OVH VPS

Since I no longer have public IPv4 assigned to my modem/router and no way to enable modem/bridge mode I use VPS to terminate incoming traffic for HTTP and VPN-in.

- Type: VPS `vps2020-starter-1-2-20` (1 vcore, 2 GiB RAM, 20 GB HDD)
- Location: London `os-uk2`
- OS: AlmaLinux 9
- IPv4: `57.128.183.232`
- IPv6: `fe80::f816:3eff:fe78:d4a7/64`

Justine (`172.17.100.3`) and Server-gw (`172.17.100.2`) establish VPN connection to it on port `51322` using `172.17.100.1/24` VPS.

```
[Interface]
PrivateKey = <REDACTED>
MTU = 1380
ListenPort = 51322
Address = 172.17.100.1/24

[Peer]
PublicKey = PTu13g5XRIVt+i1DL3g5QujHwL6TJaHkC9z8Kw7pwQE=
AllowedIPs = 172.17.100.2/32
PersistentKeepalive = 300

[Peer]
PublicKey = EnRj9UgoE1qyQ9qK9OU3jZ39tpAo24FTZMdT6nQN0wY=
AllowedIPs = 172.17.100.3/32
PersistentKeepalive = 300
```

IP tables configuration is used to forward packets to Justine and Server-gw:

```
iptables -P INPUT DROP
iptables -A INPUT ! -i vps -d 172.17.100.0/24 -j DROP
iptables -A INPUT -p icmp -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -m tcp -p tcp --dport 22 -m recent --rcheck --seconds 30 --name SSH -j
ACCEPT
iptables -A INPUT -m tcp -p tcp --dport <REDACTED> -m recent --set --name SSH -j DROP
```

```
iptables -A INPUT -p udp -m udp --dport 51322 -j ACCEPT

sysctl net.ipv4.ip_forward=1
iptables -P FORWARD DROP
iptables -A FORWARD -o vps -i eth0 -j ACCEPT
iptables -A FORWARD -i vps -o eth0 -j ACCEPT

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -o vps -d 172.17.100.3 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination
172.17.100.2:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination
172.17.100.2:443
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 4443 -j DNAT --to-destination
172.17.100.2:4443
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 10000 -j DNAT --to-destination
172.17.100.2:10000
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25565 -j DNAT --to-destination
172.17.100.2:25565
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 34563 -j DNAT --to-destination
172.17.100.3:51821
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 34564 -j DNAT --to-destination
172.17.100.3:51822
```

Vps acts as VPN router for all traffic for Server-gw and by extension for all SERVER VLAN hosts. This way enter and exit IP for servers is the public IP of Vps. Servers can also see original client IP as it is not NATed on the way in.

For VPN-in Vps will NAT connections to Justine since Justine uses Mullvad or ISP IP as default G/W.

Blocking forwarded traffic

```
ipset create forward-drop hash:net
iptables -I FORWARD 1 -m set --match-set forward-drop src -j DROP
```

List IP and add IP to block list:

```
ipset list
ipset add forward-drop 66.249.0.0/16
```

Revision #10
Created 2024-11-29 18:54:53 GMT by hxd
Updated 2025-12-06 19:49:48 GMT by hxd