#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

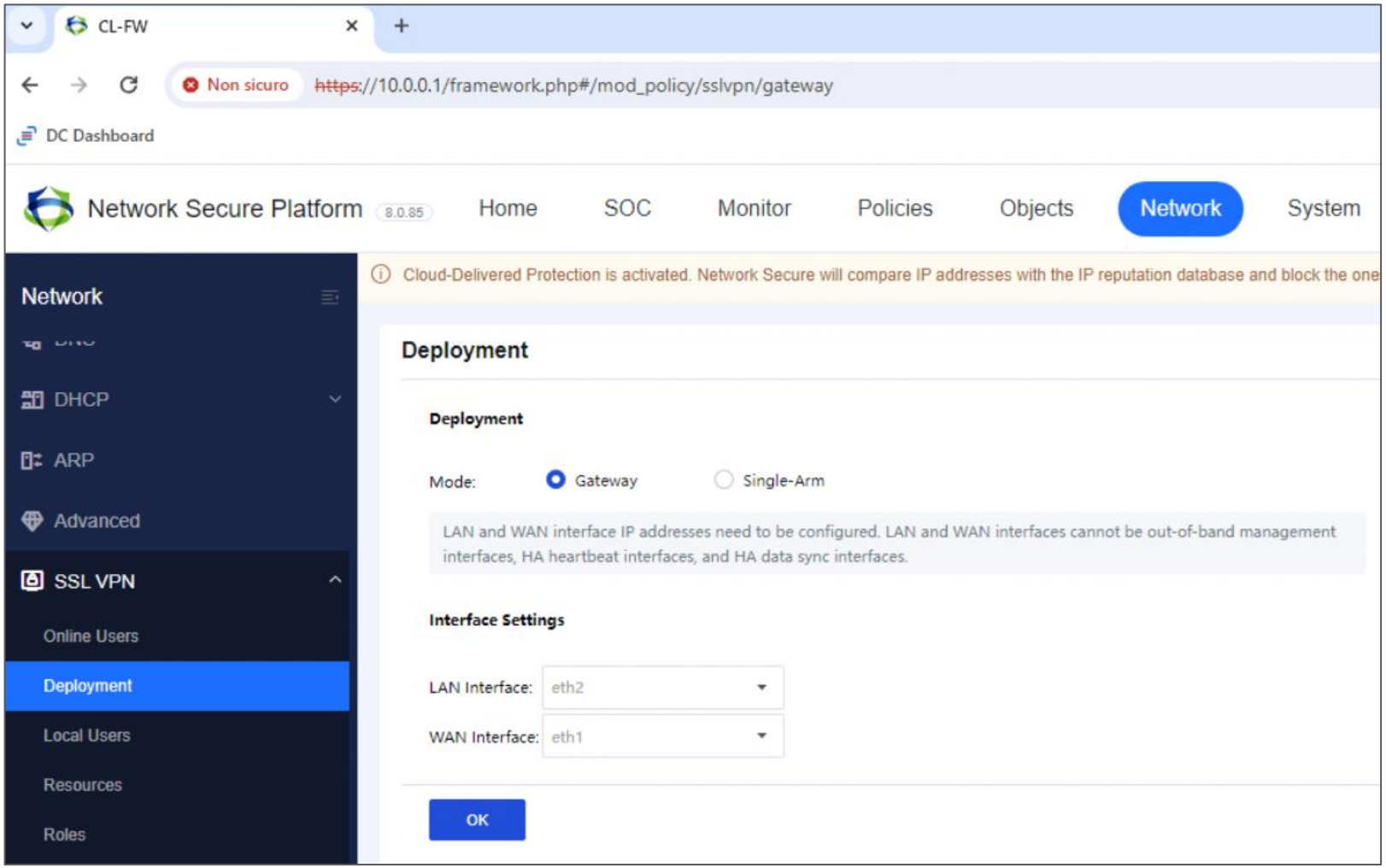
2.1.1 NGAF VPN SSL Deployment mode

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.

