

# #Configuration# Sangfor NSF SSL VPN configuration guide

**\*Product:** NSF

**\*Version:** 8.0.85

## **\*1. Introduction**

### **1.1 User Scenario**

Nowadays, connecting to the corporate network from outside can be a challenge as the complexity of networks increases more and more. Furthermore, by connecting to public networks, traffic is often filtered and only the most common protocols for web browsing are allowed. This is where SSL VPN comes into play. This type of VPN uses the https protocol commonly used for web browsing and less subject to restrictions when connecting to public networks and also get data encryption to ensure security and data integrity. Below we see how to correctly configure the SSL VPN on Sangfor NSF.

### **1.2 Requirements**

1. Firewall Sangfor NSF firmware updated to the latest release
2. A static public ip address on wan interface
3. A client with Sangfor EasyConnect

## **\*2. Configuration Guide**

### **2.1 NGAF VPN SSL Configuration**

## 2.1.1 NGAF VPN SSL Deployment mode

**Step 1.** Define the interfaces that Sangfor SSL VPN must use.

To do this you have to go to **Network > SSL VPN > Deployment.**

On this guide we'll see the gateway deployment node.

On the next screen, you must select properly ethernet interfaces on Sangfor NGAF (on this example, we have eth1 as wan and eth2 as Layer 3 Lan):

The screenshot shows a web browser window with the URL `https://10.0.0.1/framework.php#/mod_policy/sslvpn/gateway`. The page title is "Network Secure Platform 8.0.85". The navigation menu includes "Home", "SOC", "Monitor", "Policies", "Objects", "Network" (highlighted), and "System". The left sidebar shows "Network" and "SSL VPN" (expanded) with sub-items: "Online Users", "Deployment" (highlighted), "Local Users", "Resources", and "Roles". The main content area is titled "Deployment" and contains the following settings:

- Deployment**
  - Mode:  Gateway  Single-Arm
- Interface Settings**
  - LAN Interface: eth2
  - WAN Interface: eth1

A warning message at the top states: "Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the one...". A blue "OK" button is located at the bottom of the configuration panel.

After that, you can select the port of web ui ssl vpn portal.

You can achieve it by going to **Network > SSL VPN > Login Options.**

Enable only TLS 1.2 for security reasons.

Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects **Network** System

Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match. [View](#)

### Network

- Interfaces
- Zones
- Routes
- Virtual Wires
- DNS
- DHCP
- ARP
- Advanced
- SSL VPN**
  - Online Users
  - Deployment
  - Local Users
  - Resources
  - Roles
  - Login Options**

### Login Options

**Login Port**

HTTPS Port:

Disconnect user if inactivity period reaches  (5-43200) minutes. (local DNS must not be enabled)

