# #Configurazione# Guida configurazione Sangfor NGAF SSL VPN

***Prodotto:** NGAF

***Versione:** 8.0.85

## *1. Introduzione

### 1.1 Scenario

Oggi, connettersi alla rete aziendale dall'esterno può essere una sfida, poiché la complessità delle reti aumenta sempre di più. Inoltre, collegandosi a reti pubbliche, il traffico viene spesso filtrato e vengono consentiti solo i protocolli più comuni per la navigazione web. È qui che entra in gioco la VPN SSL. Questo tipo di VPN utilizza il protocollo https, comunemente usato per la navigazione web, ed è meno soggetto a restrizioni quando ci si collega a reti pubbliche. Inoltre, offre la crittografia dei dati per garantire sicurezza e integrità dei dati. Di seguito vediamo come configurare correttamente la VPN SSL su Sangfor NGAF.

### 1.2 Requisiti

1. Firewall Sangfor NGAF aggiornato all'ultima release

2. Un ip pubblico statico assegnato all'interfaccia WAN del firewall

3. Un client con installato Sangfor EasyConnect

## *2. Configurazione

## 2.1 Configurazione NGAF VPN SSL

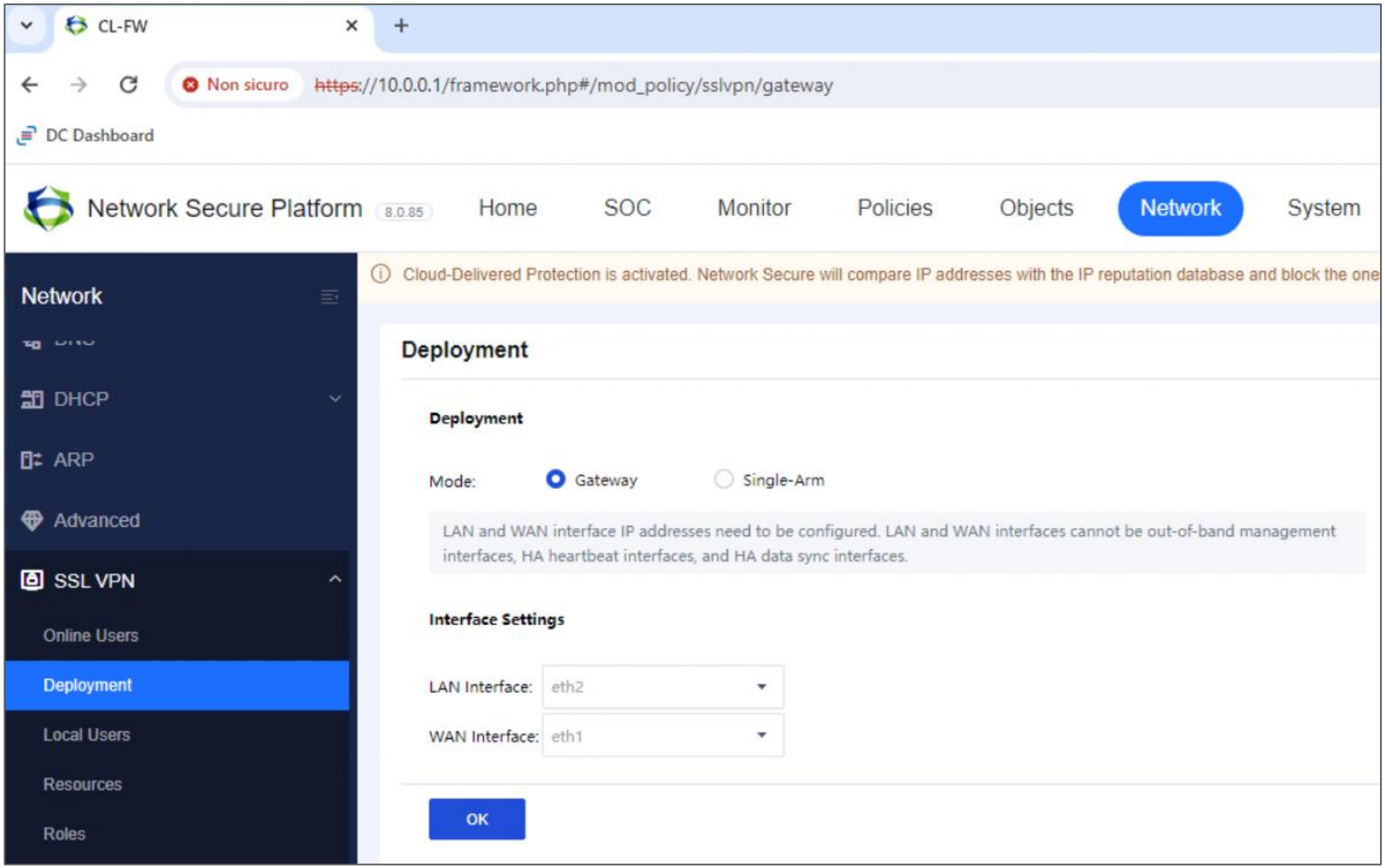
### 2.1.1 Modalità di distribuzione della VPN SSL NGAF

**Passo 1.** Definire le interfacce che la VPN SSL Sangfor deve utilizzare.

Per fare ciò, è necessario andare su **Network > SSL VPN > Deployment** .

In questa guida vedremo la modalità di distribuzione gateway.

