

# Network Connect

## **Abstract:**

The Network Connect (NC) provides a clientless VPN user experience, serving as an additional remote access mechanism to corporate resources using an IVE appliance. This feature supports all Internet-access modes including dial-up, broadband, and LAN scenarios from the client machine and works through client-side proxies and firewalls that allow SSL traffic over port 443.

## **Overview:**

Network Connect takes all traffic to and from the client and transmits over the secure Network Connect tunnel. The only exception is for traffic initiated by other IVE-enabled features, such as Web browsing, file browsing, and telnet/SSH. If you do not want to enable other IVE features for certain users, create a user role for which only the Network Connect option is enabled and make sure that users mapped to this role are not also mapped to other roles that enable other IVE features.

When Network Connect runs, the client effectively becomes a node on the remote (corporate) LAN and becomes invisible on the user's local LAN. The IVE appliance serves as the DNS gateway for the client and knows nothing about the user's LAN. Users may define static routes on their PCs to continue to access the local LAN while simultaneously connecting to the remote LAN. For security consideration, because the PC traffic goes through the Network Connect tunnel to internal corporate resources, make sure that other hosts within that user's LAN cannot connect to the PC running Network Connect.

## **Configuration:**

To Configure Network Connect, We need to follow the steps below:

1. IVE requires an NC license
2. Add IP address filters and Network Connect Server IP address under, System → Network → Network Connect. As shown below.

Overview	Internal Port	External Port	Hosts	Network Connect										
<p>You may download a stand-alone <a href="#">Network Connect installer</a> for distribution to end-users.</p> <p>Specify IP filters for this IVE to apply to Network Connect IP pools. The IVE assigns IP addresses from the filtered list to clients requesting a Network Connect session. A filter is an IP address/netmask combination. For example: 10.11.0.0/255.255.0.0 or 10.11.0.0/16</p>														
<p><b>IP Address Filter</b></p> <table border="1"> <tr> <td><input type="text"/></td> <td><input type="button" value="Add"/></td> </tr> <tr> <td>*</td> <td><input type="button" value="X"/></td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </table>				<input type="text"/>	<input type="button" value="Add"/>	*	<input type="button" value="X"/>							
<input type="text"/>	<input type="button" value="Add"/>													
*	<input type="button" value="X"/>													
<p>Specify the base (server) IP for the IVE to apply to Network Connect IP pools. This server side IP will be common to all nodes (if clustered). Be careful to choose an IP <u>other</u> than your IVE external/internal IPs.</p>														
<p><b>Network Connect Server IP Address</b></p> <table border="1"> <tr> <td><input type="text" value="10.200.200.200"/></td> <td><input type="button" value="Save"/></td> </tr> </table>				<input type="text" value="10.200.200.200"/>	<input type="button" value="Save"/>									
<input type="text" value="10.200.200.200"/>	<input type="button" value="Save"/>													

### IP address filters explained:

As you see in the above screenshot, we have entered an \* for the IP address filter. For a multi-site cluster deployment, the IP network/sub-network is required to allow the IVE to assign IP addresses from the IP pool corresponding to the defined network. This provides separation and avoids potential routing problems between the client and the backend resources.

For a stand alone or active/passive cluster scenario it is recommended to use \* as shown in the above screenshot.

3. Enable NC for a particular role.

Users → Roles → <RoleName> → General

<input checked="" type="checkbox"/> <b>Network Connect</b>	<a href="#">Options</a>
--	-------------------------

4. Configure the NC options for a particular role.

Users → Roles → <RoleName> → Network Connect

**Split Tunneling Options**

**Split Tunneling Modes**  
Choose the mode for NC split-tunneling

- Disable Split Tunneling**
- Allow access to local subnet**
- Allow access to local subnet with route change monitor**
- Enable Split Tunneling**

**Auto Launch and Upgrade Options**

- Auto-launch Network Connect**  
Use auto-launch to automatically start the Network Connect when users sign in
- Auto-upgrade Network Connect**  
Auto-upgrade Network Connect when users sign in

