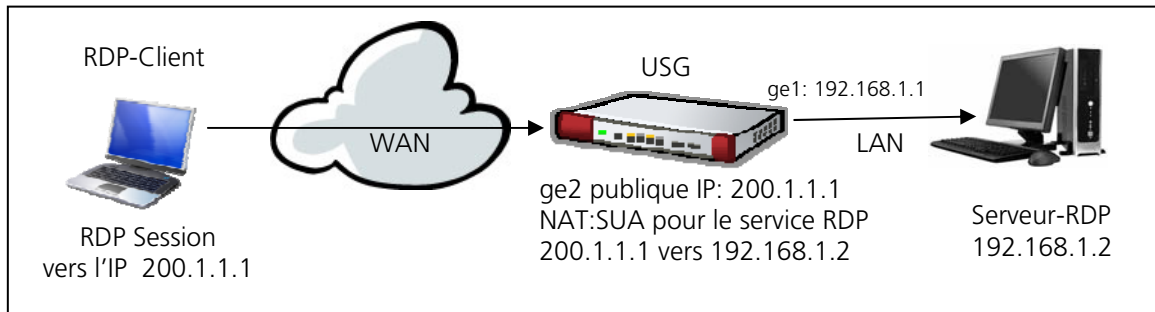


Virtual Server (NAT SUA) avec le ZyXEL USG

Cet exemple démontre, comment utiliser la fonction Virtual-Server afin d'accéder vers un serveur RDP (Connexion Bureau à distance) placé sur le réseau privé du USG depuis le réseau Internet public en lui attribuant la même adresse publique que celle du USG coté WAN (ge2). Le mode utilisé est le SUA.



Menu **Network** → **Virtual server**.



Edition et **activation** (Enable) d'une nouvelle règle, attribuer un **nom** à cette règle. Pour **Incoming Interface** choisir l'interface **ge2** (Interface WAN de l'USG). Ensuite créer un objet pour **Original IP** avec **Create Object**.

The screenshot shows the 'General Setup' and 'Mapping Rule' sections of the configuration interface. In the 'General Setup' section, 'Enable Rule' is checked, and the 'Rule Name' is 'RDP-Server'. In the 'Mapping Rule' section, the 'Incoming Interface' is set to 'ge2'. The 'Original IP' dropdown is open, showing options: 'any', 'any', 'User Defined', and 'Create Object (Address)'. The 'Mapped IP' is set to 'any' and the 'Port Mapping Type' is 'Any'.

Attribuer un **Nom** à cet objet, **Address Type** est **HOST** et rentrer sur **IP Adresse** l'adresse publique (200.1.1.1) de l'USG (ge2).

The screenshot shows the 'Configuration' screen for creating a new object. The 'Name' field contains 'RDP-Public', the 'Address Type' is set to 'HOST', and the 'IP Address' field contains '200.1.1.1'. 'OK' and 'Cancel' buttons are visible at the bottom.

Créer un objet pour la **Mapped IP** en utilisant le **Create Object**.

General Setup

Enable Rule
Rule Name: RDP-Server

Mapping Rule

Incoming Interface: ge2
Original IP: RDP-Public
Mapped IP: User Defined
User-Defined Mapped IP: Create Object (Address)
Port Mapping Type: RDP-Public

Attribuer un Nom à cet objet, **Address Type** est aussi **HOST**, rentrer sur **IP Adresse** l'adresse IP privé (192.168.1.2) du serveur-RDP.

Configuration

Name: RDP-local
Address Type: HOST
IP Address: 192.168.1.2

OK Cancel

Créer un Objet pour le **Original Service** avec **Create Object**.

General Setup

Enable Rule
Rule Name: RDP-Server

Mapping Rule

Incoming Interface: ge2
Original IP: RDP-Public
Mapped IP: RDP-local
Port Mapping Type: Service
Original Service: Create Object
Mapped Service: None

Related Settings

Any_UDP
Any_TCP

RDP-service avec le Protocole **TCP** et le Port **3389** comme **Starting Port** et **Ending Port**.

Configuration

Name: RDP-service
IP Protocol: TCP
Starting Port: 3389 (1..65535)
Ending Port: 3389 (1..65535)

OK Cancel

Choisir aussi le **RDP-service** pour le **Mapped Service**. Sauver la règle en cliquant sur **OK**.

General Setup

Enable Rule
Rule Name: RDP-Server

Mapping Rule

Incoming Interface: ge2
Original IP: RDP-Public
Mapped IP: RDP-local
Port Mapping Type: Service
Original Service: RDP-service
Mapped Service: RDP-service

Related Settings

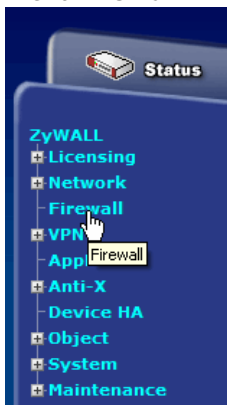
Add corresponding [Policy Route](#) rule for NAT 1:1 mapping.
 Add corresponding [Policy Route](#) rule for NAT Loopback.
[Configure Firewall](#)

OK Cancel

Ajout d'une Policy Route afin d'accéder au serveur RDP local via son IP publique ou bien son nom URL à partir du réseau local.

Maintenant une règle sur le Par-feu (Firewall) est indispensable.

Menu **Firewall**.



La règle est configuré de cette façon: **Activation** de la règle = **Enable** / **From** (depuis la zone) = **WAN** / **To** (vers la zone) = **LAN** / Donner un **Nom** (Description) à cette règle / **Destination** (déstination IP) = **RDP-local** / **Service** (service) = **RDP-service** / **Access** (accès) = **allow** (permit) / **Log** = **log** (tous les accès seront inscrits sur le journal) / Sauver la règle avec **OK**.

Configuration

Enable
From: WAN
To: LAN
Description: RDP-server
Schedule: none
User: any
Source: any
Destination: RDP-local
Service: RDP-service
Access: allow
Log: log

OK Cancel