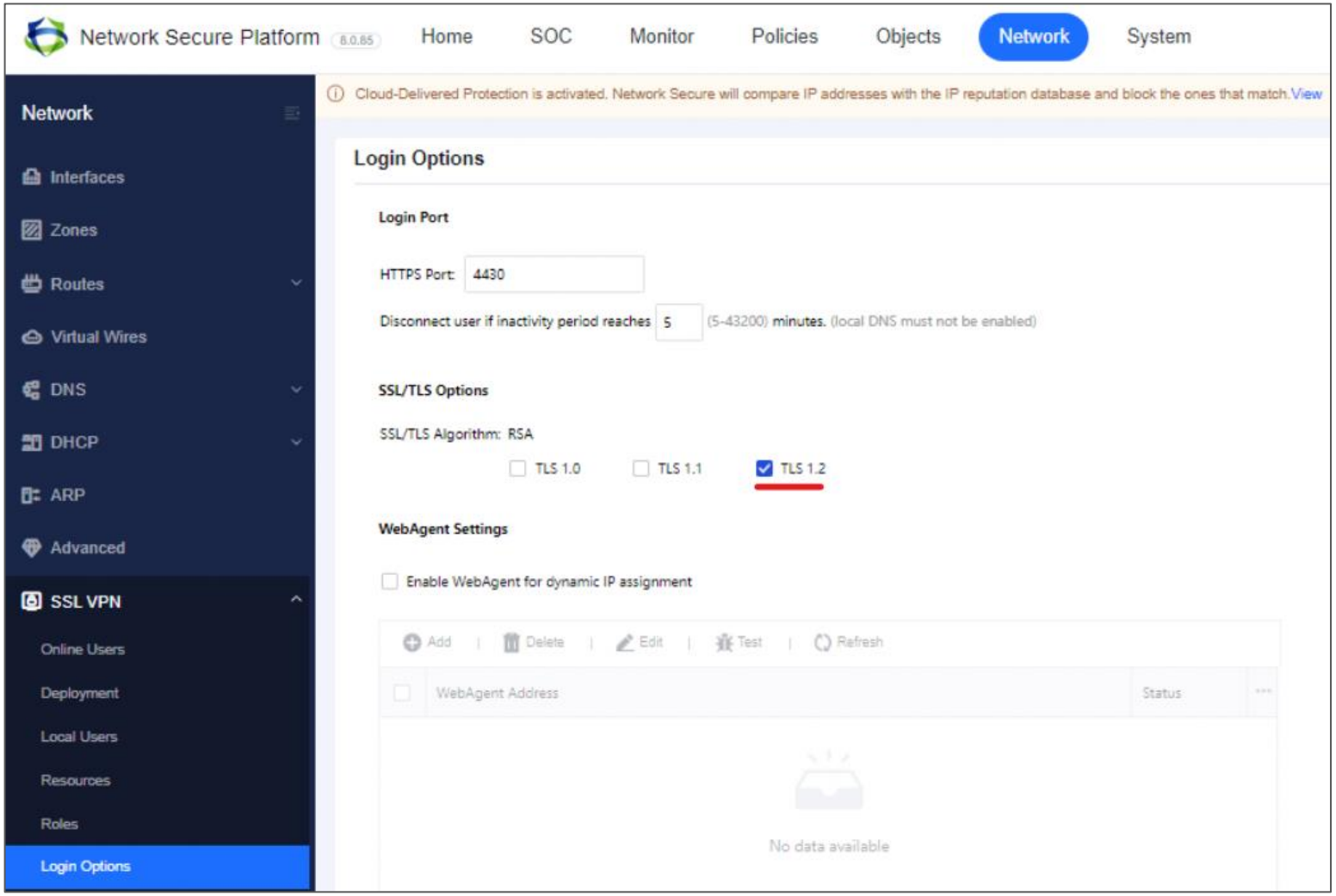
Nella schermata successiva, è necessario selezionare correttamente le interfacce Ethernet su Sangfor NGAF (nell'esempio, abbiamo eth1 come WAN e eth2 come LAN Layer 3):




In seguito, è possibile selezionare la porta cui sarà disponibile il portale web per la VPN SSL.

Per far ciò, dall'interfaccia web del firewall è necessario recarsi su **Network > SSL VPN > Login options**

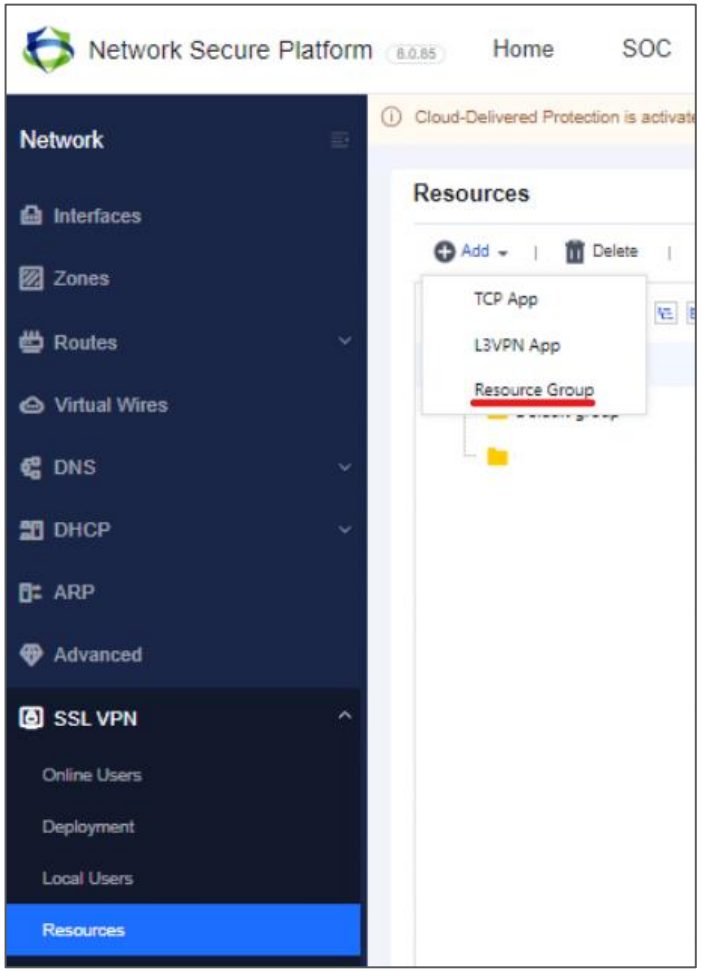
Abilitare solamente la versione TLS 1.2 per fini di sicurezza.