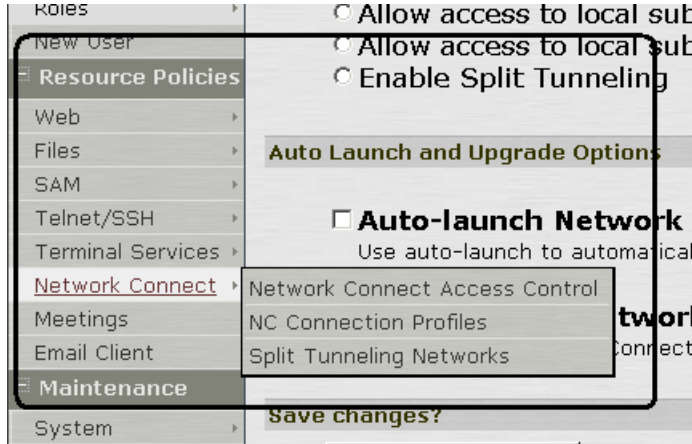
**Save changes?**

***Split Tunneling modes explained:***

- **Disable Split Tunneling:** All network traffic from the client goes through the Network Connect tunnel. When Network Connect successfully establishes a connection to the IVE, the IVE removes any predefined local subnet and host-to-host routes that might cause split-tunneling behavior. If any changes are made to the local route table during an active Network Connect session, the IVE terminates the session.
- **Allow access to local subnet:** The IVE preserves the local subnet route on the client, retaining access to local resources such as printers. The local route table may be modified during the Network Connect session.
- **Allow access to local subnet with route change monitor:** Once a Network Connect session starts, changes to the local route table terminate the session. This option retains access to local resources such as printers.
- **Enable Split Tunneling:** This option requires that you specify the Network Connect networks to which traffic must be routed through the IVE by defining Split Tunneling resource policies (see Write a Network Connect split-tunneling networks resource policy). Network Connect modifies routes on clients so that traffic meant for those networks goes to Network Connect and all other traffic

5. Resource Policies related to Network Connect

As part of NC configuration we need to configure NC Resource Policies. They include, *NC Access Control*, *NC Connection Profiles* and *Split Tunneling Networks*.



a. Network Connect Access Control

Resource Policies → Network Connect → Network Connect Access Control → New Policy...

**Bhaskar NC**

General Detailed Rules

\* Name:  Required: Label to reference this policy.

Description:

Resources

Specify the resources for which this policy applies, one per line.

\* Resources:  Examples:  
tcp://\*:1-1024  
tcp://\*:80,443  
udp://10.10.10.10/24:\*  
icmp://10.10.10.10/255.255.255.0  
10.10.10.10/24

Roles

Policy applies to ALL roles  
 Policy applies to SELECTED roles  
 Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

Action

Allow access

**An Important note on this ACL:** Since Network Connect provides L-3 access, it is recommended to fine tune this and provide access to specific resources to the backend corporate servers/applications based on IP address or application ports. See the examples below for specific ACLs

tcp://10.43.10.0/24:\* → allows access to backend server from 10.43.10.0-254 on all ports

tcp://\*:80,21,23 → allows access to http, ftp and telnet traffic to backend servers

b. NC Connection Profiles

In the Web console, choose **Resource Policies → Network Connect → NC Connection Profiles → <click New Profile>**

Configure the following:

- An arbitrary name to label this policy.
- A description of the policy (optional).
- In the **IP address pool** section, specify IP addresses or a range of IP addresses for the IVE to assign to clients that run NC.

**Note:**

***Multi-site cluster: If you are running a multi-unit cluster across a LAN or a WAN, make sure that the IP pool contains addresses that are valid for each node in the cluster - configure an IP filter for each node to apply to this IP pool.***

***Choosing IP pools: It is always advised to choose IP addresses meant for intranet purposes such as: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 (generally tagged as private address pools). Since these IP addresses will be used by virtual hosts on the network (NC clients), we have to make sure that the IP pools are unique within the corporate network and doesn't conflict with any system/servers within the corporate network.***

***Do not use IP address from these ranges (NC pools) in configuring the NC Server IP address under System → Network → Network Connect.***

In the **Network Connect proxy server configuration** section, select one of the following options:

• **No proxy server**

Select this option if the new profile requires no proxy server.

• **Automatic** (PAC file on another server)

Specify the IP address of the server on which the PAC file resides.

• **Manual configuration**

Specify the IP address of the server and give the port assignment.

In the **Custom DNS settings** section, select the checkbox to override standard DNS settings (otherwise, DNS settings configured in the IVE's network settings will be used). Then configure the following:

**Primary DNS**

Provide the IP address for the primary DNS.

**Secondary DNS**

Provide the IP address for the secondary DNS.

