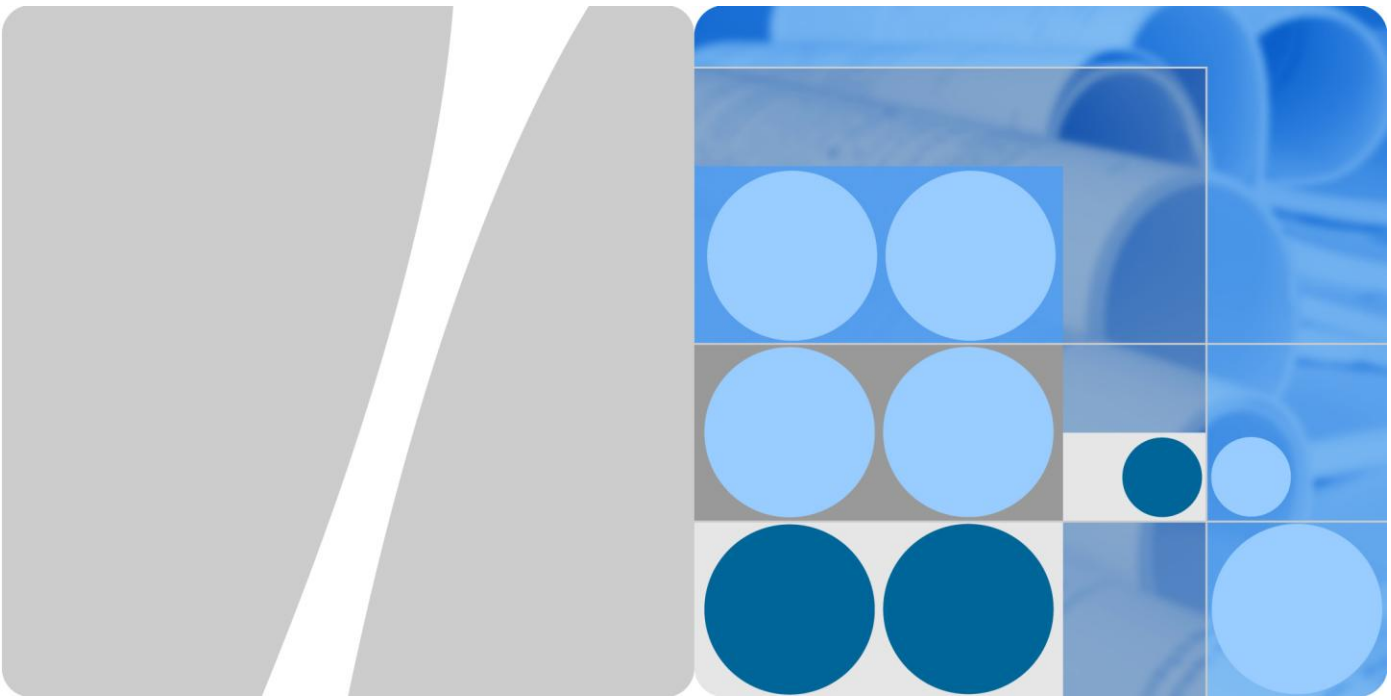


eSpace UC

SVN Configuration Case

Issue 01

Date 2012-07-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Configuration Scenario

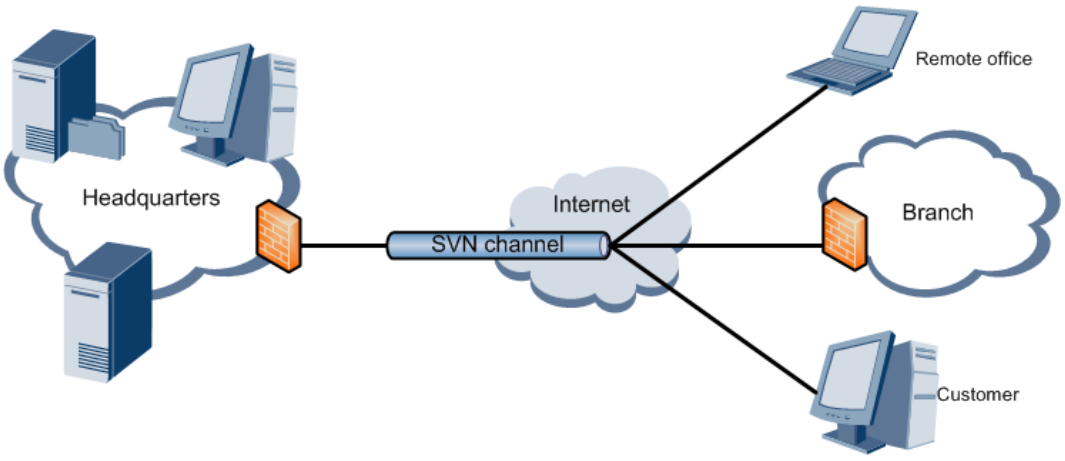
About This Chapter

This topic describes the SVN configuration scenarios.