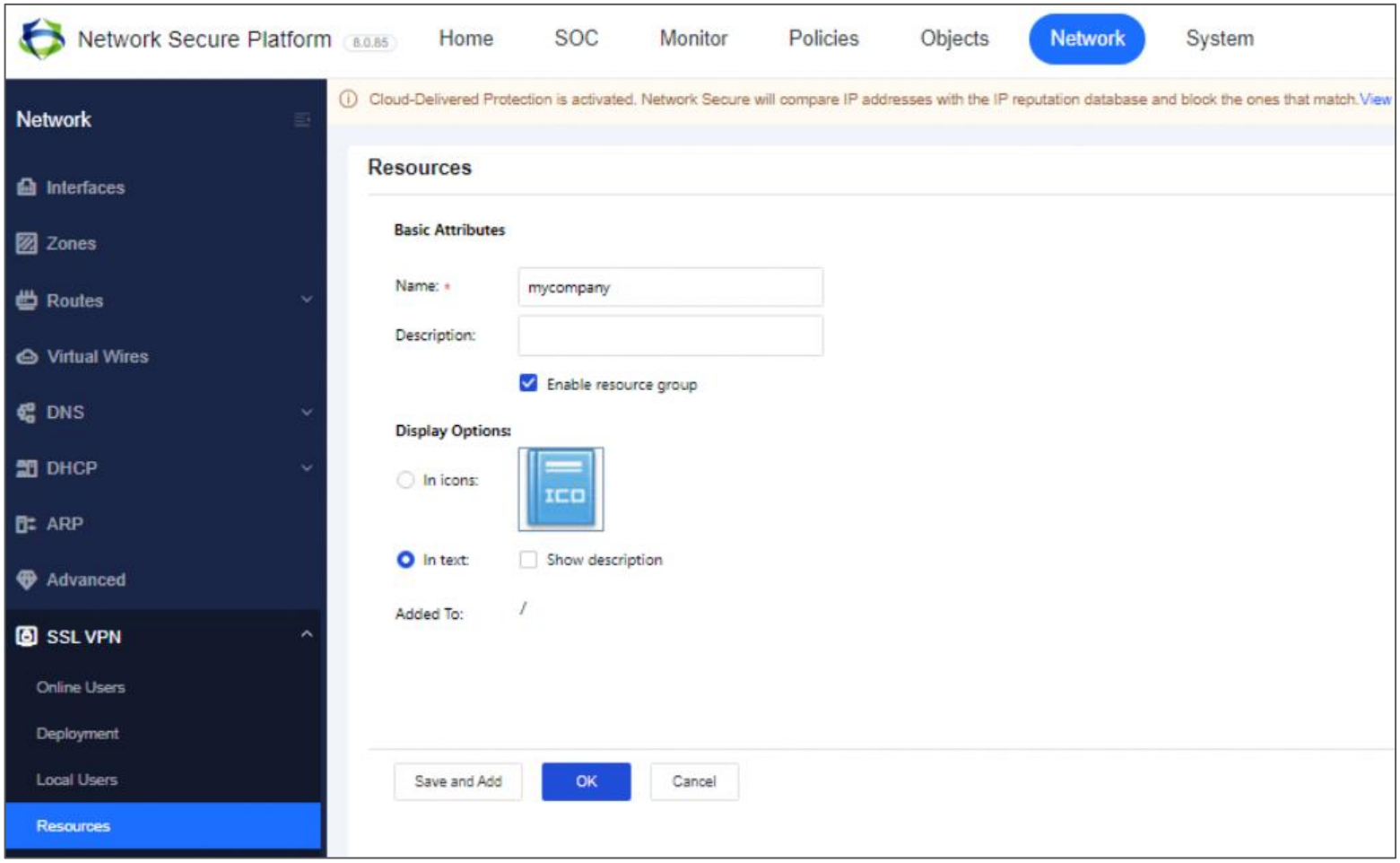



## 2.1.2 Creazione risorse NGAF VPN SSL

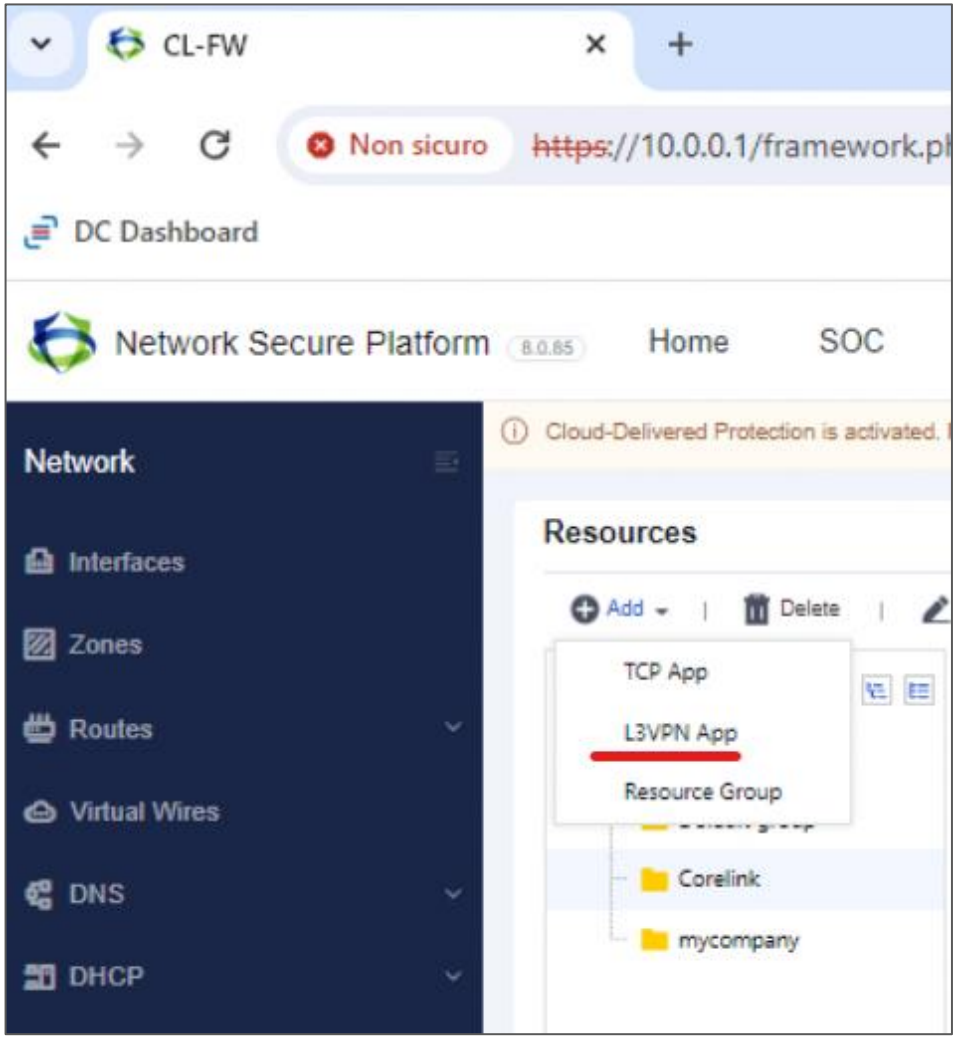
A questo punto è possibile creare un gruppo di risorse al fine di raggrupparle assieme