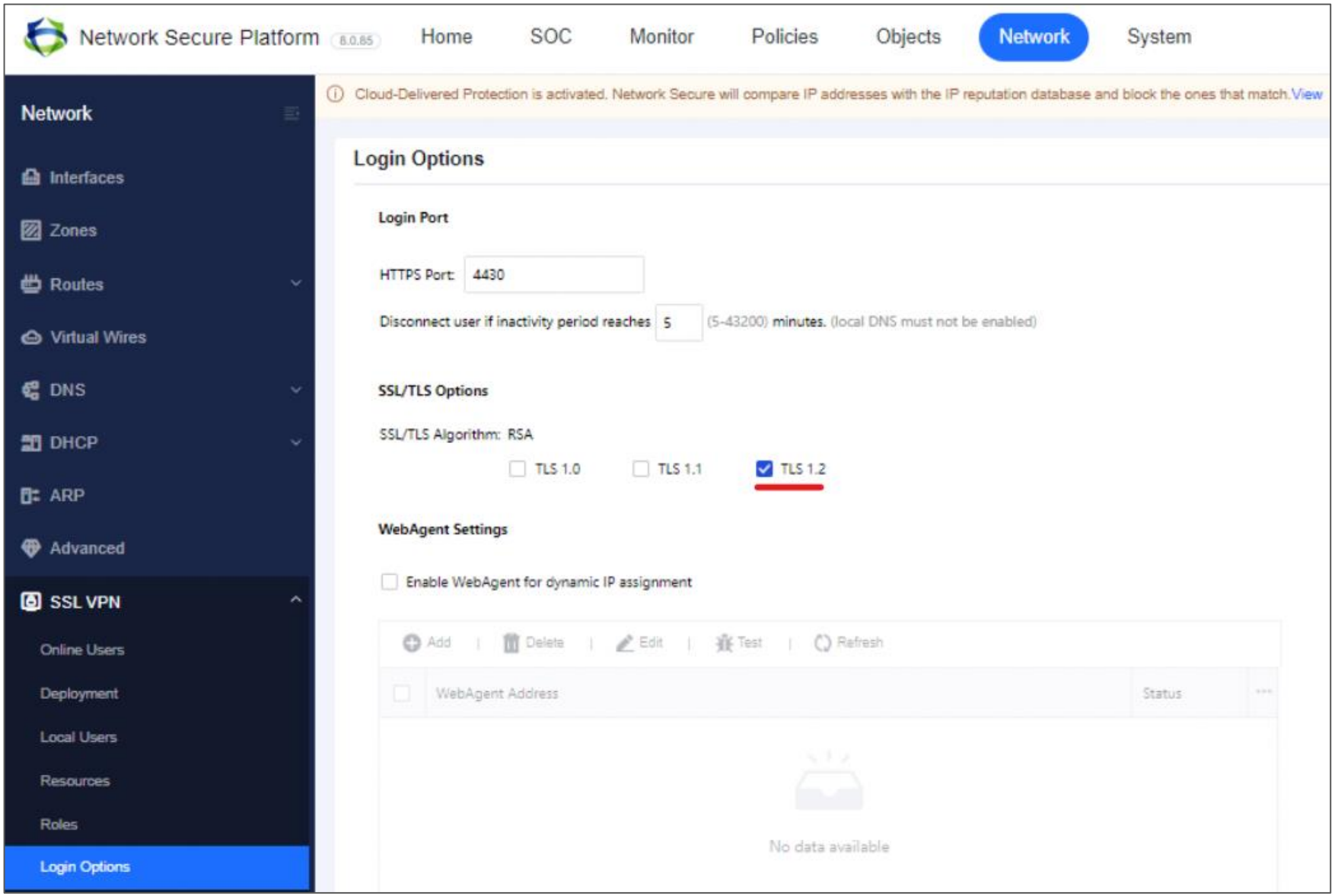
On the next screen, you must select proprely ethernet interfaces on Sangfor NGAF (on this example, we have eth1 as wan and eth2 as Layer 3 Lan):



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.**

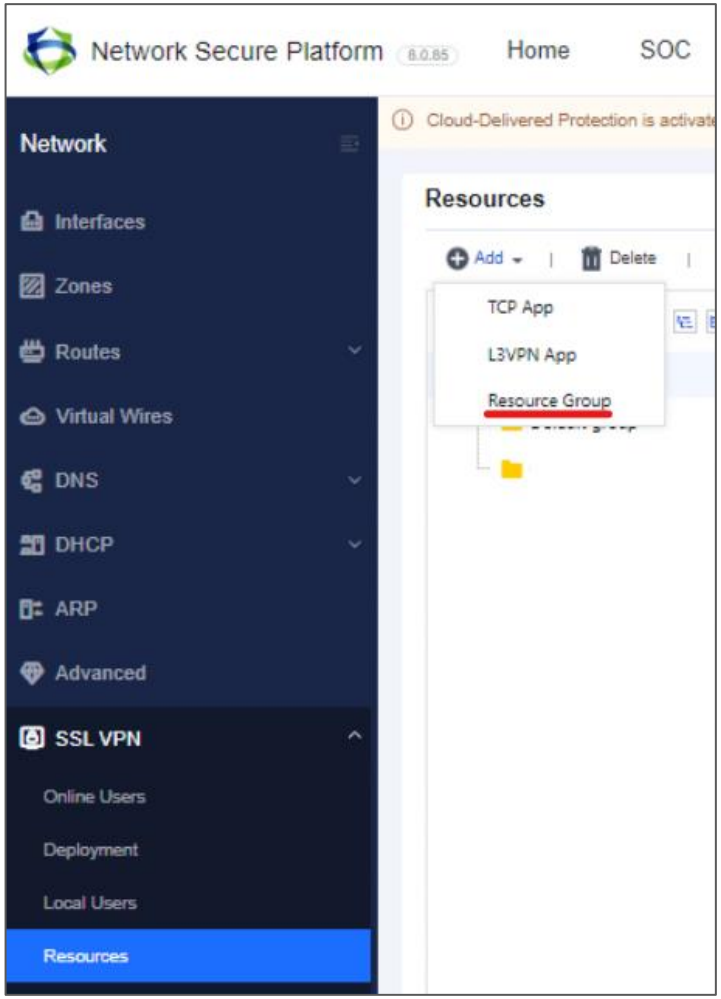
Enable only TLS 1.2 for security reasons.