1.1 Configuration Objective

The objective of configuring the SVN is to establish a secure and encrypted channel between an enterprise's network and its external networks over Internet, as shown in Figure 1-1.

Figure 1-1 SVN transmission channel



Network data is encapsulated by SSL or UDP according to the transmission protocol and then transmitted through the SVN channel. In this way, data can be transmitted in secure and encrypted manner even in complicated network conditions.

1.2 Networking

An SVN device is usually deployed between a firewall or switch and an internal server at the network ingress or egress.

An SVN device can be connected to a firewall or switch through only one network port, as shown in Figure 1-2. It can also be connected to a firewall and a switch through two network ports, as shown in Figure 1-3.

Figure 1-2 SVN single-connection

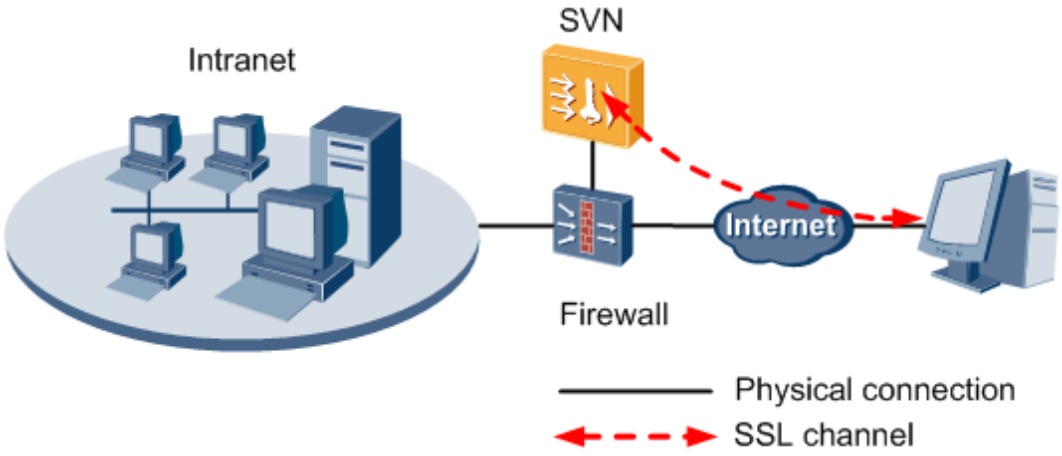
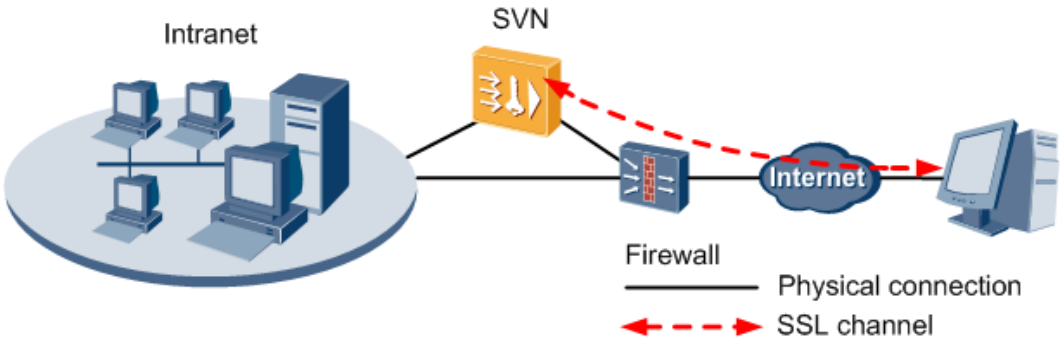


Figure 1-3 SVN dual-connection



1.3 Parameter Settings

Table 1-1 describes the parameter settings for SVN.