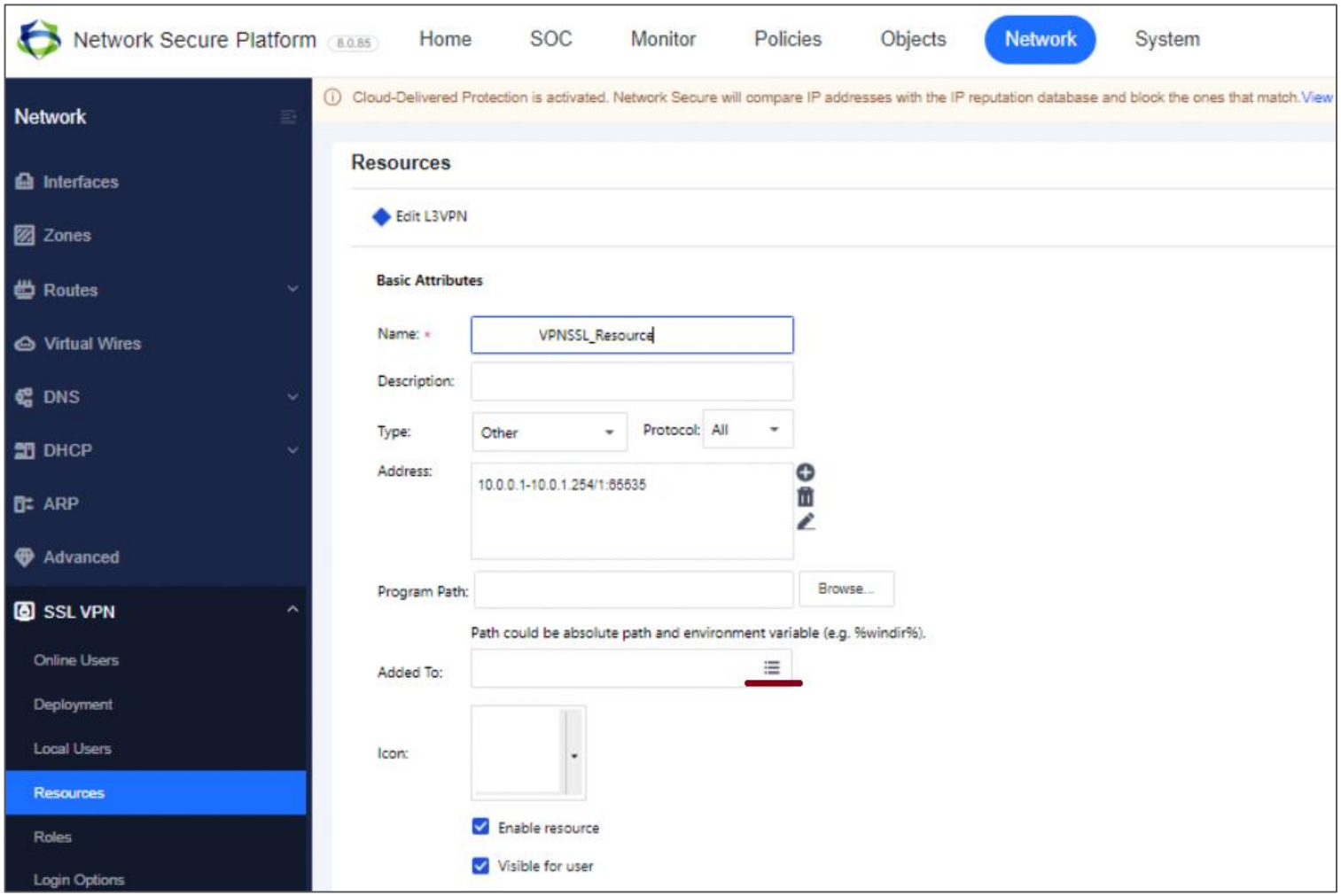
Per far ciò, recarsi su **Network > SSL VPN > Resources** e creare un nuovo gruppo di risorse (in quest'esempio ne ho creato uno chiamato mycompany)