**SSL/TLS Options**

SSL/TLS Algorithm: RSA

TLS 1.0    TLS 1.1    TLS 1.2

**WebAgent Settings**

Enable WebAgent for dynamic IP assignment

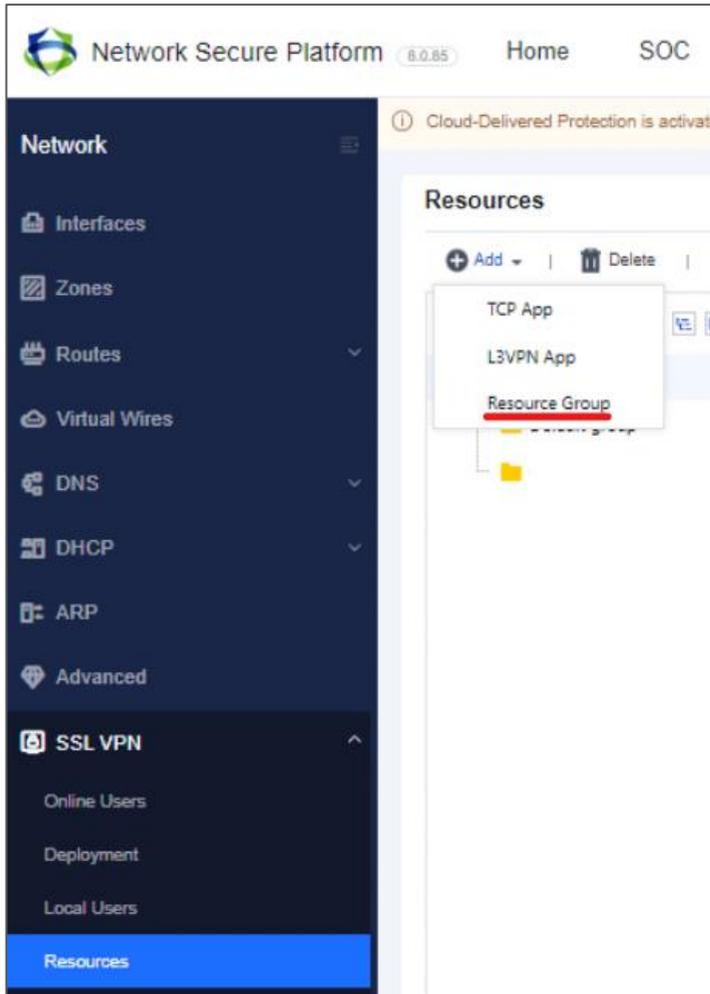
|  |  |  |

<input type="checkbox"/>	WebAgent Address	Status	...
 No data available			

## 2.1.2 NGAF VPN SSL resource creation

Now, you can create a resource group to keep together all your resources.

To create it, you must go to **Network > SSL VPN > Resources** and create a resource group (on this example I named it mycompany)



Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects **Network** System

Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match. [View](#)

### Resources

**Basic Attributes**

Name:

Description:

Enable resource group

**Display Options:**

In icons: 

In text:  Show description

Added To: /

Now on the same page, we can define the internal network as resource by creating an L3VPN App and insert your network details as follows (on our example we have 10.0.0.0/22 as internal network). Don't forget to specify the resource group created before

