How to use VNC and RDP via SSL VPN

To access the desktop of a remote PC which is behind a NATed router, you have two options. One is by opening relative ports (e.g. TCP 5900 for VNC or TCP 3389 for RDP) on the router, the other is by connecting a VPN tunnel to the router. The former is easy but not secure as the router is exposed to the whole Internet. Furthermore it’s hard to add security by using firewall policies to restrict the accessing IP addresses for mobility users. As for the latter method based on VPN connection, it provides security by requiring you to build a tunnel to the router before accessing the internal computers and the tunnel may be encrypted. There are three types of VPN connection:

- Connect a tradition VPN connection to the office, such as PPTP, L2TP or IPSec.
- Connect a SSL Tunnel or SSTP connection to the office.
- Connect a SSL VPN to the office.

With the above said method 1 and 2 you have full access to the whole office network, whereas with the method 3 you will be restricted to specific applications. Here we will introduce how to use VNC and RDP to access the desktop of a remote computer via SSL VPN.

What is VNC and RDP over SSL VPN?

VNC stands for Virtual Network Computing. It is a remote control software which allows you to view and interact with one computer (the "server") using a simple program (the "viewer") on another computer anywhere on the Internet.

Remote Desktop Protocol (RDP) is a protocol designed for secure communications in networks using Microsoft Terminal Services.

Vigor2950 now supports VNC and RDP applications and acts as VNC/RDP client. You can connect a computer to Vigor2950 via SSL VPN by using a web browser, such as IE or Firefox, then access the desktop of a computer connected behind Vigor2950 and running the VNC or RDP server. The scenario is illustrated below.
Behind Vigor2950, there are two computers with IP addresses 192.168.1.10 and 192.168.1.11. They are running VNC server and RDP server respectively. Below we will introduce how to setup Vigor2950 for SSL VNC/RDP application and how to connect SSL VPN to use this feature by following the sections listed below:

- Setup Vigor2950 for SSL VNC/RDP Application.
- Connecting SSL VPN and using VNC Application with IE browser.
  Connecting SSL VPN and using RDP Application with IE browser.
- Connecting SSL VPN and using VNC/RDP Application with Firefox.
- Troubleshooting.

**Setup Vigor2950 for SSL VNC/RDP Application**

1. Go to the SSL VPN >> SSL Application page and setup profiles.

   ![SSL Application page](image)

   2. Here we create two profiles with index 2 and 4.

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Host Address</th>
<th>Service</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Samba 11</td>
<td>\192.168.1.11\MAVUAL</td>
<td>Samba</td>
<td>v</td>
</tr>
<tr>
<td>2.</td>
<td>vnc100</td>
<td>192.168.1.10:5900</td>
<td>VNC</td>
<td>v</td>
</tr>
<tr>
<td>3.</td>
<td>Samba-10</td>
<td>\Draytek1111</td>
<td>Samba</td>
<td>v</td>
</tr>
<tr>
<td>4.</td>
<td>rdp</td>
<td>192.168.1.11:3389</td>
<td>RDP</td>
<td>v</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>10.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
3. In profile #2, setup the following items for VNC server 192.168.1.10.

<table>
<thead>
<tr>
<th>Profile Index : 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Application Service</td>
</tr>
<tr>
<td>Application Name</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Scaling</td>
</tr>
</tbody>
</table>

Note: Samba Path format must be entered as \ip\directory or \\Computer Name\directory.

**Application Name:** Name the profile. It’s local significant.

**Application:** Select Virtual Network Computing (VNC).

**IP Address:** Enter the IP address of the VNC server.

**Port:** Setup the port of the VNC server. By default it is 5900. Make sure it is consistent with the server’s setup.

**Scaling:** Adjust the size of the window in which remote desktop is presented. There are 3 options available: 60%, 80% and 100%. In this example we select “80%”.

4. In profile #4, setup the following items for RDP server 192.168.1.11.

<table>
<thead>
<tr>
<th>Profile Index : 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Application Service</td>
</tr>
<tr>
<td>Application Name</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Screen Size</td>
</tr>
</tbody>
</table>

Note: Samba Path format must be entered as \ip\directory or \\Computer Name\directory.

**Application Name:** Name the profile. It’s local significant.

**Application:** Select Remote Desktop Protocol (RDP).

**IP Address:** Enter the IP address of the RDP server.
Port: Setup the port of the RDP server. By default it is 3389. Make sure it is consistent with the server’s setup.

