamidade.gov, etc.) can be accessed with or without a proxy configuration. To get out to the internet, you need to configure to use the proxy, (Proxy.miamidade.gov). The simplest thing to do is to have the user remote to their workstation and run IE from there.

To configure IE to use the County proxy server:



Issues related to LAN systems behind a company firewall

See discussion on "Checking for banner text from <a URL or IP address>".

Cannot connect to devices in SAZ, ISZ, DMZ or another secure network segments after connecting to VPN

SAZ and ISZ are restricted network areas and require a static IP address VPN connection along with appropriate firewall rules to allow access. If the user is allowed RDP access and has a County workstation on Metronet which has access to needed systems, a simple solution would be to use RDP to connect remotely to the Metronet workstation and establish the connection to the secured systems from the Metronet workstation.

Outdated router/broadband modem firmware causes VPN problems

Check to see if the user's broadband router is at the latest version. Update the firmware to the latest version if not.

Replacement of DSL/broadband modem sometimes resolves problems.

Remote Desktop/RDP Problems

Most problems can be traced to the Metronet workstation not having RDP turned on. To turn on RDP: Control Panel->System->Remote Tab; Under Remote Desktop, click Allow users to connect remotely to this computer.

Users connecting to RDP need appropriate permissions. To do permit users to RDP to a system, add them to either group “Remote Desktop Users” or Adminstrators.

Issues connecting to systems or devices by DNS or Netbios name

One thing people overlook is that sometimes the domain needs added to the host when establishing a connection, (ie. ibmprd.miamidade.gov)

VPN client software corruption

A VPN connection can get corrupted. This may be resolved by creating and using a new connection: Menu->File->Connection Wizard.

Some issues have been resolved by uninstall and reinstalling the Nortel VPN client software. Make sure any existing installation is uninstalled before installing. Failure to uninstall the old software can lead to serious software conflicts and can corrupt the entire network stack.

TCP stack corruption

Some issues have been resolved by unloading and reloading the TCP stack. To do so, change the NIC properties->uncheck TCPIP, reboot the operating systems, change the NIC properties->check TCPIP, reboot.

NAT traversal

Some issues related to NAT have been resolved by enabling NAT traversal for the VPN account. For County employees using dynamic IP VPN connections, a special group ID, "traverse" has been configured for NAT traversal; contact the VPN team for the group password. For static IP VPN accounts, the individual account can be configured for NAT traversal; contact the VPN team to have it so configured.

If using NAT traversal insure UDP 10001 traffic is allowed to pass through remote firewalls and systems.

General troubleshooting steps

In addition to the information given elsewhere in this document, the following describes general VPN troubleshooting steps:

- First insure that the system has internet access.
- Narrow the source of the problem: The issue may be either with the system, remote router, user account or the DSL line. Actions to narrow the problem: reboot the computer; try logging on to VPN with different domain account; bypass the router and connect directly to the DSL modem; connect the computer to a known working connection; connect a known working computer to the DLS modem/router.
- If the problem is with the computer, some things to try:
    1. Disable firewall and antivirus software.
    2. Uninstall and reinstall the VPN software.
    3. Change the network interface card with a different vendor/model.
    4. Log on as a different local account to see if there may be a profile issue.

5. Look for software that may be interfering with the connection. Anything that might access the network or internet is suspect. We've experience issues with instant messenger software, other VPN software, wireless card drivers, etc.
6. Reinstall the operating system.

- If the problem is with the router:
  1. Check to see if a firmware update is available.
  2. Look to see if there is anything blocking UDP port 500 traffic.
  3. Replace the router.
- If the problem is with the user account:
  1. Insure the account is not disabled, not locked out, has an expired password, etc.
  2. Make sure that account the password is not expired or that the account is not set to force user to change password at next logon.
  3. Check to see that the account is a member of a group allowed VPN access.
  4. The Dial-in tab that remote access is allowed and no callback is selected.
- If the problem is with the DSL line, (highly unlikely, but possible):
  1. Contact the DSL vendor