Network Secure Platform
8.0.85
Home
SOC
Network
Interfaces
Zones
Routes
Virtual Wires
DNS
DHCP
ARP
Advanced
SSL VPN
Online Users
Deployment
Local Users
Resources
Cloud-Delivered Protection is activat
Resources
Add
Delete
TCP App
L3VPN App
Resource Group




Ora sulla stessa pagina, possiamo definire la rete interna come risorsa creando un'app L3VPN e inserendo i dettagli della tua rete come segue (nel nostro esempio abbiamo 10.0.0.0/22 come rete interna). Non dimenticare di specificare il gruppo di risorse creato in precedenza.


CL-FW
Non sicuro
https://10.0.0.1/framework.pl
DC Dashboard
Network Secure Platform
8.0.85
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



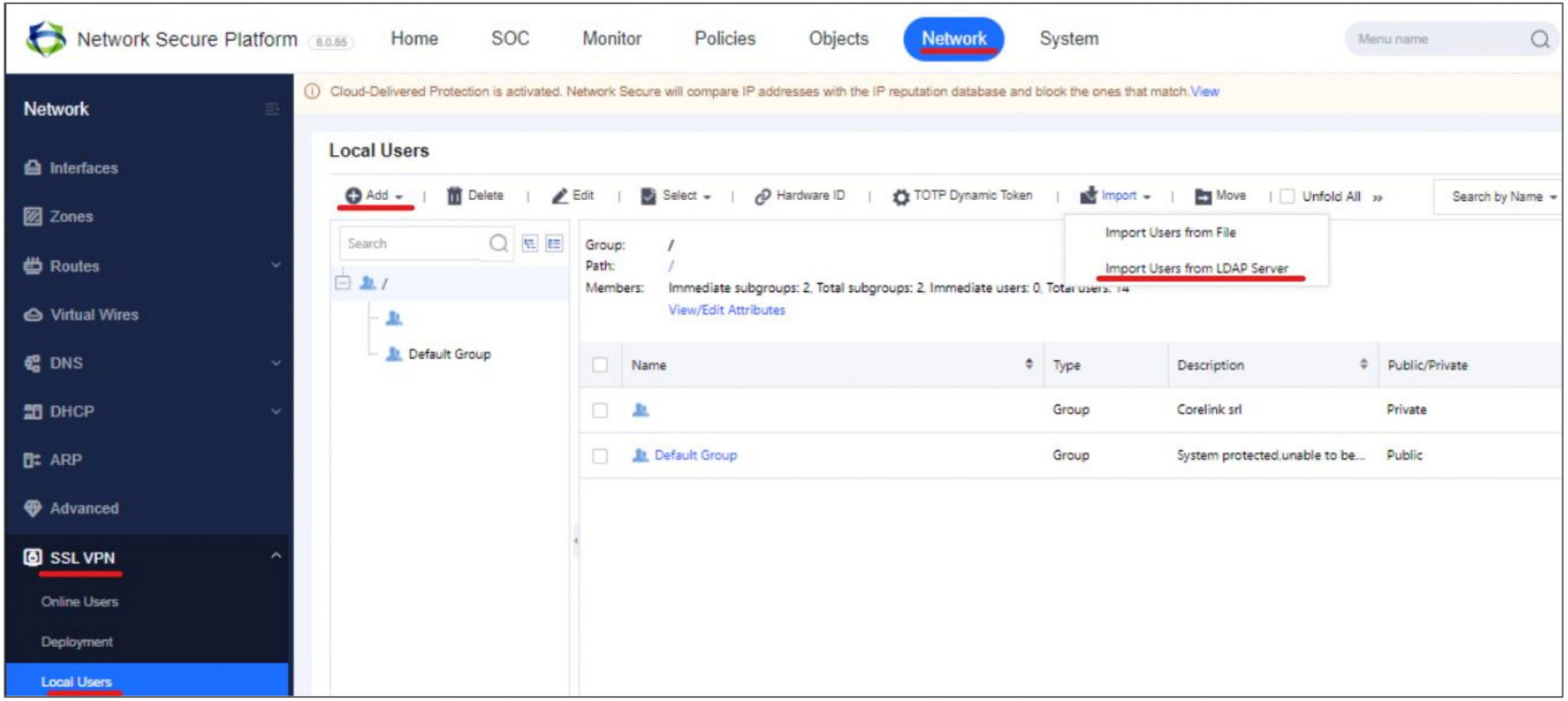

In modalità L3VPN App, il client VPN installerà una scheda di rete virtuale per instradare tutto il traffico attraverso di essa (qualsiasi protocollo). Tuttavia, se hai alcuni client a 32 bit, è meglio utilizzare l'altra opzione (TCP App) per creare un elemento di risorsa, poiché utilizza un dispositivo proxy per instradare solo le connessioni TCP.

