WireGuard VPN Server Setup Skript

Installiert einen WireGuard VPN Server - CentOS 7 und Debian 9

Skript Sourcecode

Filename: install_wireguard_server.sh

```
#!/bin/bash
################################################################################
################
#****************** WireGuard VPN Server Setup by Michael Reber - v 1.0
********************#
################################################################################
################

################################################################################
################
WG_CONFIG="/etc/wireguard/wg0.conf"

function get_free_udp_port
{
    local port=$(shuf -i 2000-65000 -n 1)
    ss -lau | grep $port > /dev/null
    if [[ $? == 1 ]] ; then
        echo "$port"
    else
        get_free_udp_port
    fi
}

if [[ "$EUID" -ne 0 ]]; then
    echo "Sorry, you need to run this as root"
    exit
fi

if [[ ! -e /dev/net/tun ]]; then
    echo "The TUN device is not available. You need to enable TUN before
running this script"
    exit
fi


if [ -e /etc/centos-release ]; then
    DISTRO="CentOS"
elif [ -e /etc/debian_version ]; then
```

```
    DISTRO=$( lsb_release -is )
else
    echo "Your distribution is not supported (yet)"
    exit
fi

if [ "$( systemd-detect-virt )" == "openvz" ]; then
    echo "OpenVZ virtualization is not supported"
    exit
fi

if [ ! -f "$WG_CONFIG" ]; then
    ### Install server and add default client
    INTERACTIVE=${INTERACTIVE:-yes}
    PRIVATE_SUBNET=${PRIVATE_SUBNET:-"10.9.0.0/24"}
    PRIVATE_SUBNET_MASK=$( echo $PRIVATE_SUBNET | cut -d "/" -f 2 )
    GATEWAY_ADDRESS="${PRIVATE_SUBNET::-4}1"

    if [ "$SERVER_HOST" == "" ]; then
        SERVER_HOST=$(ip addr | grep 'inet' | grep -v inet6 | grep -vE
'127\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | grep -oE
'[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | head -1)
        if [ "$INTERACTIVE" == "yes" ]; then
            read -p "Servers public IP address is $SERVER_HOST. Is that
correct? [y/n]: " -e -i "y" CONFIRM
            if [ "$CONFIRM" == "n" ]; then
                echo "Aborted. Use environment variable SERVER_HOST to set
the correct public IP address"
                exit
            fi
        fi
    fi

    if [ "$SERVER_PORT" == "" ]; then
        SERVER_PORT=$( get_free_udp_port )
    fi

    if [ "$CLIENT_DNS" == "" ]; then
        echo "Which DNS do you want to use with the VPN?"
        echo "   1) Cloudflare"
        echo "   2) Google"
        echo "   3) OpenDNS"
        read -p "DNS [1-3]: " -e -i 1 DNS_CHOICE

        case $DNS_CHOICE in
            1)
            CLIENT_DNS="1.1.1.1,1.0.0.1"
            ;;
            2)
```

```
            CLIENT_DNS="8.8.8.8,8.8.4.4"
            ;;
            3)
            CLIENT_DNS="208.67.222.222,208.67.220.220"
            ;;
        esac
    fi

    if [ "$DISTRO" == "Ubuntu" ]; then
    apt-get install software-properties-common -y
    add-apt-repository ppa:wireguard/wireguard -y
    apt update
    apt install wireguard qrencode iptables-persistent -y
    elif [ "$DISTRO" == "Debian" ]; then
        echo "deb http://deb.debian.org/debian/ unstable main" >
/etc/apt/sources.list.d/unstable.list
        printf 'Package: *\nPin: release a=unstable\nPin-Priority: 90\n' >
/etc/apt/preferences.d/limit-unstable
        apt-get install software-properties-common -y
        apt update
        apt install wireguard qrencode iptables-persistent -y
    elif [ "$DISTRO" == "CentOS" ]; then
        curl -Lo /etc/yum.repos.d/wireguard.repo
https://copr.fedorainfracloud.org/coprs/jdoss/wireguard/repo/epel-7/jdoss-wi
reguard-epel-7.repo
        yum install epel-release -y
        yum install wireguard-dkms qrencode wireguard-tools firewalld -y
    fi

    SERVER_PRIVKEY=$( wg genkey )
    SERVER_PUBKEY=$( echo $SERVER_PRIVKEY | wg pubkey )
    CLIENT_PRIVKEY=$( wg genkey )
