

#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):

The screenshot shows a web browser window with the address bar displaying `https://10.0.0.1/framework.php#/mod_policy/sslvpn/gateway`. The page title is "Network Secure Platform" with a version number "8.0.85". The navigation menu includes "Home", "SOC", "Monitor", "Policies", "Objects", "Network" (highlighted), and "System". The left sidebar shows the "Network" section expanded, with "SSL VPN" selected. The main content area is titled "Deployment" and contains the following settings:

- Deployment**
 - Mode: ☒ Gateway ☐ Single-Arm
 - Warning: LAN and WAN interface IP addresses need to be configured. LAN and WAN interfaces cannot be out-of-band management interfaces, HA heartbeat interfaces, and HA data sync interfaces.
- Interface Settings**
 - LAN Interface:
 - WAN Interface:
-

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.

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

+ Add | Delete | Edit | Test | Refresh

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

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

Interfaces

Zones

Routes

Virtual Wires

DNS

DHCP

ARP

Advanced

SSL VPN

Online Users

Deployment

Local Users

Resources

Cloud-Delivered Protection is activate

Resources

+ Add

Delete

TCP App

L3VPN App

Resource Group

Network Secure Platform 8.0.85

HomeSOCMonitorPoliciesObjectsNetworkSystem

Network

InterfacesZonesRoutesVirtual WiresDNSDHCPARPAdvancedSSL VPNOnline UsersDeploymentLocal UsersResources

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: *mycompany


Description:

☒ Enable resource group

Display Options:

☐ In icons:

☒ In text:



☐ Show description

Added To: /

Save and Add

OK


Cancel

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 8.0.65 Home SOC

Network

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

Resources

+ Add | Delete

TCP App

L3VPN App

Resource Group

Corelink

mycompany

Cloud-Delivered Protection is activated.

Network Secure Platform 8.0.85

HomeSOCMonitorPoliciesObjectsNetworkSystem

Network

InterfacesZonesRoutesVirtual WiresDNSDHCPARPAdvancedSSL VPNOnline UsersDeploymentLocal UsersResourcesRolesLogin Options

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

Resources

Edit L3VPN

Basic Attributes

Name: *VPNSSL_Resource

Description:

Type: OtherProtocol: All

Address:10.0.0.1-10.0.1.254/1:65535

Program Path:Browse...

Path could be absolute path and environment variable (e.g. %windir%).

Added To:

Icon:

☒ Enable resource

☒ Visible for user

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:

The screenshot displays the Sangfor Network Secure Platform web interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (selected), and 'System'. A search bar is located on the right. The left sidebar shows the 'Network' menu expanded, with 'SSL VPN' and 'Local Users' highlighted. The main content area is titled 'Local Users' and features a toolbar with options like 'Add', 'Delete', 'Edit', 'Select', 'Hardware ID', 'TOTP Dynamic Token', 'Import', 'Move', and 'Unfold All'. A search bar is also present. Below the toolbar, there is a tree view showing the 'Default Group'. The main table lists the following users:

Name	Type	Description	Public/Private
Corelink srl	Group		Private
Default Group	Group	System protected,unable to be...	Public

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

Network

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

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: testuser

Description:

Password: *****

Confirm: *****

Mobile Number:

Added To: /

☒ Inherit authentication settings from parent group

Virtual IP Assignment:

☒ Automatic ☐ Specified 0.0.0.0

Expire:

☒ Never expire ☐ On date 2029-04-11

Status:

☒ Enabled ☐ Disabled

Authentication Options

User Type: ☐ Public user ☒ Private user

Primary Authentication

Local password Local database

Secondary Authentication

☐ Hardware ID

☐ Dynamic Token Authentication Select

Assigned Roles

Roles: + Create + Associate

Save and Add OK Cancel

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)

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](#)

Roles

Basic Attributes

Name:

Description:

Assigned To:

☒ Enable Role

Associated Resources

Name	Type	Description	...
mycompany	Resource group		

Page 1 of 1 | Show 25 /page

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.

Network Secure Platform 8.0.85

HomeSOCMonitorPoliciesObjectsNetworkSystem

Network

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

Cloud-Delivered Protection is activated. Network Secure will compare IP addresses with the IP reputation database and block the ones that match.

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.

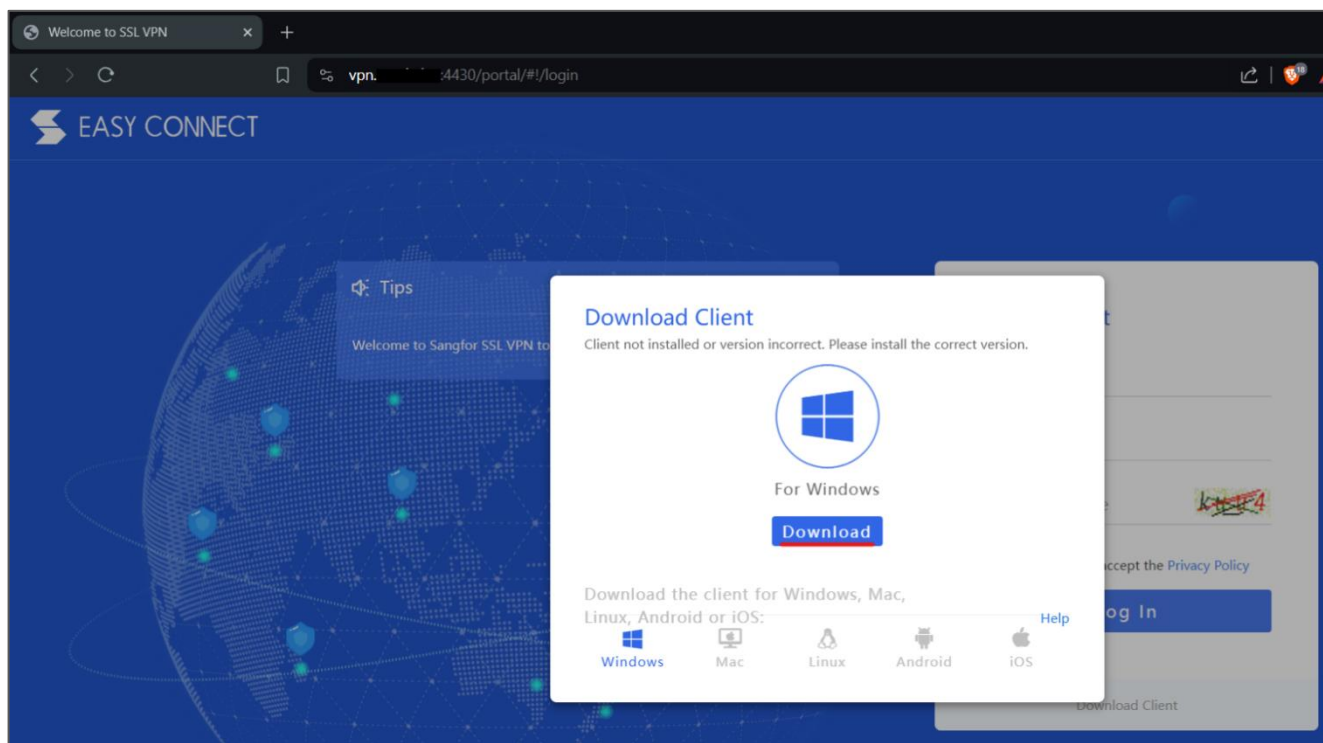
+ Add | Delete | Edit | Select

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

Page 1 of 1 | Show 25 /page

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.