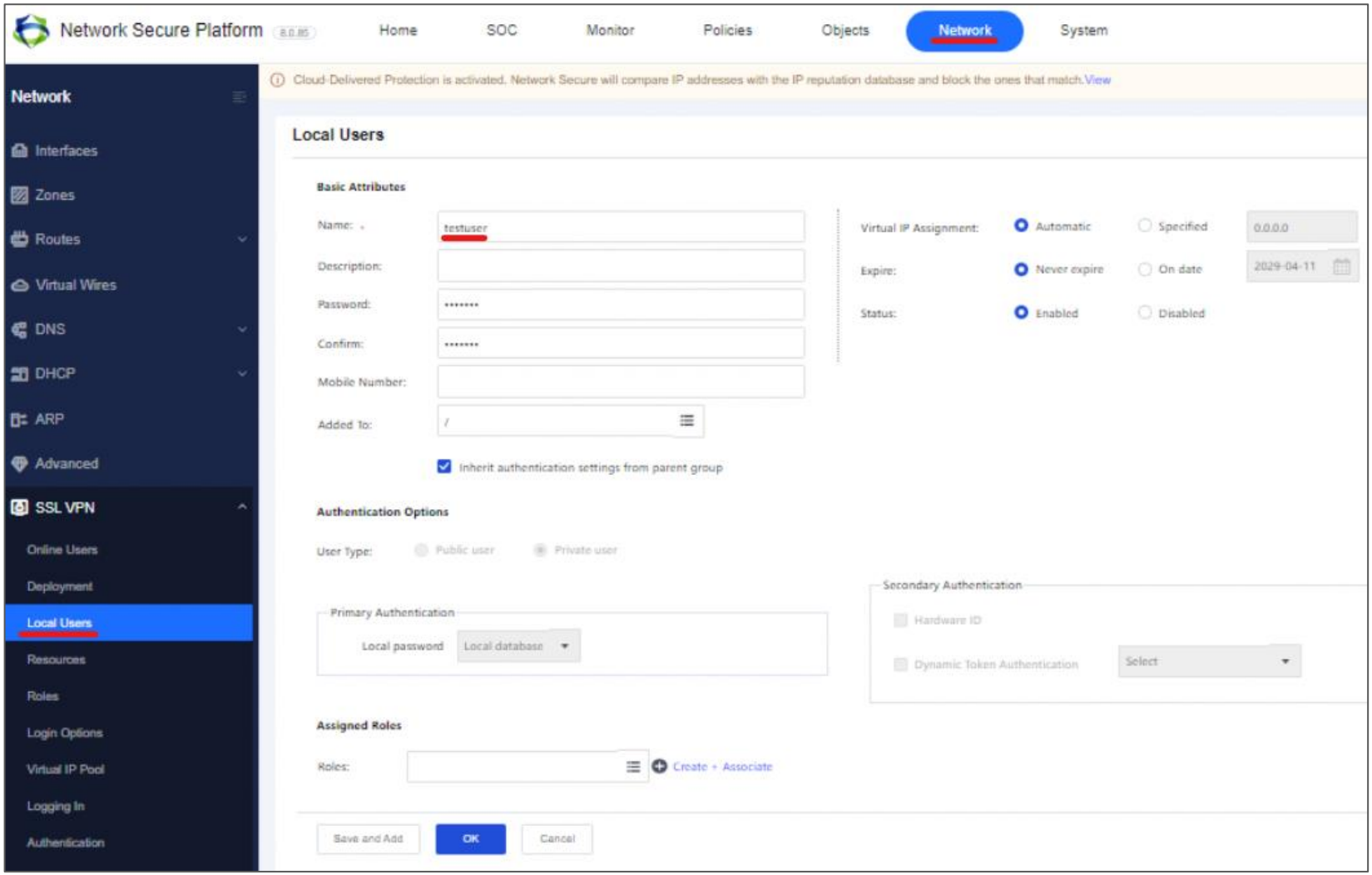
### 2.1.3 Creazione utente NGAF VPN SSL

Ora sulla seguente pagina dell'interfaccia web, possiamo scegliere di creare un utente locale o importare un elenco di utenti da fonti esterne (è necessario configurarlo prima su Sangfor NGAF).

**Network > SSL VPN > Local Users**

In questo esempio, scegliamo di creare un utente locale chiamato testuser:



