Quick Note 4

TCP/UDP port re-direction through NAT using “Static NAT Mappings” or a firewall script. (Port Redirection)

Digi Technical Support

February 2016
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Network Diagram</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Network Address Port Translation (NAPT)</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Nat Mappings</td>
<td>5</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Save config</td>
<td>6</td>
</tr>
<tr>
<td>Figure 5</td>
<td>VNC Viewer setup 1</td>
<td>6</td>
</tr>
<tr>
<td>Figure 6</td>
<td>VNC Viewer setup 2</td>
<td>6</td>
</tr>
<tr>
<td>Figure 7</td>
<td>setup the Firewall</td>
<td>7</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Turn on the firewall</td>
<td>8</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Save the config</td>
<td>8</td>
</tr>
<tr>
<td>Figure 10</td>
<td>VNC Server 1</td>
<td>9</td>
</tr>
<tr>
<td>Figure 11</td>
<td>VNC Server 2</td>
<td>9</td>
</tr>
</tbody>
</table>
1 VERSION

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
<tr>
<td>2.0</td>
<td>Updated and rebranded</td>
</tr>
<tr>
<td>2.1</td>
<td>Updated screenshots and instructions for new web interface, rebranding (Feb 2016)</td>
</tr>
</tbody>
</table>

1.1 Corrections

Requests for corrections or amendments to this Quick Note are welcome and should be addressed to: tech.support@digi.com

Requests for new Quick Notes can be sent to the same address.

2 CONFIGURATION OPTIONS & SCENARIO

In this example scenario two re-direction/forwarding options will be configured. 1 NAT (Network address translation) and 1 NAPT (Network address and port translation). PPP 1 will be used for the Internet connection. 2 internal servers are running VNC on port 5900 and the requirement is to be able to connect to each from an external location over the public Internet. Server 1 has a LAN IP address of 10.1.51.2 and Server 2 has a LAN IP address of 10.1.51.3. The same process can be applied to any TCP or UDP traffic that uses a specific port number.

![Network Diagram](image)

Figure 1: Network Diagram

There are 2 ways of achieving the same result. The IP Port Forwarding/Static NAT Mappings option in the web interface is very simple to configure and the functionality is fine for most users. However, the firewall can also be used to re-direct traffic and is much more flexible in what can be achieved.

Use one method only either:

- Configuration using IP Port Forwarding/Static NAT Mappings
- Configuration using the firewall
3 CONFIGURATION USING STATIC NAT MAPPINGS

Configuration - Network > Interfaces > Advanced > PPP 0-9 > PPP 1

On the PPP interface that will be used for the incoming connection (e.g. PPP 1), scroll to the bottom of the screen and change the NAT mode to 'IP address and Port' to allow for port translation as well as address translation.

If the PPP interface is currently up, it will need to be dropped and re-connected before the above change will take effect.

3.1 Configure the NAT mapping

Server 1. Traffic with a destination port of 5900 will be forwarded to 10.1.51.2 but the destination port remains unchanged at 5900.

Server 2. Traffic with a destination port of 5901 will be forwarded to 10.1.51.3 and the destination port is changed to 5900.

NOTE: Port numbers are both TCP and UDP.
Port Redirection

3.2 Save your config changes to profile 0

![Administration - Save configuration](image)

Save current configuration to Config 0 (power up) ▼
Save

Save all configuration. This includes the following
- Save the current configuration to config 0
- Save the current firewall
- Save all registers on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

![Save All](image)

Figure 4: Save config

3.3 Test

Check your forwarding is working to both servers.

Server 1 – NAT

Server 2 – NAPT

![VNC Viewer setup 1](image)

![VNC Viewer setup 2](image)

Figure 5: VNC Viewer setup 1

Figure 6: VNC Viewer setup 2
4 CONFIGURATION USING THE FIREWALL

Browse to Configuration - Security > Firewall

Add in the following lines:

Rule 2: Server 1 NAT
pass in break end on ppp 1 from any to addr-ppp 1 port=5900 -> to 10.1.51.2 inspect-state

Rule 4: Server 2 NAPT
pass in break end on ppp 1 from any to addr-ppp 1 port=5901 -> to 10.1.51.3 port=5900 inspect-state

Rule 6: Allow all other traffic to pass normally
Pass break end

Save the firewall rules by clicking on the Save button.

For a full description on the firewall usage please see the relevant section in TransPort User Guide.
4.1 Enable the firewall on the PPP interface

Configuration - Network > Interfaces > Advanced > PPP 0 – 9 > PPP 1

- Enable NAT on this interface
- IP address
- IP address and Port
- NAT Source IP address:
- Enable IPsec on this interface
- Enable the firewall on this interface

Figure 8: Turn on the firewall

4.2 Save your config changes to profile 0

Administration - Save configuration

Save current configuration to Config 0 (power up) ▼

Save all configuration. This includes the following:
- Save the current configuration to config 0
- Save the current firewall
- Save all sregisters on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

Save All

Figure 9: Save the config
4.3 Test

Check your forwarding is working to both servers.

Server 1 – NAT

Server 2 – NAPT

Figure 10: VNC Server 1

Figure 11: VNC Server 2