CL-FW x +

← → ↻ Non sicuro https://10.0.0.1/framework.pl

DC Dashboard

Network Secure Platform 8.0.65 Home SOC

Network

- Interfaces
- Zones
- Routes
- Virtual Wires
- DNS
- DHCP

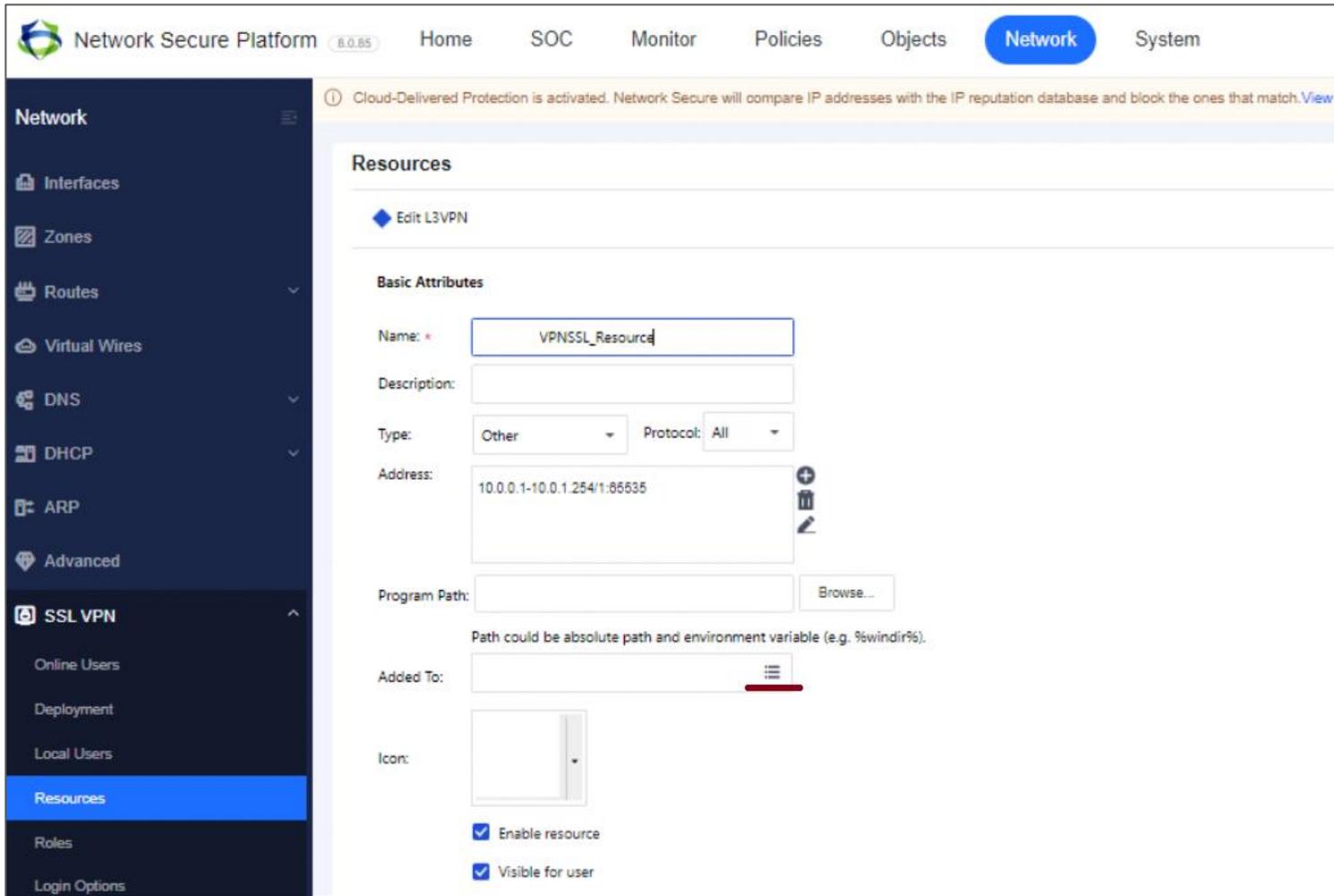
Cloud-Delivered Protection is activated.