- c. Split Tunneling Networks  
Internal networks are specified under this tab for which the IVE handles traffic.
6. Cluster Considerations:  
If you are running a multi-site cluster and each node utilizes different network addresses, you need to the following:
- a) Configure an IP Address Pool policy that accounts for the different network addresses used by each node in the cluster.
  - b) For each node in the cluster, specify an IP filter that filters out only those network addresses available to that node.
  - c) Create a static route on your router pointing to the IP address of the internal port of each cluster node as the gateway to the subnet as specified in above step b.

## Troubleshooting

### Collecting NC Logs

For 4.0 and previous version:

Neosetup.txt, neotrace.txt are in \program files\neoteris\network connect\  
rasphone.pbk is in %ALLUSERSPROFILE%\Application  
Data\Microsoft\Network\Connections\Pbk\ or %windir%\system32\ras\

For 4.1:

Neosetup.txt, neotrace.txt, ncsvc.log are in \program files\neoteris\network  
connect\

rasphone.pbk is in

%ALLUSERSPROFILE%\Application Data\Microsoft\Network\Connections\Pbk\  
or %windir%\system32\ras\

For 4.1.1 or above versions:

Neosetup.txt, ncsvc.log \program files\neoteris\network connect\

neotrace.txt

%userprofile%\Application Data\Neoteris\Network Connect\Logs\

For 4.2 it will be in %userprofile%\Application Data\Juniper  
Networks\Network Connect\Logs\

rasphone.pbk  
%ALLUSERSPROFILE%\Application Data\Microsoft\Network\Connections\Pbk\  
or %windir%\system32\ras\  
Note: Neotrace.txt is in \document and setting\”log in user”\application  
data\neoters\network connect\logs”.

To get neotrace.txt and ncsvc.log, Client Side logging for NC should be enabled with IVE admin “security”->”client logging”.

Collect “ipconfig /all” and “route print” outputs before and after NC connected, especially if there is disconnect problem.

If there is modem installation problem, such as NC is not attached to “Standard” modem, please collect %windir%\inf\mdmgen.inf. If there is not such file, NC won’t work. Except with 4.2, see next for 4.2 modem specific problem.

With 4.2, NC uses “Standard Juniper Modem” to replace the localized “Standard 33600 bps Modem”. NC will not require the PC to have %windir%\inf\mdmgen.inf because NC will package its own modem file. With the new modem, NC will only delete one instance; therefore, NC will remove previous installed “Standard 33600 bps Modem” and “Standard Juniper Modem” first; and will then install a new “Standard Juniper Modem”. If Device Manger shows there are “Standard 33600 bps Modem” and/or “Standard Juniper Modem” after NC installs, NC may not work.

## Common NC Errors

1. If NC connecting dialog pops up for a while (you can see hundred or more send and receive bytes) then disconnect immediately, check whether there is enough IPs in the IVE’s IP pool and whether IP filter is set correctly. If connecting to a cluster, make sure both nodes have IP filter set.

**2. If NC reports “Ras error”, if the Ras call back error code is as follows (look for “UI: Dial callback, unMsg = 52429, rasconnstate = 0, dwError = xxx” in neotrace.txt):**

### **680 – no dial tone**

This could be due to no “standard” modem is installed due to no mdmgen.inf.  
Fix: copy a mdmgen.inf from a similar system.

Or NC does not install the right localized “standard” modem due to no support for the locale or NC can’t detect the right locale.

Fix: make sure the locale is supported. If it’s supported, file a bug. If it is not, manually switch the modem from “Network Connect” dial up entry and talk to marketing or sales to add support with next NC release.

### **797 – connecting device not found**

VCP (virtual com port) is not functioning or it's used by another program.

MS TAPI modules is not installed.

Check if there is an "accept incoming connection" entry in Network Control Panel

### **692 – hardware failure in the modem**

VCP (virtual com port) is not functioning or it's used by another program. Run takeport.exe or takeport41.exe to check this. If the message is "failed 2", it means either the com port was uninstalled or there's problem with NC installation.

Here are links for takeport.exe and takeport41.exe:

<http://download.juniper.net/software/ive/docs/supplemental/tac/kb/nc/takeport40.exe>  
<http://download.juniper.net/software/ive/docs/supplemental/tac/kb/nc/takeport41.exe>

### **720 – Protocols (TCP/IP) not config**

NC started before system setting up protocol configuration for NC connection. This can be due to a timing problem. It happens when NC is installed the first time and is started before the TCP/IP configuration is set up by the system. This can happen when a user manually removes a related Registry entry. When this happens wait a minute or two and start NC again. If it still doesn't work, uninstall and reinstall NC or try to disable and re-enable TCP/IP for the NC connection.