Table 1-1 Parameter settings

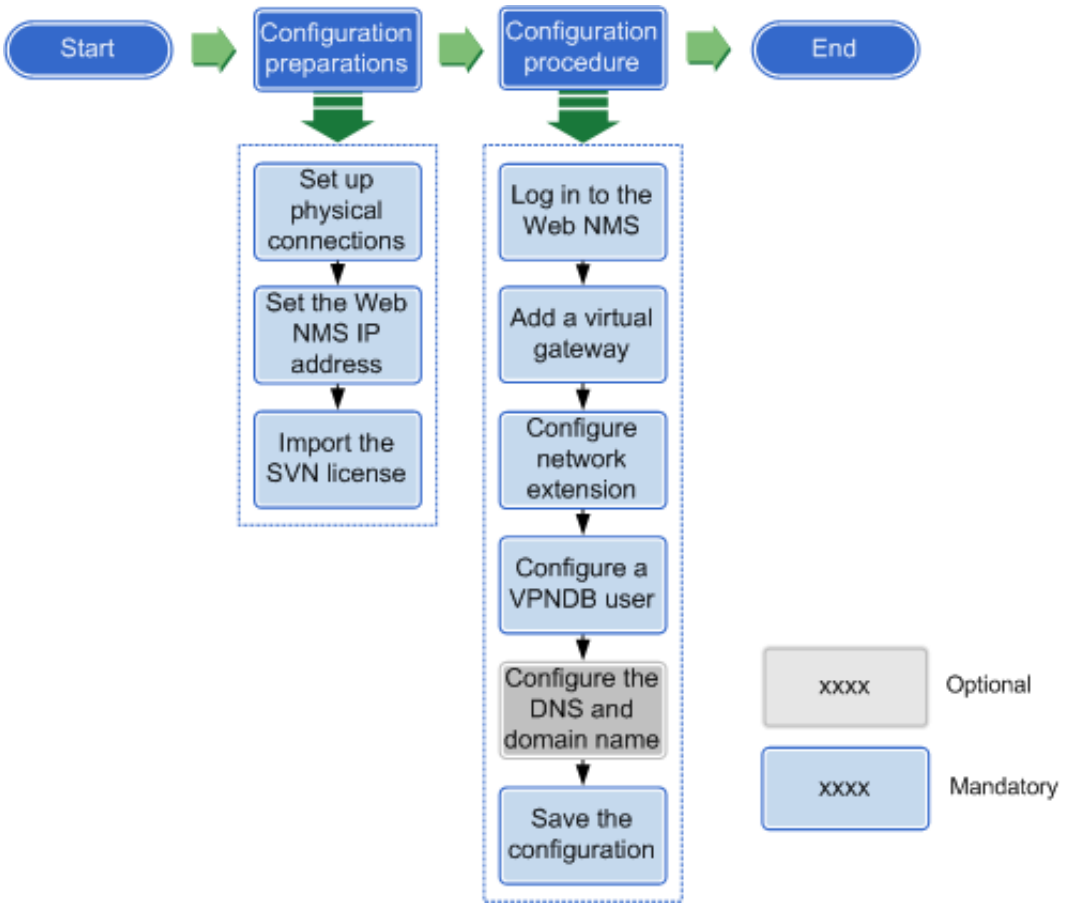
Configuration Item	IP Address	Subnet Mask	Gateway IP Address
External SVN IP	11.11.11.1	255.255.255.0	11.11.11.1

Configuration Item	IP Address	Subnet Mask	Gateway IP Address
address			
Internal SVN IP address	192.162.1.5	255.255.255.0	192.162.1.1
IP address of the web-based network management system (Web NMS)	192.162.1.5	255.255.255.0	192.162.1.1
Virtual IP address pool	192.162.1.10~192.162.1.250	255.255.255.0	192.162.1.1
Virtual gateway IP address	11.11.11.1	255.255.255.0	-

2 Configuration Process

This topic describes the process of configuring SVN. SVN3000 is used as an example. Figure 2-1 shows the configuration process.

Figure 2-1 Configuration process



3 Preparations for the Configuration

About This Chapter

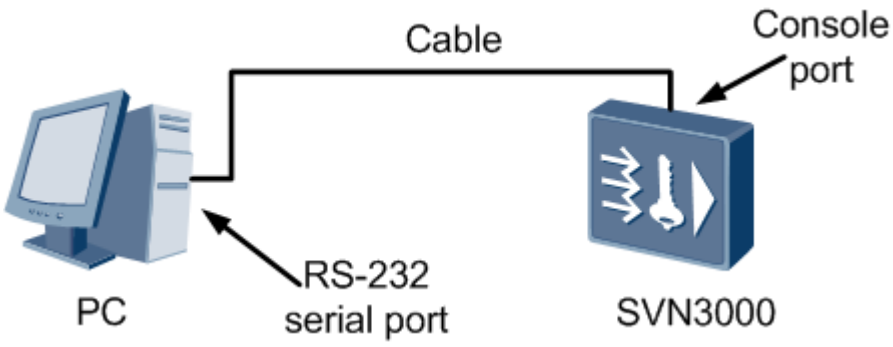
3.1 Setting Up Physical Connections

SVN3000 provides an EIA/TIA-232 asynchronous serial port, that is, the console port. Users can configure SVN3000 through this port.

Procedure

Step 1 Use a cable to connect the PC's RS-232 serial port to the SVN3000's console port, as shown in Figure 3-1.

Figure 3-1 Console port connection



Step 2 Connect to SVN3000 using the HyperTerminal on the PC.

Set parameters according to Table 3-1. The HyperTerminal in the Windows XP is used as an example.

Table 3-1 Configuring parameters on the HyperTerminal

Parameter	Setting	Reference
Bits per second	9600	-
Data bits	8	-
Parity	-	-
Stop bits	1	-
Flow control	-	-
Emulation	VT100	In the **HyperTerminal** window, choose **File** > **Properties** > **Setting**.
User name and password	admin/Admin@123	-

----End

3.2 Setting the IP Address

To configure SVN, you must set its IP address and log in to the Web NMS.