### Resources

+ Add | Delete

- TCP App
- L3VPN App
- Resource Group

- Corelink
- mycompany



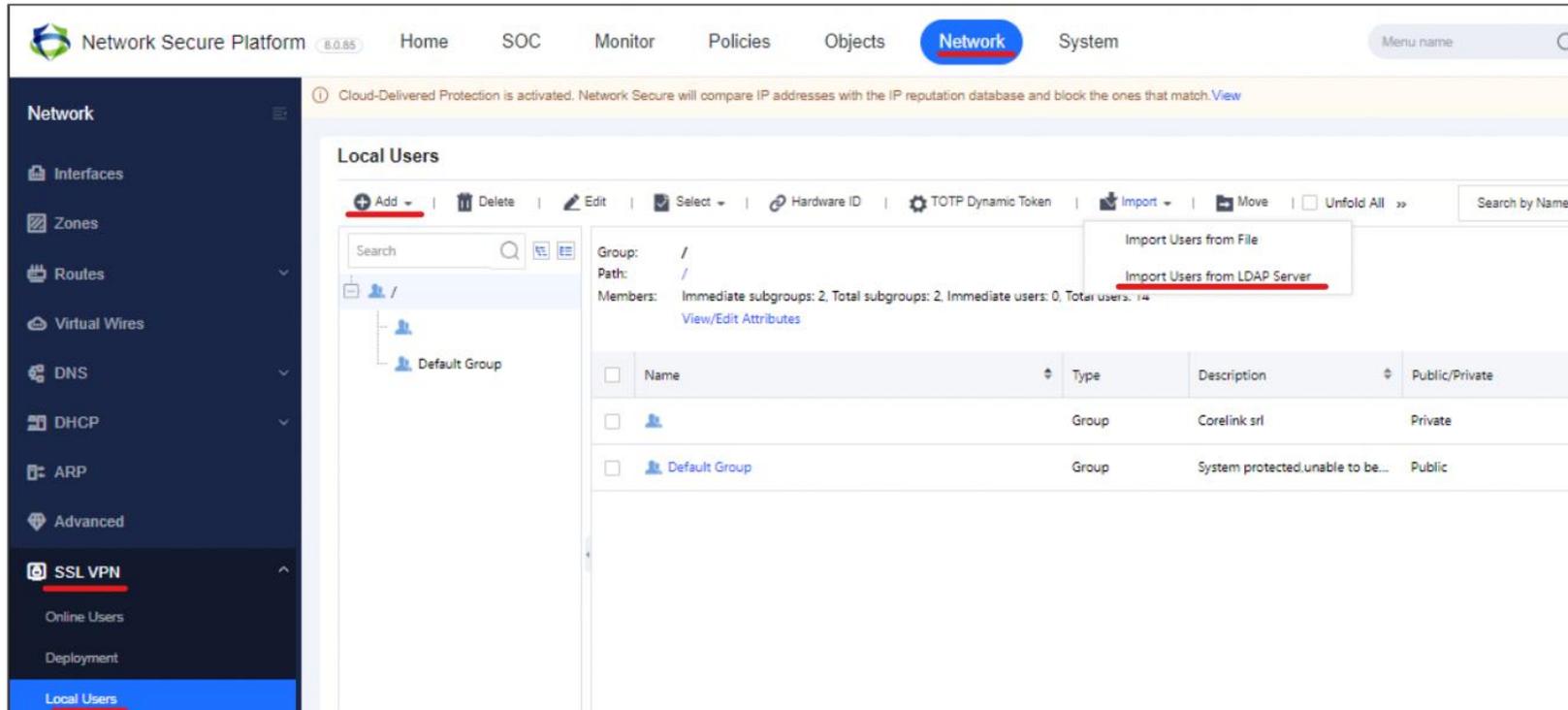
On L3VPN App mode, the VPN client will install a virtual network card to route all traffic into it (any protocols).

### 2.1.3 NGAF VPN SSL user creation

Now on this web UI path we can choose to create a local user or import a user list from an external source (you must configure it first on Sangfor NGAF)

## Network > SSL VPN > Local Users

On this example we choose to create a local user named testuser.



The screenshot displays the Network Secure Platform interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (highlighted), and 'System'. A search bar is located on the right. The left sidebar shows the 'Network' menu with sub-items: Interfaces, Zones, Routes, Virtual Wires, DNS, DHCP, ARP, Advanced, SSL VPN (highlighted), Online Users, and Deployment. The 'Local Users' sub-item under SSL VPN is also highlighted.

The main content area is titled 'Local Users'. It features a toolbar with 'Add', 'Delete', 'Edit', 'Select', 'Hardware ID', 'TOTP Dynamic Token', 'Import', 'Move', and 'Unfold All' buttons. A search bar is present on the right. The 'Add' button is highlighted with a red underline. A dropdown menu is open over the 'Import' button, showing 'Import Users from File' and 'Import Users from LDAP Server' (highlighted with a red underline).