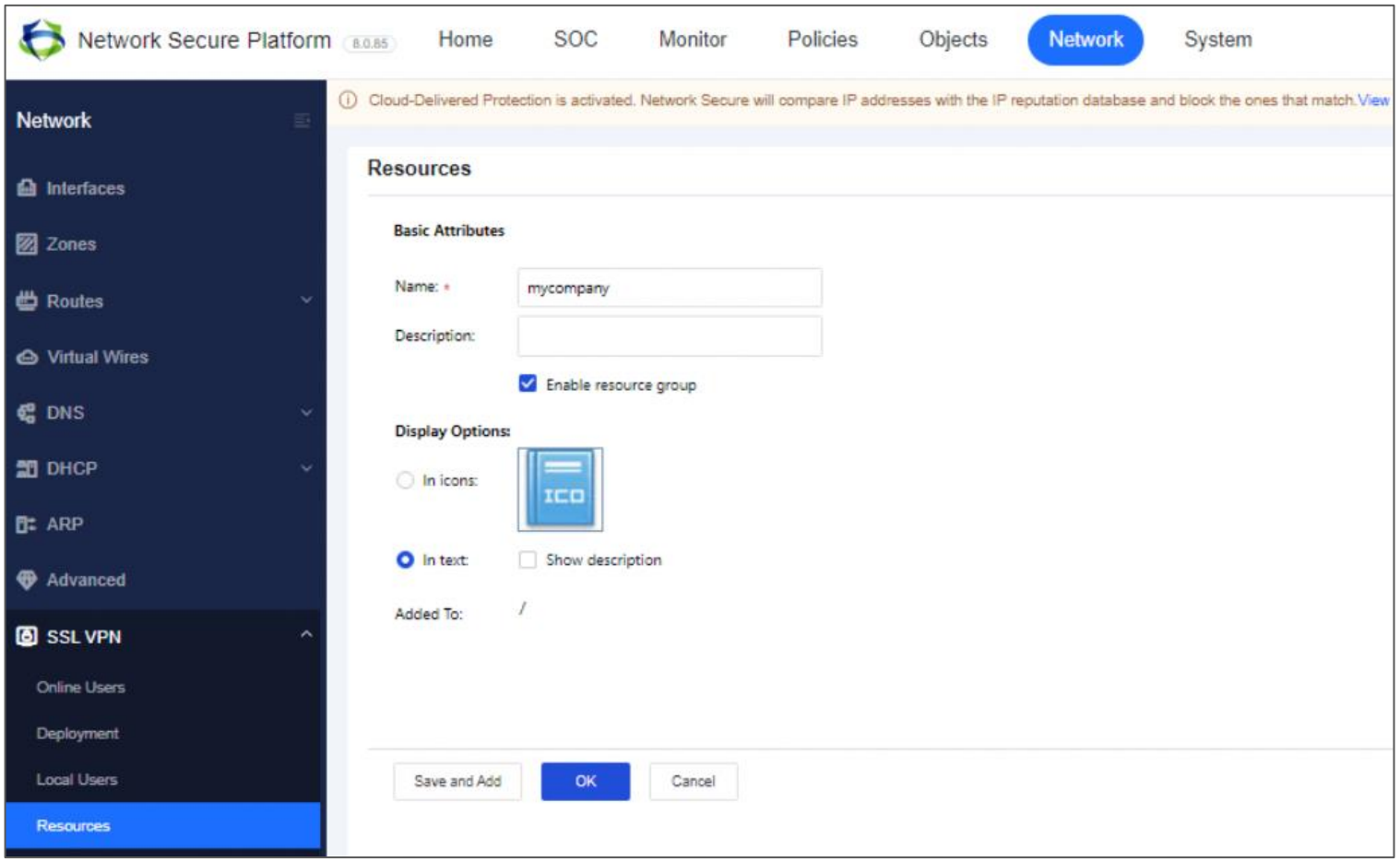


2.1.2 NGAF VPN SSL resource creation

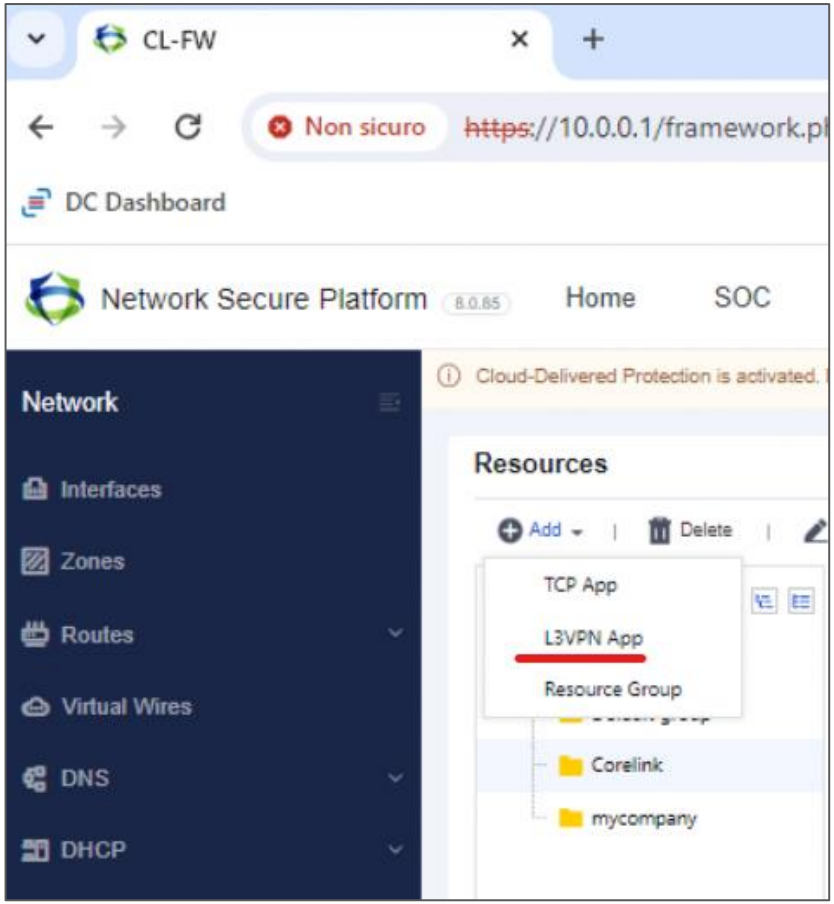
Now, you can create a resource group to keep together all your resources.