    CLIENT_PUBKEY=$( echo $CLIENT_PRIVKEY | wg pubkey )
    CLIENT_ADDRESS="${PRIVATE_SUBNET::-4}3"

    mkdir -p /etc/wireguard
    touch $WG_CONFIG && chmod 600 $WG_CONFIG

    echo "# $PRIVATE_SUBNET $SERVER_HOST:$SERVER_PORT $SERVER_PUBKEY
$CLIENT_DNS
[Interface]
Address = $GATEWAY_ADDRESS/$PRIVATE_SUBNET_MASK
ListenPort = $SERVER_PORT
PrivateKey = $SERVER_PRIVKEY
SaveConfig = false" > $WG_CONFIG

    echo "# client
[Peer]
PublicKey = $CLIENT_PUBKEY
AllowedIPs = $CLIENT_ADDRESS/32" >> $WG_CONFIG
```

```
    echo "[Interface]
PrivateKey = $CLIENT_PRIVKEY
Address = $CLIENT_ADDRESS/$PRIVATE_SUBNET_MASK
DNS = $CLIENT_DNS
[Peer]
PublicKey = $SERVER_PUBKEY
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = $SERVER_HOST:$SERVER_PORT
PersistentKeepalive = 25" > $HOME/client-wg0.conf
qrencode -t ansiutf8 -l L < $HOME/client-wg0.conf

    echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
    echo "net.ipv4.conf.all.forwarding=1" >> /etc/sysctl.conf
    echo "net.ipv6.conf.all.forwarding=1" >> /etc/sysctl.conf
    sysctl -p

    if [ "$DISTRO" == "CentOS" ]; then
        systemctl start firewalld
        firewall-cmd --zone=public --add-port=$SERVER_PORT/udp
        firewall-cmd --zone=trusted --add-source=$PRIVATE_SUBNET
        firewall-cmd --permanent --zone=public --add-port=$SERVER_PORT/udp
        firewall-cmd --permanent --zone=trusted --add-source=$PRIVATE_SUBNET
        firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -s
$PRIVATE_SUBNET ! -d $PRIVATE_SUBNET -j SNAT --to $SERVER_HOST
        firewall-cmd --permanent --direct --add-rule ipv4 nat POSTROUTING 0
-s $PRIVATE_SUBNET ! -d $PRIVATE_SUBNET -j SNAT --to $SERVER_HOST
    else
        iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j
ACCEPT
        iptables -A FORWARD -m conntrack --ctstate NEW -s $PRIVATE_SUBNET -m
policy --pol none --dir in -j ACCEPT
        iptables -t nat -A POSTROUTING -s $PRIVATE_SUBNET -m policy --pol
none --dir out -j MASQUERADE
        iptables -A INPUT -p udp --dport $SERVER_PORT -j ACCEPT
        iptables-save > /etc/iptables/rules.v4
    fi

    systemctl enable wg-quick@wg0.service
    systemctl start wg-quick@wg0.service

    # TODO: unattended updates, apt install dnsmasq ntp
    echo "Client config --> $HOME/client-wg0.conf"
    echo "Now reboot the server and enjoy your fresh VPN installation! :^)"
else
    ### Server is installed, add a new client
    CLIENT_NAME="$1"
    if [ "$CLIENT_NAME" == "" ]; then
        echo "Tell me a name for the client config file. Use one word only,
no special characters."
```

```
        read -p "Client name: " -e CLIENT_NAME
    fi
    CLIENT_PRIVKEY=$( wg genkey )
    CLIENT_PUBKEY=$( echo $CLIENT_PRIVKEY | wg pubkey )
    PRIVATE_SUBNET=$( head -n1 $WG_CONFIG | awk '{print $2}')
    PRIVATE_SUBNET_MASK=$( echo $PRIVATE_SUBNET | cut -d "/" -f 2 )
    SERVER_ENDPOINT=$( head -n1 $WG_CONFIG | awk '{print $3}')
    SERVER_PUBKEY=$( head -n1 $WG_CONFIG | awk '{print $4}')
    CLIENT_DNS=$( head -n1 $WG_CONFIG | awk '{print $5}')
    LASTIP=$( grep "/32" $WG_CONFIG | tail -n1 | awk '{print $3}' | cut -d
"/" -f 1 | cut -d "." -f 4 )
    CLIENT_ADDRESS="${PRIVATE_SUBNET::-4}$((LASTIP+1))"
    echo "# $CLIENT_NAME
[Peer]
PublicKey = $CLIENT_PUBKEY
AllowedIPs = $CLIENT_ADDRESS/32" >> $WG_CONFIG

    echo "[Interface]
PrivateKey = $CLIENT_PRIVKEY
Address = $CLIENT_ADDRESS/$PRIVATE_SUBNET_MASK
DNS = $CLIENT_DNS
[Peer]
PublicKey = $SERVER_PUBKEY
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = $SERVER_ENDPOINT
PersistentKeepalive = 25" > $HOME/$CLIENT_NAME-wg0.conf
qrencode -t ansiutf8 -l L < $HOME/$CLIENT_NAME-wg0.conf

    ip address | grep -q wg0 && wg set wg0 peer "$CLIENT_PUBKEY" allowed-ips
"$CLIENT_ADDRESS/32"
    echo "Client added, new configuration file --> $HOME/$CLIENT_NAME-
wg0.conf"
fi
```

Last update: **2019/05/07 12:13**