

Runcloud + Iptable + redirection + proxypass

il faut desactiver firewalld de runcloud pour minimiser les soucis

Quand on met ce script

```
#!/bin/bash
sleep 2
echo "FIREWALL OK";

#Install iptables if you haven't already
#Alternatively use packet manager of your choice
#apt-get install iptables

#Allow all incoming traffic to begin with
sudo iptables -P INPUT ACCEPT
#Clean out any existing input rules. You may also remove the "INPUT" argument and run only "iptables -F" to
clear all chains. When doing so, make sure there are no rules in other chains that you still need (list via "iptables
-L"), for example Oracle cloud servers will have preset rules, which should not be removed.
sudo iptables -F INPUT

#Allow all internal connections
sudo iptables -A INPUT -i lo -j ACCEPT

#Allow continuing setup connections
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#Allow ssh, adjust port if you run it on non-default

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT #SSH
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 34210 -j ACCEPT
```

```
sudo iptables -A INPUT -p udp --dport 22 -j ACCEPT #SSH
sudo iptables -A INPUT -p udp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p udp --dport 34210 -j ACCEPT

# Ajouter les règles de redirection
sudo iptables -t nat -A PREROUTING -p udp --dport 50120 -j DNAT --to-destination 176.9.63.27:40120
sudo iptables -t nat -A PREROUTING -p tcp --dport 50120 -j DNAT --to-destination 176.9.63.27:40120
# Ajouter la règle de masquage
sudo iptables -t nat -A POSTROUTING -j MASQUERADE

# Activer l'IP forwarding temporairement
sudo sysctl -w net.ipv4.ip_forward=1

sudo iptables -P INPUT DROP

#Block all forwarding
#sudo iptables -P FORWARD DROP

#Allow all outgoing
sudo iptables -P OUTPUT ACCEPT
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

Nous ne pouvons plus ping alors il faut modifier le resolv.conf pour mettre des nameserver autre que celui present mais apres un reboot ça disparaît.

Pour ajouter des lignes permanentes dans `/etc/resolv.conf` vous pourriez installer le `resolvconf` ligne de commande:

```
sudo apt install resolvconf
```

alors tu dois éditer `/etc/resolvconf/resolv.conf.d/head` et ajoutez les lignes permanentes dont vous avez besoin. Par exemple:

```
nameserver 8.8.8.8
nameserver 1.1.1.1
```

et enfin exécutez ces commandes :

```
sudo resolvconf --enable-updates  
sudo resolvconf -u
```

Un petit script pour reset l'iptables au cas ou

```
#!/bin/bash  
  
# Vider toutes les règles  
sudo iptables -F  
sudo iptables -t nat -F  
sudo iptables -t mangle -F  
sudo iptables -t raw -F  
  
# Supprimer toutes les chaînes personnalisées  
sudo iptables -X  
sudo iptables -t nat -X  
sudo iptables -t mangle -X  
sudo iptables -t raw -X  
  
# Réinitialiser toutes les politiques par défaut à ACCEPT  
sudo iptables -P INPUT ACCEPT  
sudo iptables -P FORWARD ACCEPT  
sudo iptables -P OUTPUT ACCEPT  
  
# Vérifier les règles  
sudo iptables -L -v -n  
sudo iptables -t nat -L -v -n
```

Et ça devrait etre bon vérifié si ping google.com focntionne bien et que rundcloud agent fonctionne bien et est détecter par le panel rundcloud.

Revision #4

Created 3 July 2024 03:14:03 by alexwilliam

Updated 3 July 2024 13:18:33 by alexwilliam