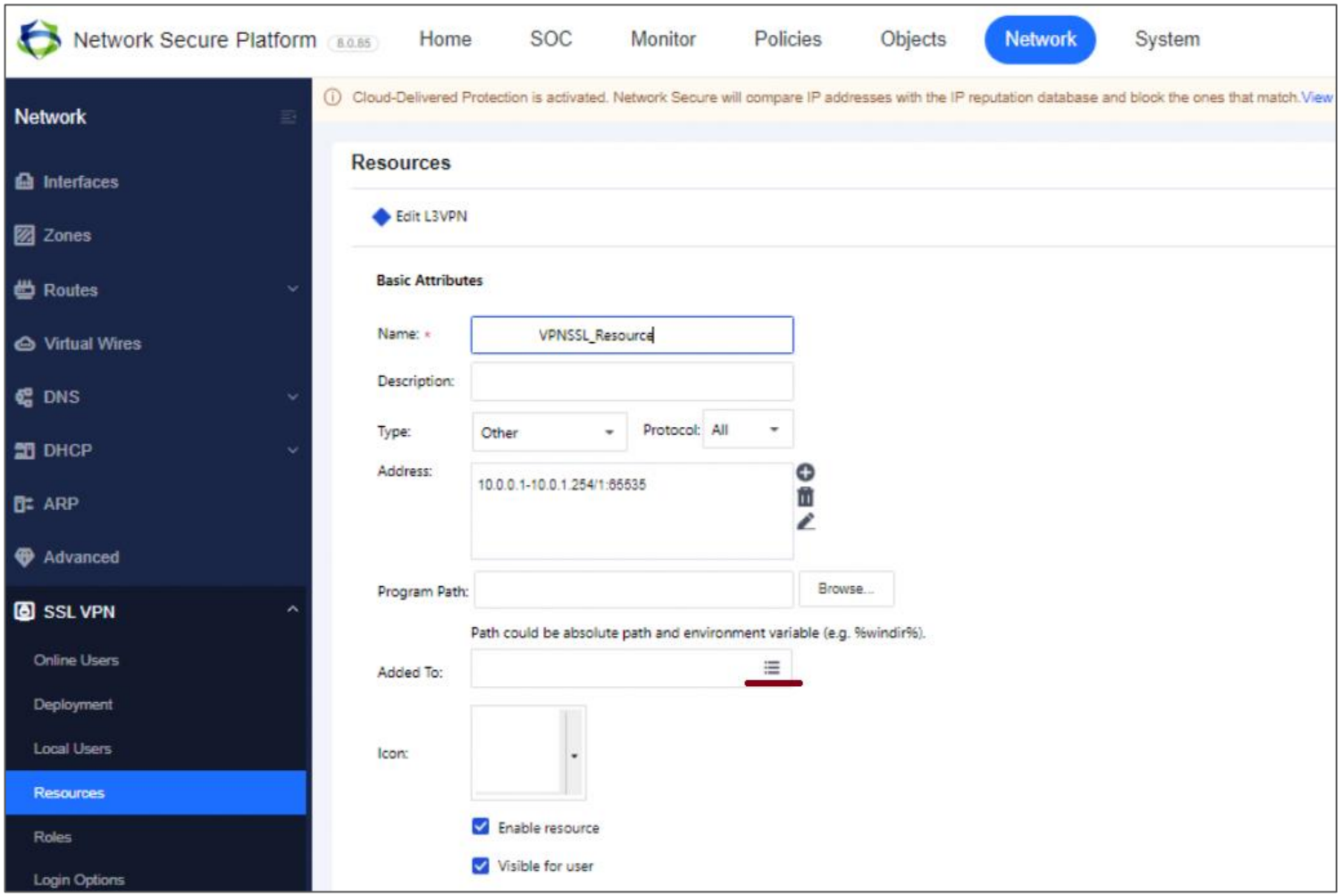
To create it, you must go to **Network > SSL VPN > Resources** and create a resource group (on this example I named it mycompany)