Also check out the registry entry according to the Microsoft instruction:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;123298>

Please know if there are Network Components, such as firewall or VPN installed, reinstalling TCP/IP could break dial-up connections which include NC. If this has happened, refer to the above link for a potential fix.

When reinstalling TCP/IP, all third party network software, including NC should be removed first. Then reinstall them after TCP/IP is reinstalled.

## **PPP Tracing**

The RRAS service should be running. From a command prompt, run "netsh ras set tracing ppp enable". To stop tracing, run "netsh ras set tracing ppp disable".

In XP, the commands are "netsh set tracing ppp enable" and "netsh set tracing ppp disable".

## **How to Get Temporary Proxy PAC file that NC Created during the Session:**

If proxy is detected and its option is supported by NC, NC will create a temporary proxy PAC file during the session. The PAC file will be removed after NC exits. It should be copied to another file name or directory before NC exists.

For 4.1.1 or lower versions, it will be under C:\program files\neoteris\network connect\instantproxy.pac

For 4.2 it will be %userprofile%\Application Data\Juniper Networks\Network Connect\instantprxoy.pac.

## **What's not supported in Proxy:**

No proxy support for split tunnel enabled.

If there's an active Wininet connection, such as Meeting or WSAM, Prxoy configuration cannot be changed. Therefore, NC will not work.

4.1 supports static proxy setting with the box "Use proxy for all services" checked. It does not support different proxy setting for different services even though they are the same proxy server. It dose not support proxy exception list and "local subnet bypass"

4.1.1 supports static proxy setting with the box "Use proxy for all services" checked. It does not support different proxy setting for different services even though they are the same proxy server.

4.1R1 dose not have the above restriction.

When proxy is not working, besides the usual log files, we should collect the temporary PAC file NC created to check whether there's bug in the PAC file. The file should be collected before exiting NC. The PAC file is in:

%userprofile%\Application Data\Neoteris\Network Connect\instanceproxy.pac For 4.2 it will be in %userprofile%\Application Data\Juniper Network\Network Connect\instanceproxy.pac.

Prior to 4.2, NC does not support proxy between IVE and the internal resources (internal proxy). The proxy support before 4.2 is for proxy server between NC client and IVE (external proxy). NC 4.2 does not support "internal proxy" and "external proxy" at the same time.

## **Proxy support developments in IVE 5.x**

(Though this section is not relevant here as this document is purely meant for IVE OS up to 4.X, we are providing here to give a quick knowledge on proxy support enhancements with 5.x)

Network Connect provides support for remote clients using a proxy server to access the Internet (and the IVE via the Internet), as well as clients who do not need a proxy to access the Internet, but who access resources on an internal network through a proxy. Network Connect also provides support for clients accessing a Proxy Automatic

Configuration (PAC) file that specifies client and IVE proxy settings enabling access to Web applications.

To address these varying methods of proxy implementation, Network Connect temporarily changes the proxy settings of the browser so that only traffic intended for the Network Connect session uses the temporary proxy settings. All traffic not intended for the Network Connect session uses the existing proxy settings.

Whether split-tunneling is enabled or disabled, the IVE supports the following proxy scenarios:

- Using an explicit proxy to access the IVE
- Using an explicit proxy to access internal applications
- Using a PAC file to access the IVE
- Using a PAC file to access internal applications

When split-tunneling is enabled on the IVE, Network Connect manages proxy settings in one of the following ways, depending on the method with which the proxy is implemented:

- For remote clients using a proxy server to access the Internet, all HTTP requests generated by the browser and intended for the IVE (including NCP transport traffic) go through either an explicit proxy or a PAC file accessed by the remote client. Because the presence of an explicit proxy or access to a PAC file is already provisioned on the client-side, the client sets up the local, temporary proxy before attempting to establish a Network Connect session.
- For remote clients using a proxy to access corporate resources on a corporate network, yet still able to connect directly to the Internet without a proxy, Network Connect identifies the proxy settings on the client even though the proxy server is not reachable until Network Connect establishes a connection. Once Network Connect establishes a connection, it then creates the local, temporary proxy.
- When a remote client accesses a pre-configured HTTP-based PAC file, the client cannot access the PAC file until after Network Connect establishes a session connection. After Network Connect establishes a connection, the client accesses the PAC file, includes the PAC file contents in the local, temporary proxy, and then refreshes the browser proxy setting.