Below the toolbar, the 'Members' section shows 'Immediate subgroups: 2, Total subgroups: 2, Immediate users: 0, Total users: 14'. A 'View/Edit Attributes' link is available. A table lists the members:

<input type="checkbox"/>	Name	Type	Description	Public/Private
<input type="checkbox"/>	Corelink srl	Group	Corelink srl	Private
<input type="checkbox"/>	Default Group	Group	System protected,unable to be...	Public

Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects **Network** System

Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match. [View](#)

### Local Users

**Basic Attributes**

Name:

Description:

Password:

Confirm:

Mobile Number:

Added To:

Inherit authentication settings from parent group

**Virtual IP Assignment:**  Automatic  Specified

**Expire:**  Never expire  On date

**Status:**  Enabled  Disabled

**Authentication Options**

User Type:  Public user  Private user

**Primary Authentication:** Local password Local database

**Secondary Authentication:**  Hardware ID  Dynamic Token Authentication

**Assigned Roles**

Roles:  [+ Create + Associate](#)

## 2.1.4 NGAF VPN SSL role assignment

At this stage, we must assign a role to the newly created user to associate them with resources.

To do it, you must go to **Network > SSL VPN > Roles and** assign a role.

On our example we'll create a new role to grant testuser connect to the resources that stands on resource group that we create before (named mycompany)

The screenshot displays the 'Network Secure Platform' interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (highlighted), and 'System'. A notification banner at the top states: 'Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match. View'. The left sidebar lists various network settings, with 'SSL VPN' and 'Roles' highlighted. The main panel is titled 'Roles' and contains the following configuration fields:

- Basic Attributes:**
  - Name: mycompany\_vpnrole
  - Description: (empty)
  - Assigned To: testuser (with a 'Select UserGroup' button)
  - Enable Role
- Associated Resources:**
  - A table with columns: Name, Type, Description, and a menu icon (\*\*\*).
  - The table contains one entry: 'mycompany' (Resource group).
  - Below the table is a pagination control: 'Page 1 of 1 | Show 25 /page'.

At the bottom of the form are three buttons: 'Save and Add', 'OK', and 'Cancel'.

## 2.1.5 NGAF VPN SSL virtual IP pool

On the following section, we'll see which ip range to assign to vpn ssl users that connects from external by using Sangfor VPN SSL.

For a specific resource group you can define a virtual ip range to use.

By default, there is 2.0.1.1 - 2.0.1.254 virtual ip range to all resources group.

I recommend to not delete this default virtual ip range.

The screenshot displays the Network Secure Platform interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (highlighted), and 'System'. The left sidebar lists various network-related options, with 'SSL VPN' expanded to show 'Virtual IP Pool' selected. The main content area is titled 'Virtual IP Pool' and contains a descriptive text box explaining that users accessing resources over SSL VPN are assigned a virtual IP address from this pool. Below the text is a table with columns for 'IP Range', 'Assigned To', and 'Description'. A single entry is shown with the IP range '2.0.1.1 - 2.0.1.254' (underlined in red), assigned to 'Any group', and described as the 'Default virtual IP pool'. The table includes action icons for 'Add', 'Delete', 'Edit', and 'Select'. At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and 'Show 25 /page'.

Network Secure Platform 8.0.85 Home SOC Monitor Policies Objects **Network** System

Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match. [View](#)

### Virtual IP Pool

When a user starts to access resources over SSL VPN, it will be assigned a virtual IP address. This IP address could be the virtual IP address specified in User Attribute or an IP address dynamically assigned from the virtual IP pool.