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
Non sicuro
https://10.0.0.1/framework.pl
DC Dashboard
Network Secure Platform
8.0.65
Home
SOC
Network
Cloud-Delivered Protection is activated.
Interfaces
Zones
Routes
Virtual Wires
DNS
DHCP
Resources
Add
Delete
TCP App
L3VPN App
Resource Group
Corelink
mycompany



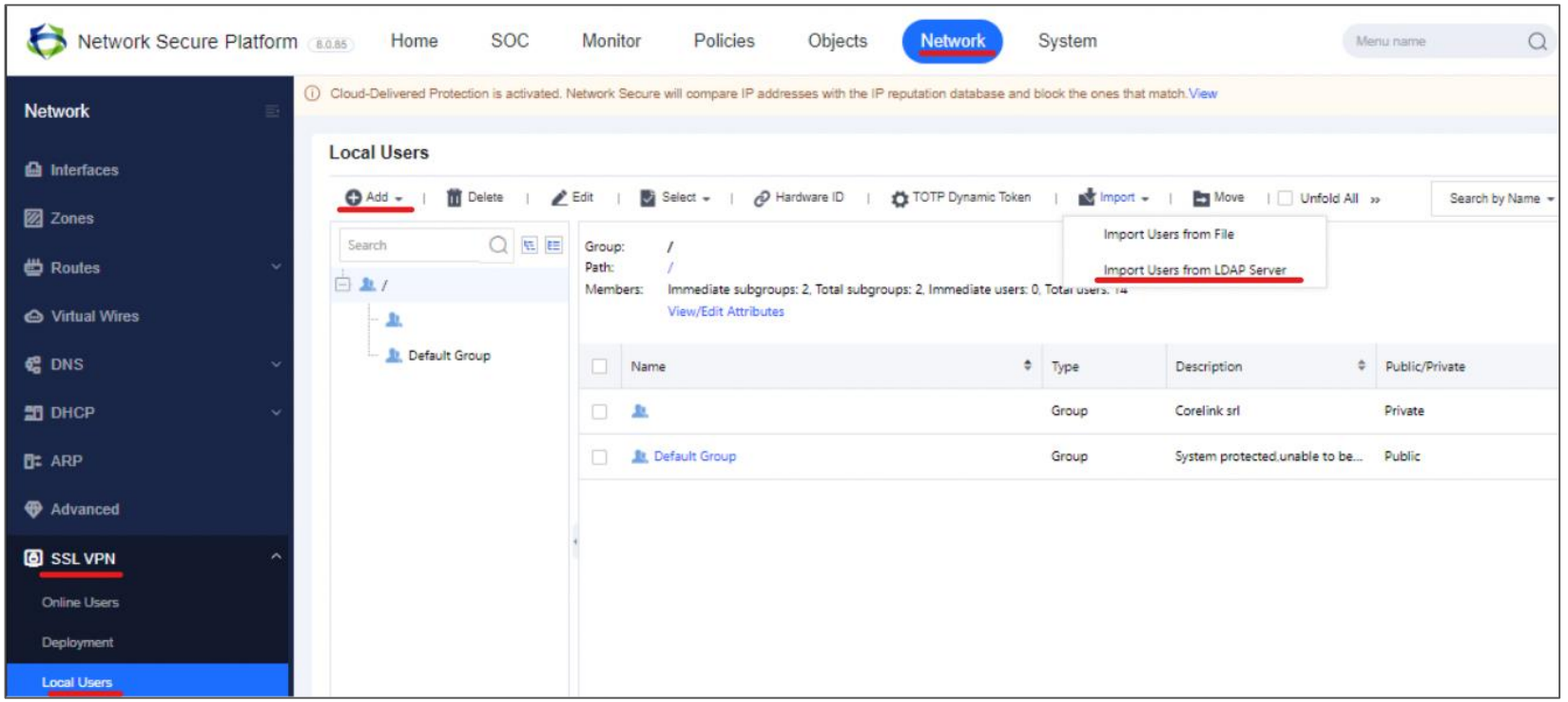
On L3VPN App mode, the VPN client will install a virtual network card to route all traffic into it (any protocols).

