qBittorrent

La configuration de qBittorrent est un peu particulière pour éviter de sortir directement avec les IPs d'Altaïr. Un point de sortie (ici Alshain) est utilisé, et tout le traffic de qBittorrent est routé par ce point de sortie. Un tunnel Wireguard assure la liaison entre Altaïr et Alshain. L'IPv6 est routée directement alors que l'IPv4 est NATé (en deux fois, sur Altaïr et sur Alshain pour le moment).

Configuration réseaux :

Serveur	Interace	IP/Masque	Description
Alshain	int-ppsfleet	10.114.20.1/24	Réseau privée interne entre serveur PPSFleet.
Alshain	int-ppsfleet	2001:bc8:24d8:114:20::1/80	Équivalent IPv6 du réseau précédant. Le découpage du réseau est fait par bloc de 16 bits de manière à ce que chanque client aie un /96.
Altaïr	int-ppsfleet	10.114.20.10/24	IPv4 du client VPN sur Altaïr
Altaïr	int-ppsfleet	2001:bc8:24d8:114:20:10:0:1/112	IPv6 du client VPN sur Altaïr. Un sous découpage en /112 par interace dans ce /96 sur Altaïr.
Altaïr	net-external	10.89.0.1/24	Réseau IPv4 des conteneurs sortant via le VPN. Ce réseau est NATé sur Altaïr de manière à ce que le point de sortie ne voit que l'IP du client VPN.
Altaïr	net-external	2001:bc8:24d8:114:20:10:1:0/112	Réseau IPv6 des conteneurs sortant via le VPN.

Configuration du point VPN pour le point de sortie

1. Création les clés pour l'autentification et le chiffrement.

```
# Altaïr
bash -c '(umask 0077; wg genkey > altair.key)'
wg pubkey < altair.key > altair.pub
# Alshain
bash -c '(umask 0077; wg genkey > alshain.key)'
wg pubkey < alshain.key > alshain.pub

# Secret partagé
wg genpsk > altair-alshain.psk
```

2. Configurer le réseau sur Alshain en éditant le fichier `/etc/NetworkManager/system-connections/int-ppsfleet.nmconnection`

```
[connection]
id=int-ppsfleet
type=wireguard
interface-name=int-ppsfleet

[wireguard]
listen-port=51756
private-key=$ALSHAIN_PRIVATE_KEY

[wireguard-peer.$ALTAIR_PUBLIC_KEY]
preshared-key=$ALTAIR_ALSHAIN_SHARED_SECRET
preshared-key-flags=0
allowed-ips=10.114.20.10/32;2001:bc8:24d8:114:20:10::/96;

[ipv4]
address1=10.114.20.1/24
method=manual

[ipv6]
address1=2001:bc8:24d8:114:20::1/80
addr-gen-mode=stable-privacy
method=manual
```

3. Redémarrer NetworkManager sur Alshain

```
sudo systemctl restart NetworkManager
```

Configuration du réseau sur Altaïr

1. Créer la table de routage `external` avec comme ID `200` en ajoutant la ligne suivante au fichier `/etc/iproute2/rt_tables`.

```
200 external
```

2. Configurer le client VPN sur Altaïr en utilisant les clés générées précédemment. Créer le fichier `/etc/NetworkManager/system-connections/int-ppsfleet.nmconnection` avec le contenu suivant.

```
[connection]
id=int-ppsfleet
uuid=fe155cee-4941-3f9b-a441-a7fd21d2412a
type=wireguard
interface-name=int-ppsfleet

[wireguard]
peer-routes=false
private-key=$ALTAIR_PRIVATE_KEY

[wireguard-peer.$ALSHAIN_PUBLIC_KEY]
endpoint=[2001:bc8:24d8::]:51756
preshared-key=$ALTAIR_ALSHAIN_SHARED_SECRET
preshared-key-flags=0
allowed-ips=0.0.0.0/0;::/0;

[ipv4]
address1=10.114.20.10/24
method=manual
route-table=200
gateway=10.114.20.1
routing-rule1=priority 5 oif int-ppsfleet table 200

[ipv6]
addr-gen-mode=stable-privacy
address1=2001:bc8:24d8:114:20:10::1/112
method=manual
route-table=200
```

```
gateway=2001:bc8:24d8:114:20::1
routing-rule1=priority 5 oif int-ppsfleet table 200
```

3. Configurer l'interface de bridge pour les conteneurs en créant le fichier `/etc/NetworkManager/system-connections/net-external.nmconnection` avec le contenu suivant.

```
[connection]
id=net-external
uuid=d72a0e46-85bc-4b4c-bb64-fb904c463894
type=bridge
autoconnect=true
interface-name=net-external

[ethernet]

[bridge]
stp=false

[ipv4]
address1=10.89.0.1/24
method=manual
route-table=200
routing-rule1=priority 5 from 10.89.0.0/24 table 200

[ipv6]
addr-gen-mode=default
address1=2001:bc8:24d8:114:20:10:1:1/112
method=manual
route-table=200
routing-rule1=priority 5 from 2001:bc8:24d8:114:20:10:1:0/112 table 200
```

4. Redémarrer NetworkManager.

```
sudo systemctl restart NetworkManager
```

5. Configurer le firewall pour éviter d'avoir du NAT sur l'IPv6 en ajoutant les lignes suivante au fichier `/etc/sysconfig/nftables.conf`

```
table ip6 nat {
  chain POSTROUTING {
    type nat hook postrouting priority srcnat; policy accept;
```

```
    ip6 saddr 2001:bc8:24d8:114:20:10:1:0/112 return
    #iifname tun0 masquerade
  }
}
```

6. Puis redémarrer nftables.

```
sudo systemctl restart nftables
```

Créer le conteneur qBittorrent sur Altaïr

1. Créer le réseau Podman

```
nmcli c down net-external
podman network create --subnet 10.89.0.0/24 --subnet 2001:bc8:24d8:114:20:10:1:0/112 --interface-name=net-external --ignore net-external
nmcli c up net-external
```

2. Démarrer le conteneur qBittorrent une première fois

```
sudo podman run -d --name=qbittorrent \
  -e PUID=985 -e PGID=985 -e TZ=Europe/Paris -e WEBUI_PORT=8080 \
  -p '[::1]:8080:8080' -p 127.0.0.1:8080:8080 -p 6881:6881 -p 6881:6881/udp \
  -v /var/opt/qbittorrent/config:/config:Z -v /data/downloads:/downloads:Z \
  --restart always \
  --network net-external \
  lscr.io/linuxserver/qbittorrent:latest
```

3. Créer une policy SELinux custom (voir page sur le SELinux du wiki), et re-run le conteneur avec la policy

```
sudo podman run --security-opt label=type:qbittorrent.process \
  -d --name=qbittorrent \
  -e PUID=985 -e PGID=985 -e TZ=Europe/Paris -e WEBUI_PORT=8080 \
  -p '[::1]:8080:8080' -p 127.0.0.1:8080:8080 -p 6881:6881 -p 6881:6881/udp \
  -v /var/opt/qbittorrent/config:/config -v /data/downloads:/data/downloads \
  --restart always \
  --network net-external \
```

```
lscr.io/linuxserver/qbittorrent:latest
```

4. Créer le service associé et l'activer

```
sudo podman generate systemd --new --name qbittorrent | sudo tee
/etc/systemd/system/qbittorrent.service
systemctl daemon-reload
systemctl enable qbittorrent
```

Révision #12
Créé 28 mai 2023 17:31:43 par blacksponge
Mis à jour 10 mai 2024 22:15:13 par blacksponge