OpenVPN - Firewall Configuration

FirewallD

Use the following commands to open all ports required by OpenVPN:

```
firewall-cmd --list-services
firewall-cmd --permanent --add-service openvpn
firewall-cmd --permanent --add-masquerade
firewall-cmd --query-masquerade
firewall-cmd --reload
```

IPTables

My IPTables configuration `/etc/iptables/iptables.rules` for OpenVPN:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [32:2712]
:LOGGING - [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp -m icmp --icmp-type 0 -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo0 -m comment --comment "Allow loopback lo0" -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT
-A INPUT -j LOGGING
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -i tun+ -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A LOGGING -j LOG --log-prefix "DROPPED: " \--log-level 7
-A LOGGING -j DROP
COMMIT
# Completed on Mon Jun 30 06:48:44 2014
# Generated by iptables-save v1.4.7 on Mon Jun 30 06:48:44 2014
```

```
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [2:165]
:OUTPUT ACCEPT [2:165]
-A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
COMMIT
```

Revision #1
Created 11 April 2017 21:11:06 by Tingwai
Updated 17 April 2017 18:33:49 by Tingwai