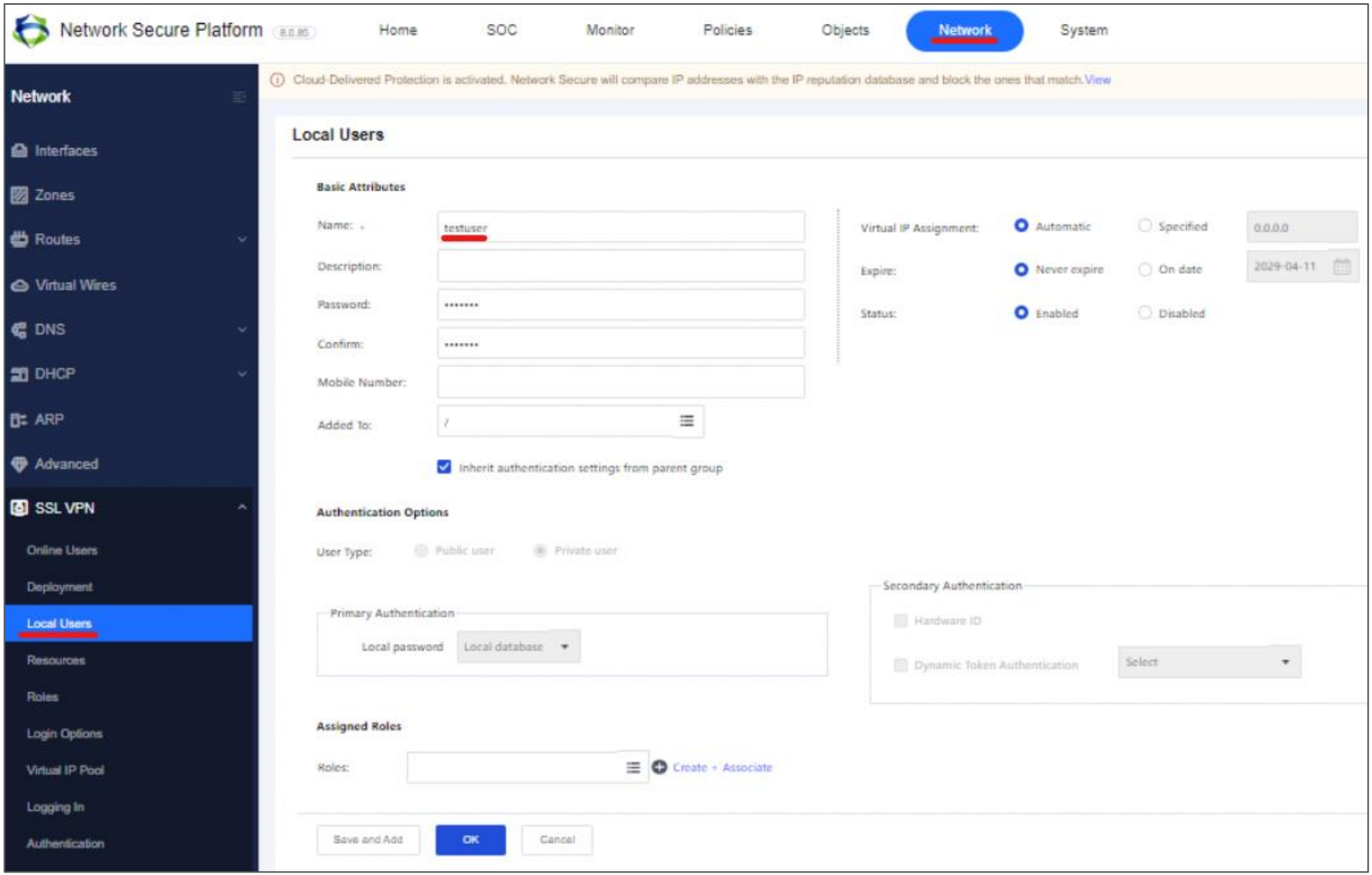
2.1.3 NGAF VPN SSL user creation

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.