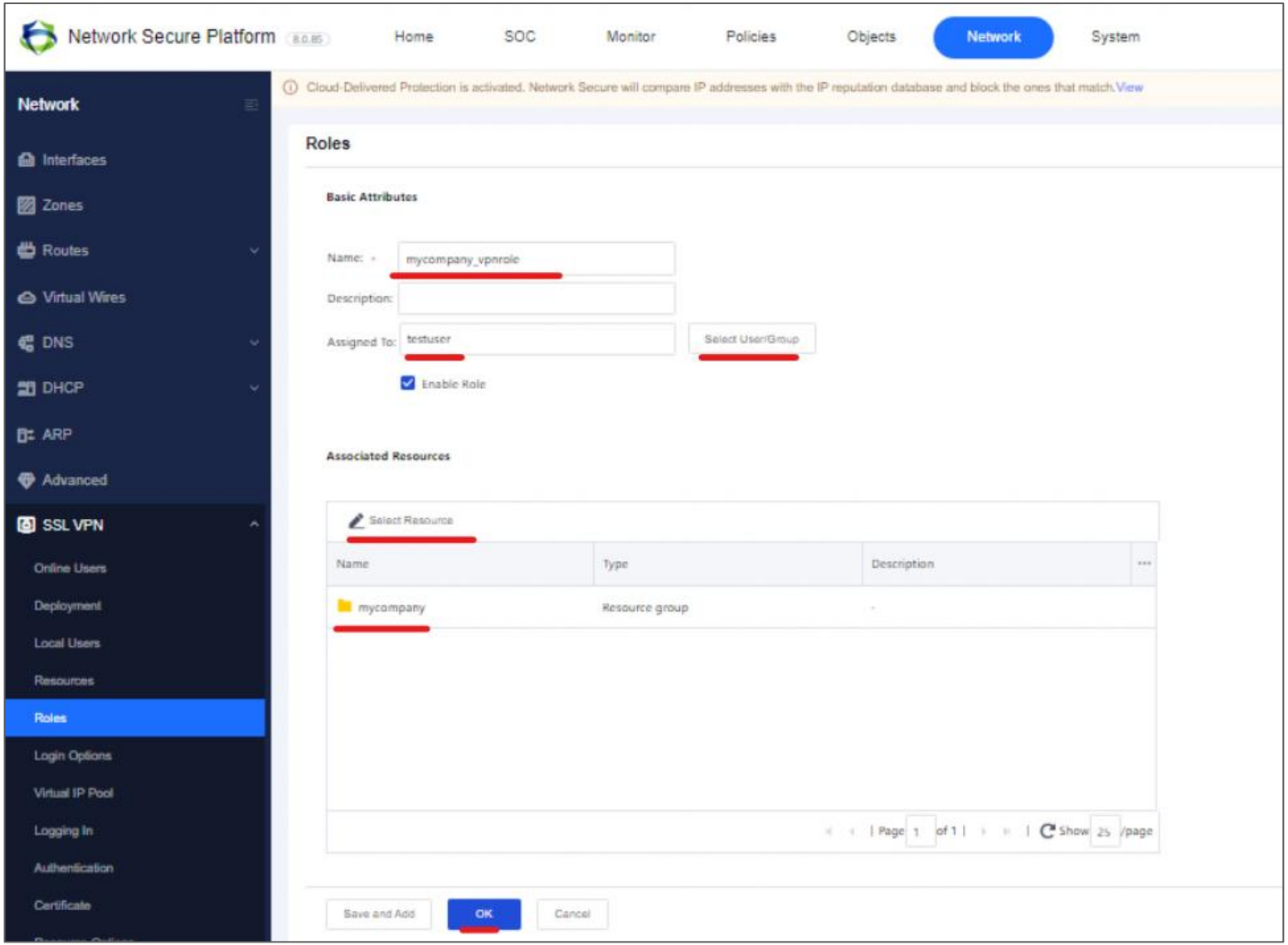



## 2.1.4 Assegnazione ruolo NGAF VPN SSL

In questa fase, è necessario assegnare un ruolo al nuovo utente creato per concedere la connessione VPN SSL.

Per farlo, devi andare su **Network > SSL VPN > Roles** e assegnare un ruolo.

Nel nostro esempio, creeremo un nuovo ruolo per consentire a testuser di connettersi alle risorse presenti nel gruppo di risorse creato in precedenza (chiamato mycompany)