Procedure

Step 1 Run the **system-view** command. The system view is displayed.

Step 2 Run the **interface GigabitEthernet** *interface-number* command. The Ethernet interface view is displayed.

In the command, *interface-number* indicates an SVN interface, such as interface 0/0 or 0/1.

NOTE
The Ethernet interfaces on SVN5300 are 0/0/0 and 0/0/1.

Step 3 Run the **ip address** *ip address net-mask* command to set the interface IP address.

In the command, *ip address* indicates an IP address and *ip address net-mask* indicates a subnet mask.

Step 4 Run the **quit** command to return to the system view.

Step 5 Run the **web-manager ip address** *ip-address***[port** *port-number***]** command to set the SVN interface's IP address as the Web NMS IP address.

In the command, *port-number* indicates the port number for logging in to the Web NMS.

----End

Example

Set the following parameters as planned:

1. Run the **interface GigabitEthernet 0/0** command. The view of Ethernet interface 0 is displayed.
2. Run the **ip address 11.11.11.1 255.255.255.0** command to configure the external IP address of the interface.
3. Run the **interface GigabitEthernet 0/1** command. The view of Ethernet interface 1 is displayed.
4. Run the **ip address 192.162.1.5 255.255.255.0** command to configure the internal IP address of the interface.
5. Run the **quit** command to return to the system view.
6. Run the **web-manager ip address 192.162.1.5** command to set the IP address of the Web NMS to the internal IP address.

NOTE
- Users can connect to SVN3000's Web NMS through a maximum of two interface IP addresses.
- The default port number for logging in to the Web NMS is 443. If another port number is specified when you run the **web-manager ip address** *ip-address***[port** *port-number***]** command, you need to provide the port number in https://*x.x.x.x*:*port* to log in to the Web NMS.

After the IP address of the Web NMS is set, you can log in to the Web NMS using this IP address.

CAUTION
Ensure that the specified port, usually port 443, is enabled for SVN3000 on the firewall.

3.3 Importing the System License

When the system license file is not imported, there are only two virtual gateways and 10 users. Therefore, you are advised to import the system license before using the Web NMS to configure SVN.

Downloading the System License File

Step 1 Place the system license file to the FTP server.

Step 2 Log in to SVN3000 using the HyperTerminal.

Step 3 Run the **ftp** *host-ip* command. The FTP client view is displayed.

In the command, *host-ip* indicates the IP address of the FTP server.

Step 4 Enter the user name and password of the FTP server.

Step 5 Run the **dir** command to view the directory of the FTP server.

Step 6 Run **get** *source-file-name* **[***filepath***]** command to download the license file to SVN3000 through FTP.

In the command, *source-file-name* indicates the system license file name, and *filepath* indicates the path of the system license file on SVN3000.

----End

Activating the System License

CAUTION

When a license file is updated, the old license file will be invalid. For example, if the old license file supports 10 virtual gateways and 20 concurrent users and the update license file supports 5 virtual gateways and 15 concurrent users, then the system only supports 5 virtual gateways and 15 users after the license file is updated. Therefore, before importing a new license, ensure that the number of virtual gateways in use and the number of concurrent users are respectively smaller than those supported by the new license.

Step 1 Run the **license file** *filename* command to activate the system license.

Step 2 Run the **reboot** command to restart the device.

----End

4 Configuration Procedure

About This Chapter

4.1 Logging In to the Web NMS

Step 1 Open a browser and enter the IP address of the web NMS, for example, **https://192.162.1.5:443**, and press **Enter**.

The login page is displayed.

Step 2 Enter the user name and password to log in to SVN3000.

The web NMS home page is displayed, as shown in Figure 4-1.

Figure 4-1 Web NMS home page

NOTE

To ensure data security, choose **System Management** > **Administrator Management** and change the password; create a new system administrator to manage SVN3000.

----End

4.2 Adding a Virtual Gateway

Step 1 In the **System management** navigation tree, click **Virtual Gateway** to access the configuration window.

