GNU/Linux Administration - Support #976

Install WireGuard Server on Debian

04/10/2023 02:27 PM - Daniel Curtis

Status:	Resolved	**Start date:**	04/10/2023
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Server	**Estimated time:**	1.00 hour
Target version:	Debian	**Spent time:**	3.00 hours

Description

This is a guide on installing a WireGuard server with IPv4 only on Debian 11. This guide will be using nftables, since that is the default firewall on Debian.

Prepare the Environment

- Make sure the system is up to date:

```
sudo apt update && sudo apt upgrade
```

Install WireGuard

- Install WireGuard:

```
sudo apt install wireguard
```

Setup Key Pair

- Create the private key and restrict permission to it:

```
wg genkey | sudo tee /etc/wireguard/private.key
sudo chmod go= /etc/wireguard/private.key
```

- Create a public key:

```
sudo cat /etc/wireguard/private.key | wg pubkey | sudo tee /etc/wireguard/public.key
```

Create Configuration

- Create a new config:

```
sudo nano /etc/wireguard/wg0.conf
```

  - And add the following

```
[Interface]
PrivateKey = base64_encoded_private_key_goes_here
Address = 172.16.0.1/24
ListenPort = 51820
SaveConfig = true
```

Enable IPv4 Forwarding

- Enable forwading:

```
sudo nano /etc/sysctl.d/99-sysctl.conf
```

  - And uncomment the following line:

```
net.ipv4.ip_forward=1
```

- Reload the sysctl values:

```
sudo sysctl -p
```

Configure Firewall

- Find the public network interface:

```
ip route list default
```

  NOTE: The public interface is the string found within this command's output that follows the word "dev", in this case enp0s3

- Edit the nftables config:

```
sudo nano /etc/nftables.conf
```

  - And add/edit the following:

```
#!/usr/sbin/nft -f

flush ruleset

# `inet` applies to both IPv4 and IPv6.
table inet filter {
    chain input {
        type filter hook input priority 0;

        # accept any localhost traffic
        iif lo accept

        # accept traffic originated from us
        ct state established,related accept

        # ssh
        tcp dport 22 accept

    # wireguard
    udp dport 51820 accept

    # (Optional) Allow VPN clients to communicate with each other
    # iifname wg0 oifname wg0 ct state new accept

        # count and drop any other traffic
        counter drop
    }

    chain output {
        type filter hook output priority 0;
```

```
        policy accept;
    }

    chain forward {
        type filter hook forward priority 0;

    # Drop invalid packets.
    ct state invalid drop

    # Forward all established and related traffic.
    ct state established,related accept

    # Forward wireguard traffic from enp0s3
    iifname wg0 oifname enp0s3 ct state new accept

    # (Optional) Forward wireguard traffic from wg0
    #iifname wg0 oifname wg0 ct state new accept

        policy drop;
    }
}

table ip router {
    chain prerouting {
        type nat hook prerouting priority 0;
    }

    chain postrouting {
        type nat hook postrouting priority 100;

        # masquerade wireguard traffic as server IP address
        oifname enp0s3 ip saddr 172.16.0.0/24 masquerade
    }
}
```

- Start and enable wireguard, as well as restart nftables:

```
sudo systemctl restart nftables
sudo systemctl enable wg-quick@wg0
sudo systemctl start wg-quick@wg0
```

Resources

- https://www.digitalocean.com/community/tutorials/how-to-set-up-wireguard-on-debian-11
- https://jwcxz.com/notes/200702-simple-wireguard-vpn/
- https://xdeb.org/post/2019/setting-up-a-server-firewall-with-nftables-that-support-wireguard-vpn/
- https://www.howtoforge.com/how-to-install-wireguard-vpn-on-debian-11/

History

#1 - 04/10/2023 11:38 PM - Daniel Curtis

- % Done changed from 0 to 100

- Status changed from New to Resolved

- Description updated

#2 - 04/11/2023 12:05 AM - Daniel Curtis

- Description updated

#3 - 04/14/2023 10:41 AM - Daniel Curtis

- Description updated

#4 - 04/14/2023 10:42 AM - Daniel Curtis

- Description updated

#5 - 04/14/2023 03:02 PM - Daniel Curtis

- Description updated