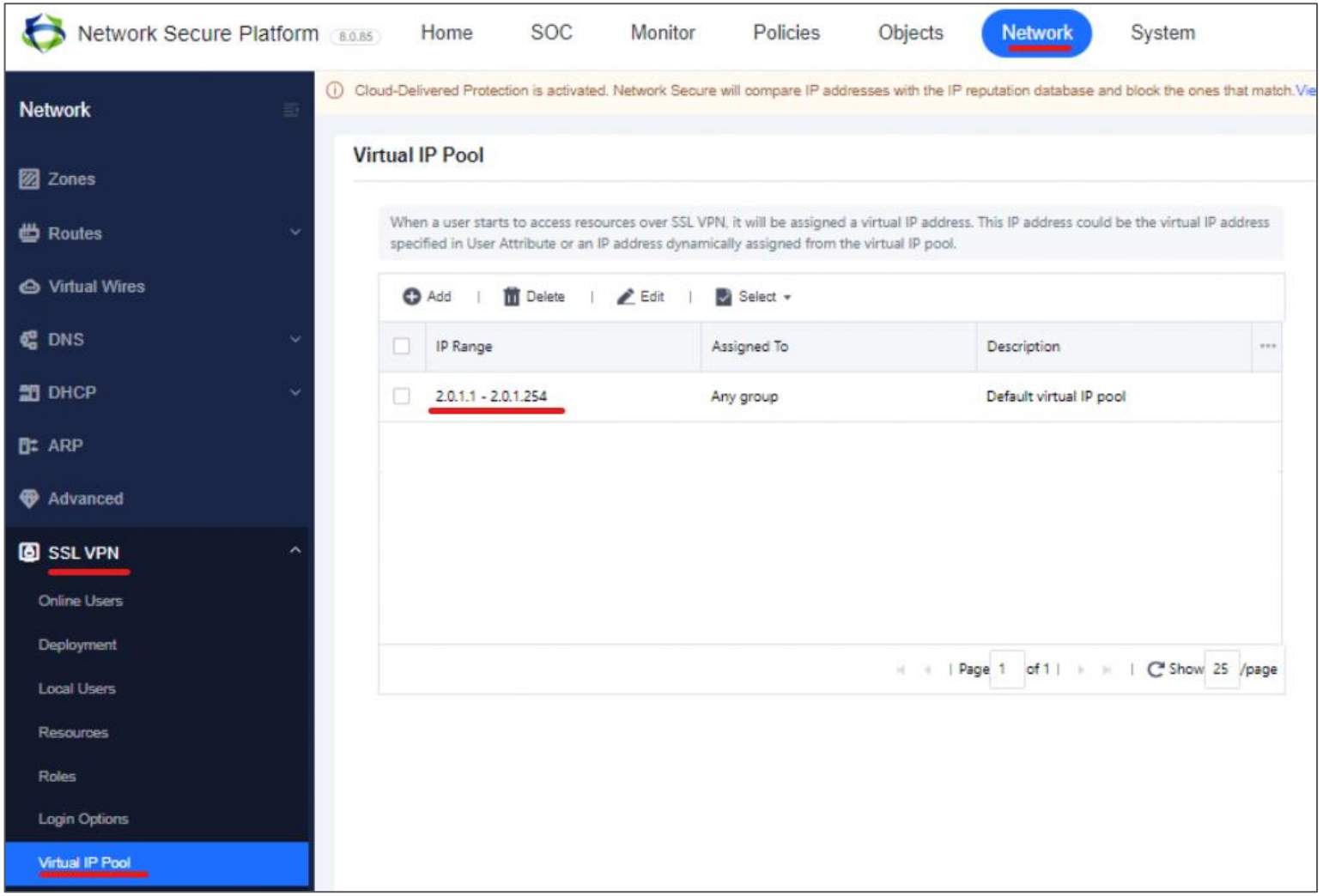
### 2.1.5 Ip pool virtuale NGAF VPN SSL

Nella sezione seguente, vedremo quale intervallo di indirizzi IP assegnare agli utenti VPN SSL che si connettono dall'esterno utilizzando Sangfor VPN SSL.

Per un gruppo di risorse specifico, puoi definire un intervallo di indirizzi IP virtuali da utilizzare.

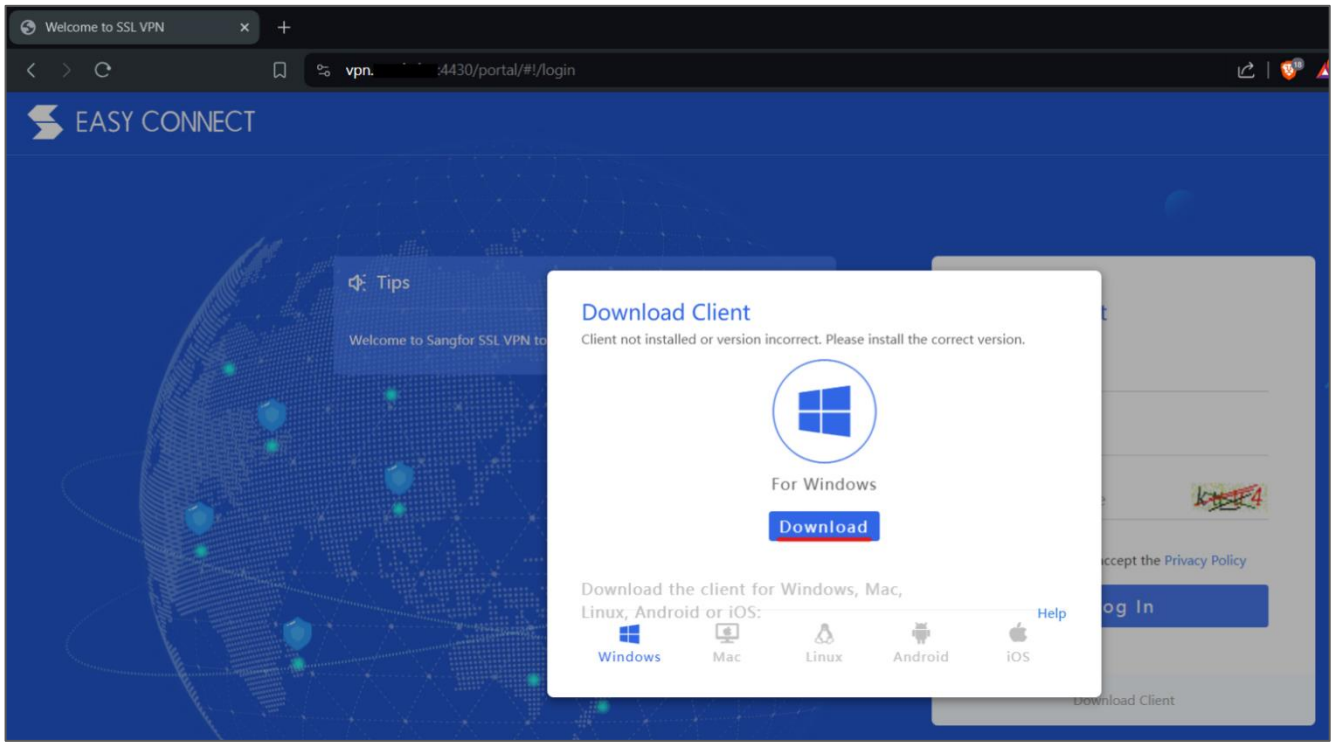
Per impostazione predefinita, esiste un intervallo di indirizzi IP virtuali da 2.0.1.1 a 2.0.1.254 per tutti i gruppi di risorse.

Consiglio di non eliminare questo intervallo di indirizzi IP virtuali predefinito.




### 2.1.6 Pagina accesso web NGAF VPN SSL

A questo punto gli utenti possono raggiungere la pagina di accesso web da reti esterne digitando l' indirizzo IP pubblico su un browser (è consigliato di creare un record di dominio specifico).




Come potete vedere, nella pagina web verrà chiesto di installare il client Sangfor EasyConnect sul PC. Dopo l'installazione, è possibile effettuare il login su questa pagina web per instaurare la connessione con Sangfor EasyConnect. Una volta effettuato il login, è possibile verificare sulla pagina web le risorse a cui si ha accesso.

## *3. Attenzione

Quando gli utenti esterni desiderano connettersi alle risorse intranet utilizzando Sangfor VPN SSL, è importante verificare che la rete locale dell'utente esterno non si sovrapponga con il pool di indirizzi IP virtuali o la rete intranet.