NOTE

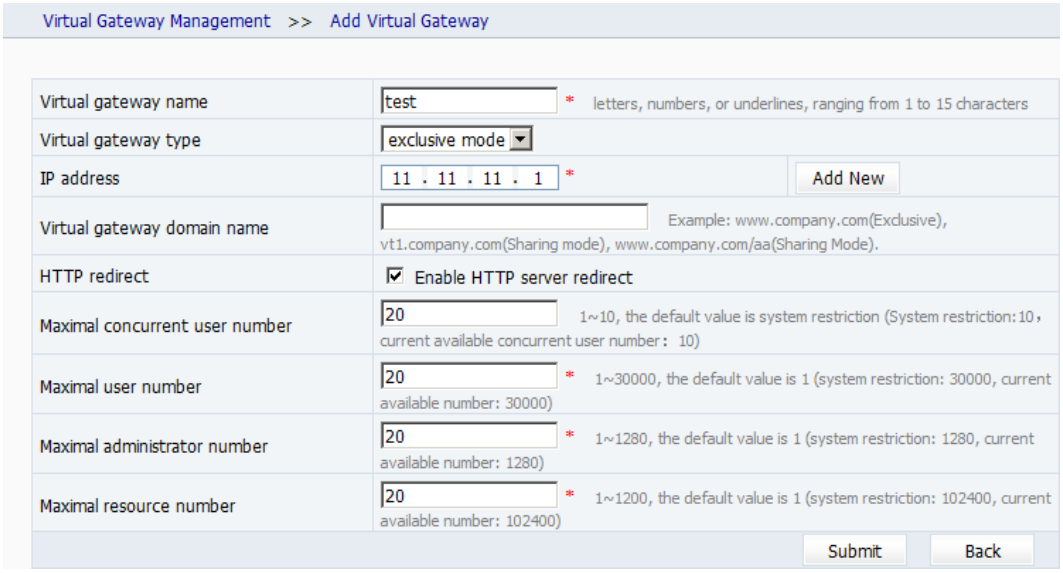
The path for configuring the virtual gateway of the SVN5300 is **SSL Virtual Gateway** > **Virtual Gateway**.

Step 2 Click **Add** in the lower right of the virtual gateway list.

The **Add Virtual Gateway** window is displayed.

Step 3 Set parameters on the **Add Virtual Gateway** page, as shown in Figure 4-2.

Figure 4-2 Add Virtual Gateway



1. Enter the name of the virtual gateway in the **Virtual gateway name** text box.
2. Select a type in the **Virtual gateway type** drop-down list.

   Virtual gateways are classified into two types: exclusive mode and sharing mode.

- exclusive mode: Virtual gateway occupies the IP address and domain name exclusively.
- sharing mode: Multiple virtual gateways share the same IP address and the main domain name. The gateways are identified by the sub-domain name.

3. Enter the IP address of the virtual gateway in the **IP address** text box.

   The IP address of the virtual gateway has been configured on the SVN interface or its sub-interface.

4. Enter the domain name of the virtual gateway in the **Virtual gateway domain name** text box.

   In the exclusive virtual gateway, **Virtual gateway domain name** is optional. In the shared virtual gateway, **Virtual gateway domain name** is mandatory.

5. Configure the **Maximal concurrent user number**, **Maximal user number**, **Maximal administrator number**, and **Maximal resource number** parameters based on the site requirements.

Step 4 Click **Submit** to submit the configuration.

NOTE

After the configuration is completed, open a browser and enter **https://***IP address of the virtual gateway* in the address box to access the virtual gateway.

----End

4.3 Configuring Network Extension

Using the SVN network extension function, clients (such as PCs) can obtain the virtual IP address of an enterprise' intranet and then client users can have access to the resources on the intranet. In this case, clients communicate with the enterprise gateway using the SSL protocol.

By configuring network extension settings, the Web NMS administrator can determine whether to allow clients to access external resources, such as, Internet.

Step 1 Click the **Virtual Gateway List** tab in the upper-left part, click next to the newly added virtual gateway in the left navigation tree, and then choose **Network Extension**.

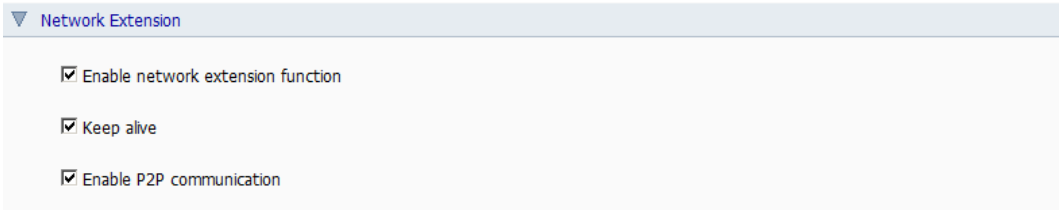
The **Network Extension** page is displayed.

NOTE

The path for configuring the network extension of the SVN5300 is **Resource Management** > **Network Extension** > **SSL Network Extension Configuration**.

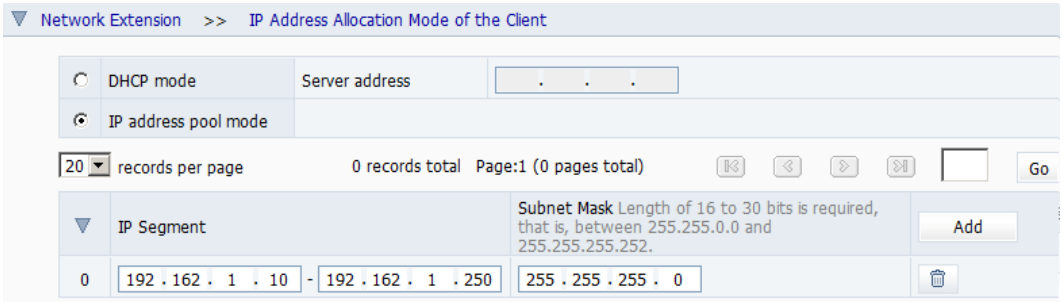
Step 2 Select **Enable network extension function**, **Keep alive** and **Enable P2P communication** in **Network Extension**, as shown in Figure 4-3.