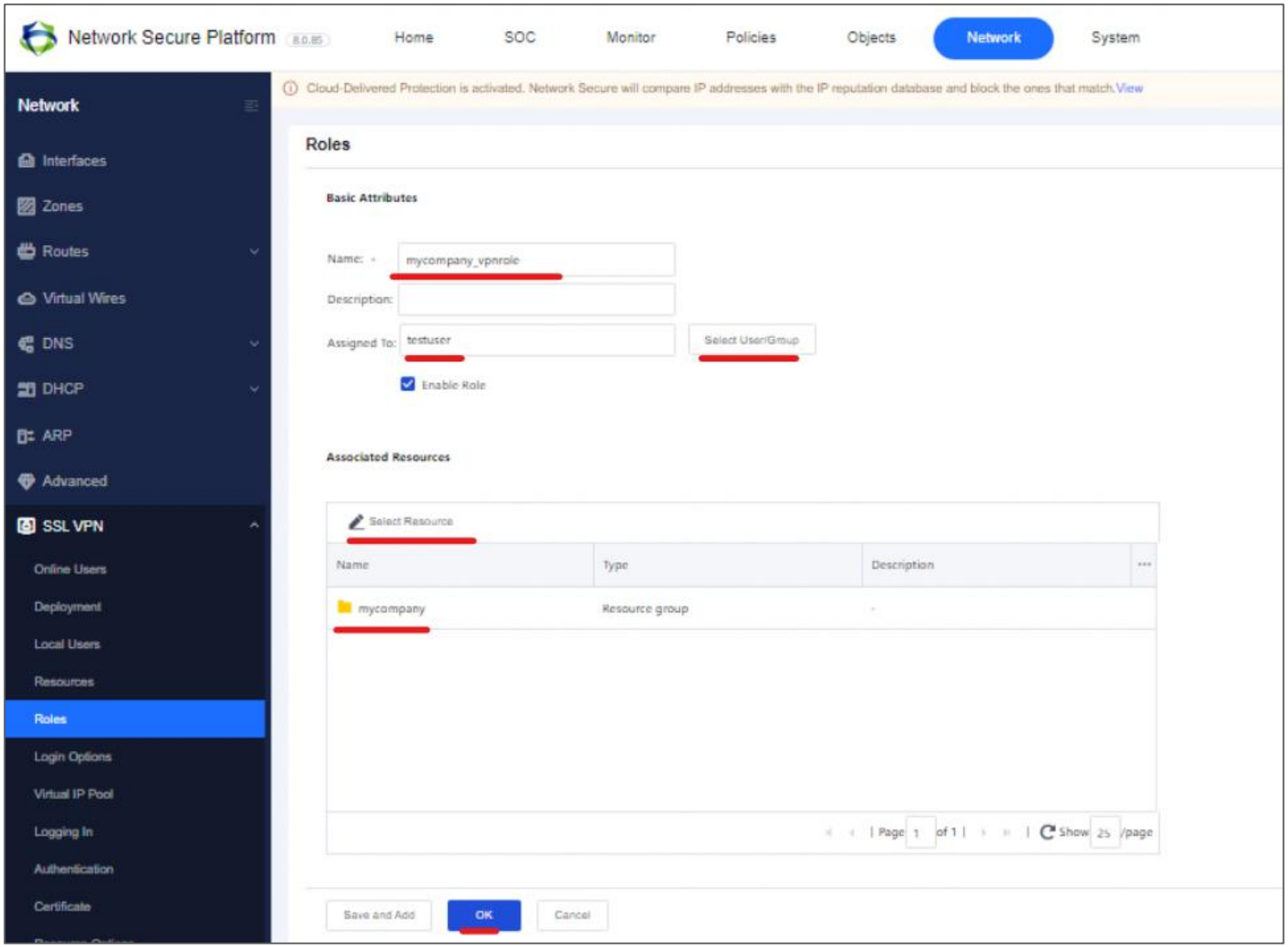


2.1.4 NGAF VPN SSL role assignment

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)