Screen Size: Adjust the resolution of the window in which remote desktop is presented. There are 3 options available: 1024*768, 800*600 and 680*480. In this example we select “800*600”.

5. Create an account first. Open SSL VPN >> User Account and access into the VPN accounts setup page. The username and password is polo/polo. For security consideration, you’d better uncheck the other VPN types and just enable the services which the user is allowed to access.
6. If you don’t want to use the standard TCP 443 port for the SSL VPN connection, please go to the SSL VPN >> General Setup page and change the port as follows. Here we change it to 4443.

![SSL VPN General Setup](image)

<table>
<thead>
<tr>
<th>Port</th>
<th>4443</th>
<th>(Default: 443)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Certificate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Encryption Key Algorithm</td>
<td>High - AES (128 bits) and 3DES</td>
<td>Low - DES</td>
</tr>
<tr>
<td></td>
<td>Default - RC4 (128 bits)</td>
<td></td>
</tr>
</tbody>
</table>

Note: The settings will act on all SSL applications.

![OK Cancel](image)

**Connecting SSL VPN and using VNC Application with IE browser.**

1. Open the IE browser, and go to the following URL: [https://172.17.1.53:4443](https://172.17.1.53:4443)

2. Internet Explorer 6 will display the following security alert stating that the security certificate is valid but is not from a known source. Please accept the certificate with confidence by pressing the Yes button.

![Security Alert](image)
Internet Explorer 7 will display the following security alert stating that the security certificate is valid but is not from a known source. Please select the *Continue to this website (not recommended)* choice.

3. In the login window please input the username and password.
4. If login successfully, you will see a window like the one shown below. Press **SSL Application**.

5. This page will list all available links to access the VNC/RDP servers for this account.
6. Pressing the Connect link for “vnc100”, you will get a Connection Status window and a Security Information warning window as shown below. Please press Yes anyway.

7. If you’ve already installed the Sun Java Runtime Environment edition 5 or higher on your system, please jump to step 9. Otherwise, you will be prompted to install ‘Java Plug-in 1.5’ which is Sun Java Runtime Environment edition 5. Please click it and select Install ActiveX Control...
8. Press **Install** button.

9. Wait for the browser to download the Java tool.
10. Press the **Run** button to install the Java Runtime Environment edition 5.

![Java(TM) 2 Platform Standard Edition binary - Security Warning](image)

11. After the tool is installed successfully, it is shown in the task tray.

![Java(TM) 2 Platform](image)

12. Turn off IE browser then turn it on again. Repeat the steps 1 through 6.

13. You will get the following window showing a bar indicating **Press SPACEBAR or ENTER to activate and use this control**. Mouse clicking the white table in the window or pressing the SPACEBAR/ENTER button anyway.

![Press SPACEBAR or ENTER to activate and use this control](image)
14. Depending on your Java Runtime Environment edition number, you may get different warning windows as figures shown below. **Note: You must press the Yes button within 5 seconds when this warning window pops up.**

Warning window for edition 5.


15. Then a new window pops up showing the connection status.
16. If the connection is established successfully, you will get the following login window.

![VNC Authentication Window]

17. Enter the password for entering the VNC server. The desktop is shown in the window as figure shown below.

![Desktop Screen]
Connecting SSL VPN and using RDP Application with IE browser

The steps from 1 through 14 are the same as VNC application.

15. If you are using Java Runtime Environment edition 5, you may be prompted with another warning window as figure shown below. Press Yes.
16. You will get the login window as figure shown below. It is a bit different from the VNC window.

17. Do not close below window before RDP session is terminated.
Connecting SSL VPN and using VNC/RDP Application with Firefox

The steps for firefox is similar with IE. The only difference is that you must install Java Runtime Environment manually before connecting the VNC/RDP.

Troubleshooting

- If you have installed Java Runtime Environment edition 6 but still can’t establish the connection, please make sure you have disabled “Use TLS 1.0” in the Java Control Panel as figure shown below.
If you get the following error warning window, please close the browser completely. Next, open the browser again and reconnect the SSL VPN. Please make sure you click the Yes button quickly as described in step 10 in Part 2A. Connecting SSL VPN and using VNC Application with IE browser.