Figure 4-3 Network Extension



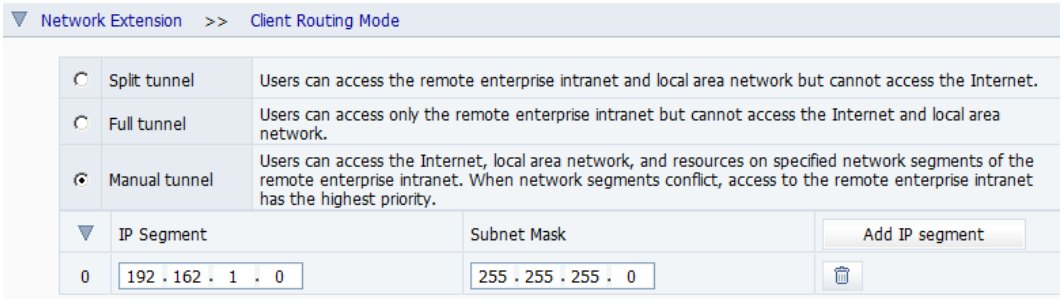
Step 3 Select **IP address pool mode** in **Network Extension >> IP Address Allocation Mode of the Client** and add the planned network segment, as shown in Figure 4-4.

Figure 4-4 IP Address Allocation Mode of the Client



Step 4 Select **Manual Tunnel** in **Network Extension >> Client Routing Mode** and add the planned network segment, as shown in Figure 4-5.

Figure 4-5 Client Routing Mode



Step 5 Click **Submit**.

----End

4.4 Configuring a VPNDB User

Step 1 Click the **Virtual Gateway List** tab in the upper-left part, and click next to the newly added virtual gateway on the left navigation tree.

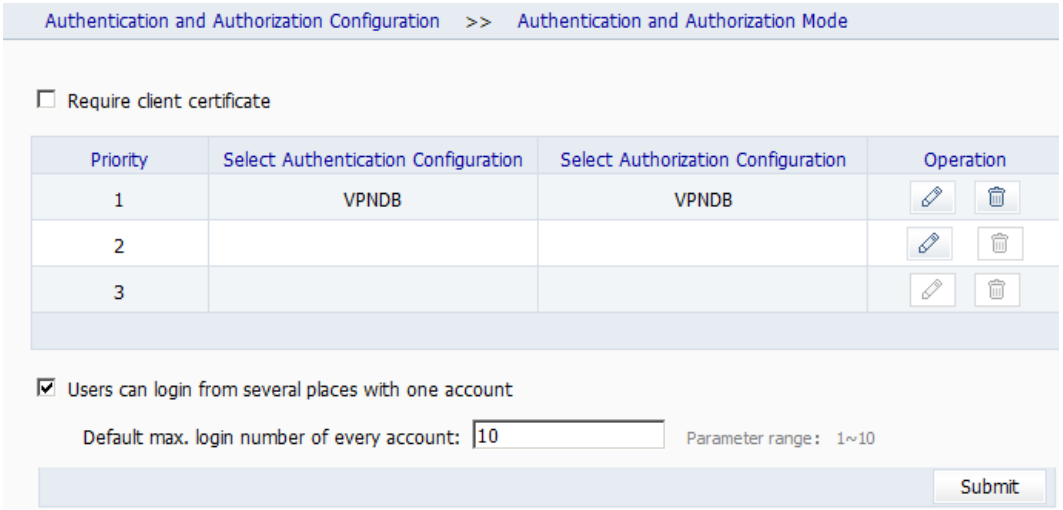
Step 2 Choose **Authentication and Authorization** from the left navigation tree, and click the **Authentication and Authorization Mode** tab on the right.

Step 3 Click in each row, and select **VPNDB** for **Select Authentication Configuration** and **Select Authorization Configuration**, as shown in Figure 4-6.

NOTE

The path for configuring the authentication and authorization of the SVN5300 is **Authentication and Authorization** > **Authentication and Authorization Mode** > **Authentication and Authorization Mode**.