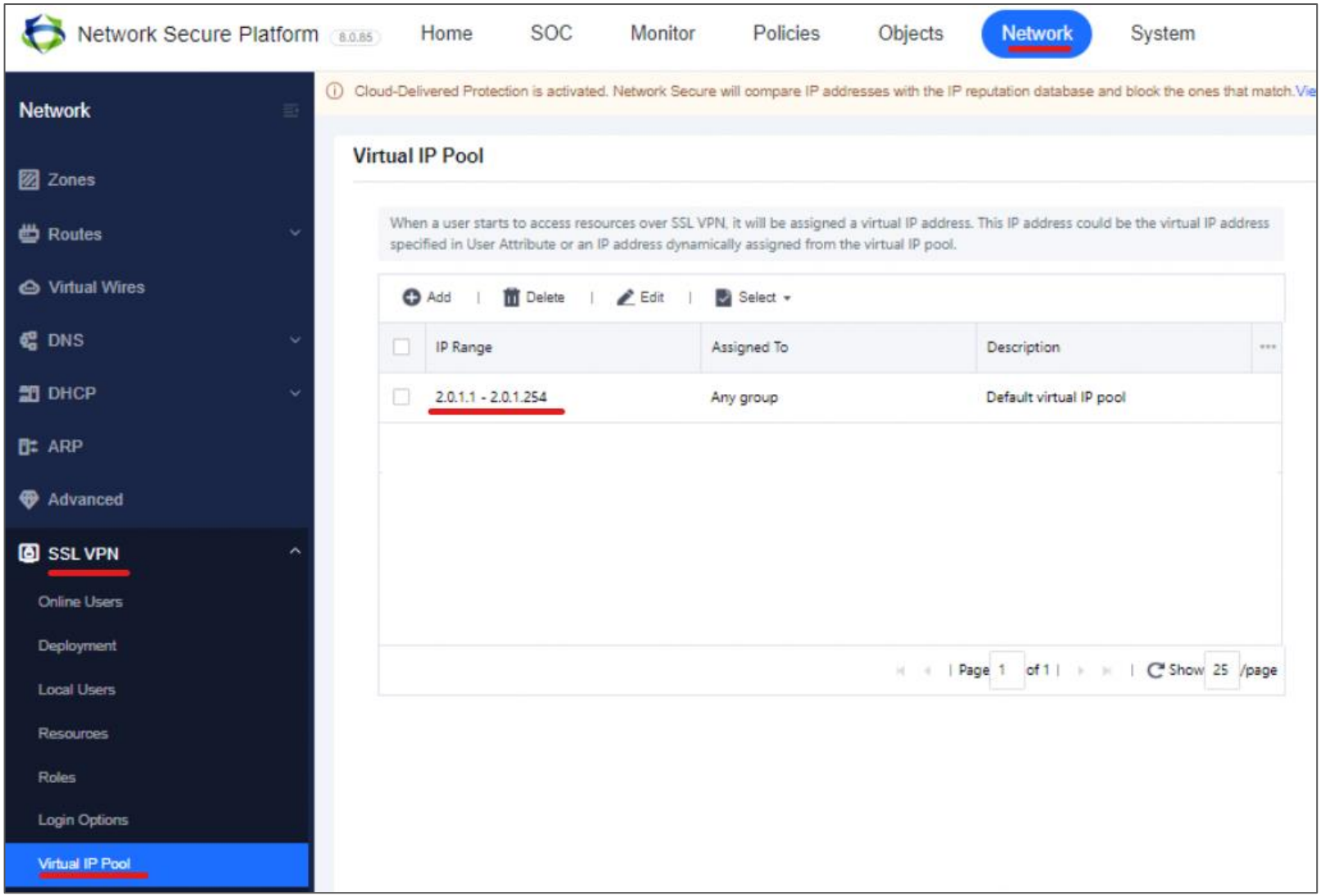
2.1.5 NGAF VPN SSL virtual IP pool

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.

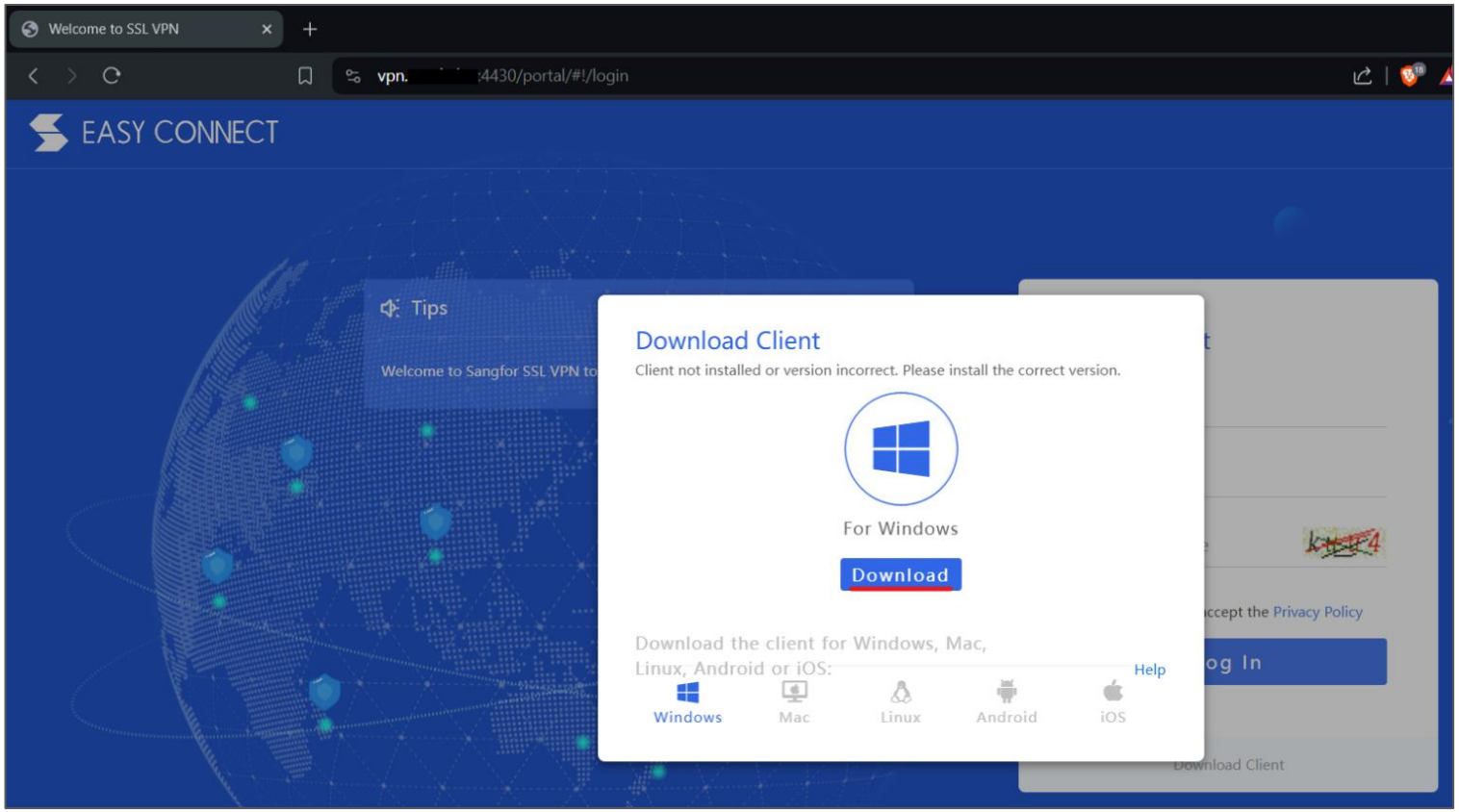
I recommend to not delete this default virtual ip range.



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.