+ Add | Delete | Edit | Select ▾

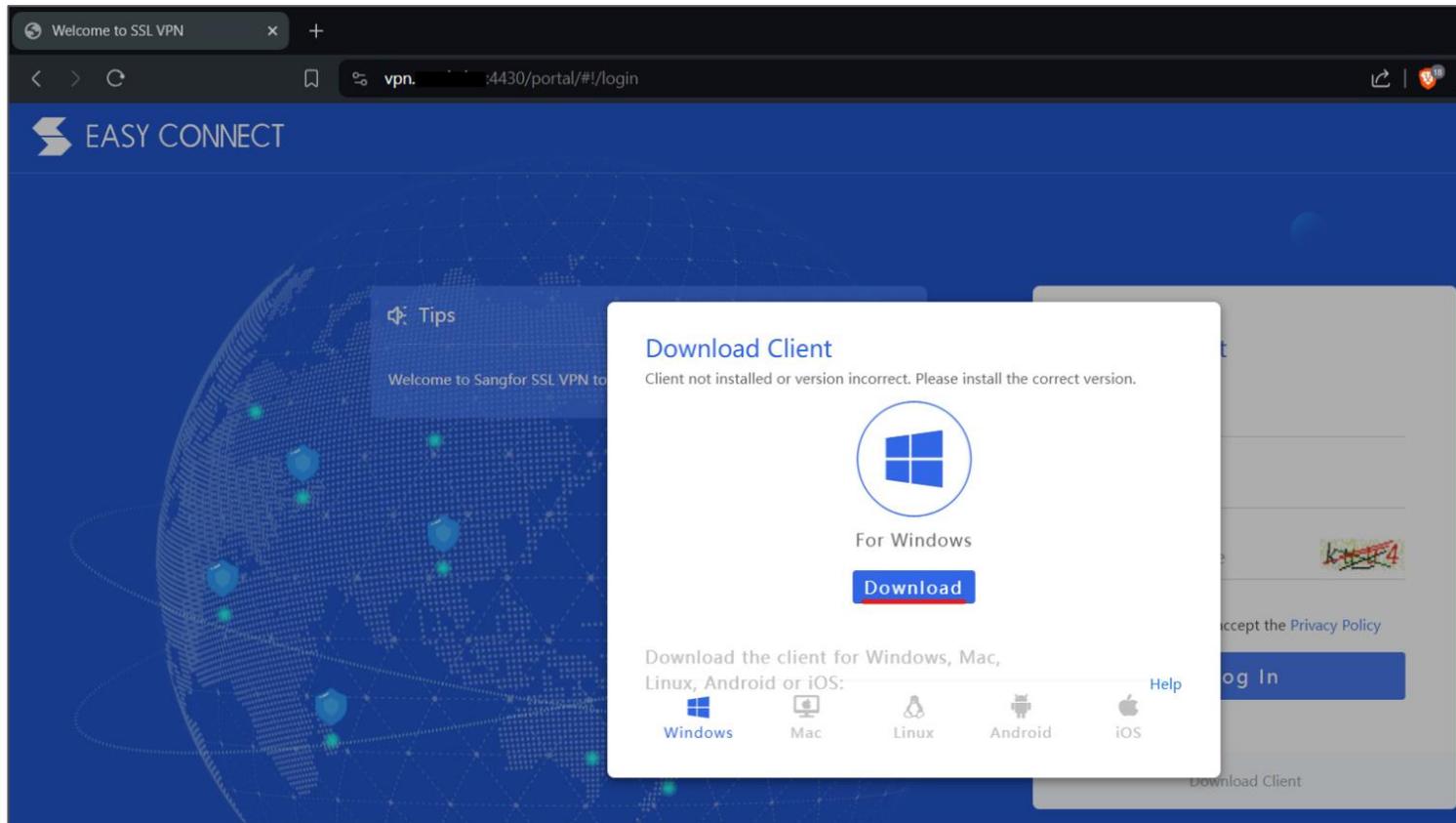
<input type="checkbox"/>	IP Range	Assigned To	Description	...
<input type="checkbox"/>	<u>2.0.1.1 - 2.0.1.254</u>	Any group	Default virtual IP pool	

Page 1 of 1 | Show 25 /page

## 2.1.6 NGAF VPN SSL login page

Make sure the users can reach the NSF port 4430(SSLVPN default port) from external networks, by typing the public ip with port on a

browser(https://x.x.x.x:4430).



As you can see, the web page will prompt you to install Sangfor EasyConnect client on your pc.

After installation, you can log in to the SSLVPN and you are connected.

After login, you can check on the web page the resources you can connect to.

### **\*3. Precaution**

When external users want to connect to intranet resources by using Sangfor VPN SSL, it's important to check that the external user's local network doesn't overlap with the virtual ip pool or intranet network.