Figure 4-6 Authentication and Authorization Mode



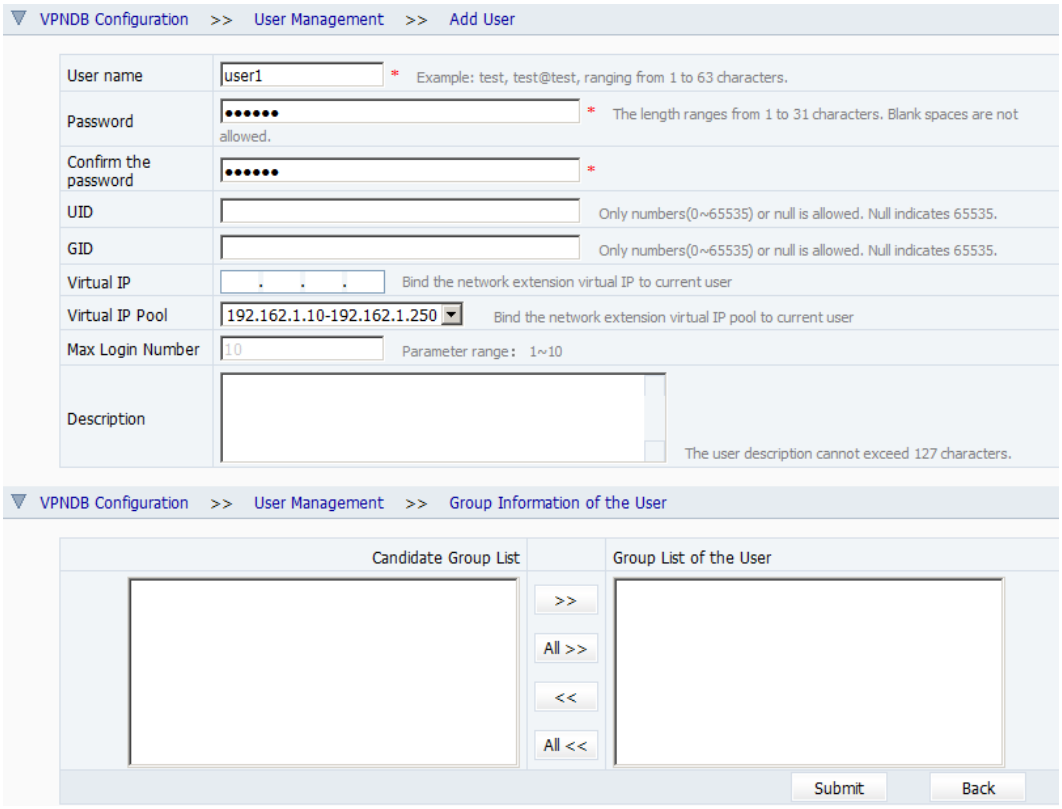
Step 4 Click **Submit** to make the settings take effect.

Step 5 Choose **VPNDB Configuration** from the left navigation tree, and click the **User Management** tab.

Step 6 Click **Add**.

The VPNDB user configuration page is displayed. Set the user name and password, and select the virtual IP address pool, as shown in Figure 4-7.

Figure 4-7 Adding a user



Step 7 Click **Submit** to add the user.

NOTE

To add users in batches, see section **Configuring a Local User** in the *Quidway SVN3000 Product Documentation*.

----End

4.5 Configuring the DNS and Domain Name (Optional)

Step 1 Click **Virtual Gateway List** on the web NMS home page.

The virtual gateway list is displayed.

Step 2 Click next to the newly added virtual gateway.

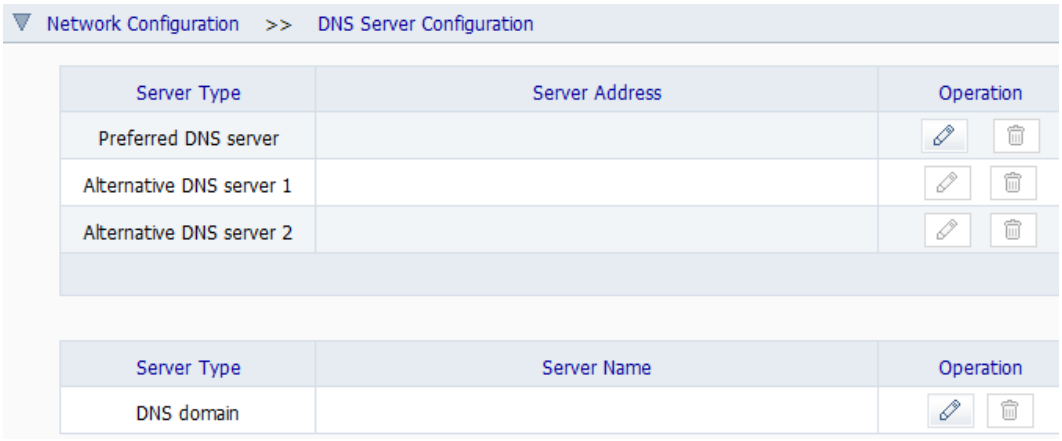
Unfold the virtual gateway navigation tree.

Step 3 Choose **Network Configuration** from the navigation tree.

The Domain Name System (DNS) page is displayed, as shown in Figure 4-8.

NOTE
The path for configuring the DNS of the SVN5300 is **Virtual Gateway** > **DNS** > **DNS**.

Figure 4-8 Network Configuration



Set the parameters based on the actual scenario.

----End

4.6 Saving the Configuration

Step 1 Choose **Device Maintenance** > **System Management** from the navigation tree.

Step 2 Click **Save** on the right.

----End

5 Precautions

- Ensure that the port (usually port 443) used by SVN3000 is enabled for external users on the firewall. If enterprise users want to manage SVN3000 on an external network, enable the port bound to the Web NMS.
- Ensure that a route for SVN3000 has been added on the internal switch or router so that the SVN3000 can communicate with the internal server.

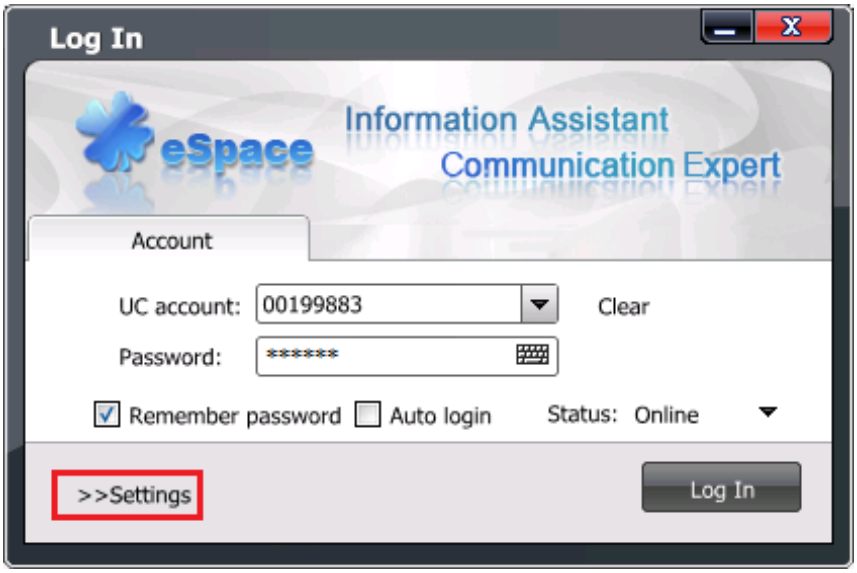
6 Verification

The SVN configuration is successful if you can log in to and communicate with an application server on the intranet through a client running the SVN software or the software that integrates the SSL VPN access capability.

This topic uses the eSpace Desktop as an example.

Step 1 Start the eSpace Desktop, as shown in Figure 6-1.

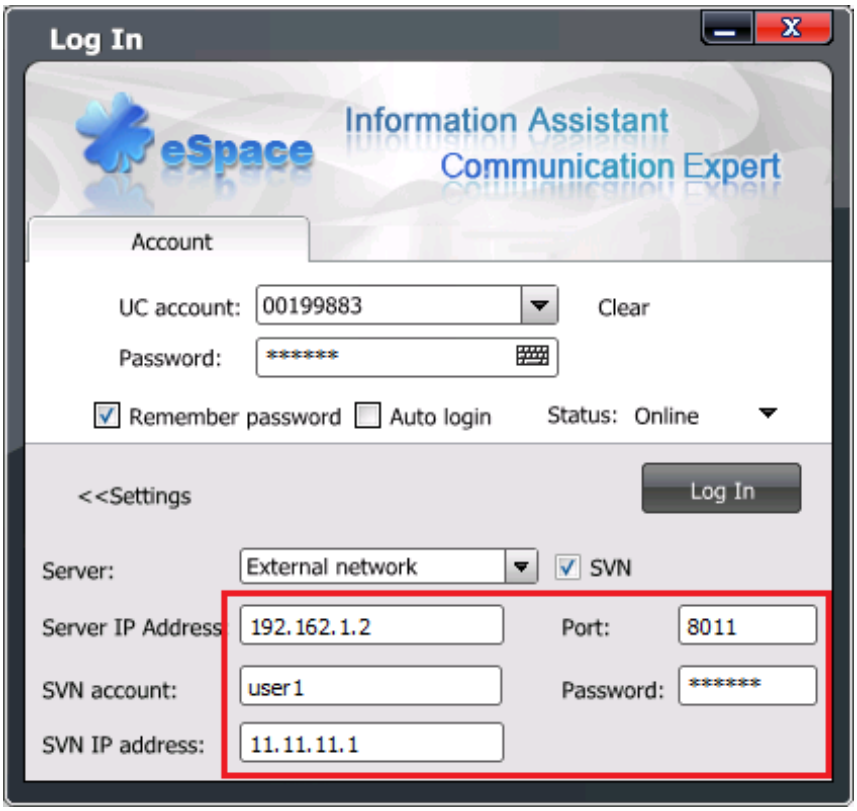
Figure 6-1 eSpace login page



Step 2 Click **Settings**.

Select **External network** from the login server drop-down list, and select **SVN**, as shown in Figure 6-2.

Figure 6-2 Login from an external network through eSpace



Step 3 Enter the IP address of the eServer, SVN account, password, and the external IP address of the SVN server.

Step 4 Enter the UC account and password, and click **Log In**.

If the login and communication are successful, the SVN configuration is correct.

----End