KB 51375: OVPNIP4

IP-Tunnel mit OpenVPN einrichten auf Linux

Stand	24.02.2022, 12:51:26
Version	6217713e
Referenz-URL	https://www.internet-xs.de/kb/51375
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-51375-6217713e.pdf

Inhalt

Voraussetzungen 4
root-Rechte erhalten 4
System-Updates installieren 4
OpenVPN installieren 4
Konfigurationsdatei herunterladen und platzieren 5
Datei mit Zugangsdaten erstellen 5
Variante 1: nano 5
Variante 2: echo 5
..... 6
Dienst starten 6
..... 6
Dienst bei Systemstart automatisch starten 6
Avahi-Daemon und rpcd deaktivieren 6
Weitere Einstellungen, falls das Linux-Betriebssystem als Router / Gateway fungieren soll 7
Fehlerdiagnose 7

Wir betreiben verschiedene Einwahl-Server zur Bereitstellung von IP-Tunnel-Verbindungen / festen, öffentlichen IPv4-Adressen. Die Anleitungen in dieser Kategorie sind speziell abgestimmt auf diesen Server:

- Name: OVPNIP4
- Hostname: ovpnip4.internet-xs.de
- IP-Adresse: 212.58.69.4
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.82.0/24 (212.58.82.1 - 212.58.82.254)
- Benutzername / Zugangskennung Format: ixs004-....-.....

Bitte prüfen Sie, ob Ihr IP-Tunnel-Zugang auch auf dem o.g. Server registriert ist.

Alle Arbeiten geschehen auf eigene Gefahr. Für Schäden an Soft- und Hardware sowie für Ausfälle Ihrer Infrastruktur sind Sie selbst verantwortlich. Wir können keine Unterstützung für nicht von uns getestete Szenarien, Hardware, Software und Betriebssysteme anbieten. Alle Anleitungen setzen ein Blanko- bzw. minimal konfiguriertes System voraus und sind als eine mögliche Konfigurationsvariante zu verstehen, die ggf. an Ihr lokales Umfeld und Ihre Anforderungen angepasst werden muss. Bitte beachten Sie immer die Sicherheitshinweise in der Bedienungsanleitung des Herstellers, besonders zum Betrieb von Hardware, dem Aufstellungsort und Betriebstemperaturen. Führen Sie Tests nicht in Produktivumgebungen durch. Testen Sie die Lösung ausgiebig, bevor Sie sie produktiv einsetzen. IT-Systeme sollten nur von qualifiziertem Personal konfiguriert werden. Als Administrator müssen Sie selbst abwägen, ob unsere Produkte und Dienstleistungen für Ihren Anwendungszweck und die gewünschte Verfügbarkeit geeignet sind, oder nicht. Führen Sie Änderungen nicht über eine entfernte Verbindung (Remote-Verbindung) durch. **Verwenden Sie stets sichere Passwörter, ändern Sie Standard-Passwörter umgehend ab.**

In einer PDF-Datei können Zeilenumbrüche innerhalb von Code-Blöcken vorhanden sein, da die Seitenbreite begrenzt ist. Bitte verwenden Sie für Copy & Paste im Zweifelsfall ein Editor-Programm als Zwischenritt und entfernen Sie unerwünschte Zeilenumbrüche.

Voraussetzungen

- IP-Tunnel-Zugang (Test-Zugang oder bezahlter Zugang)
- root-Zugang
- Kernel-Modul “tun” geladen oder ladbar (häufig nicht möglich innerhalb containerbasierter Virtualisierung wie OpenVZ, Virtouzzo, LXC, Docker)
- Debian / Raspbian / Raspberry Pi OS 10+ (“Buster”), RHEL / CentOS 7+ (die Anleitung ist möglicherweise auch auf andere Betriebssystemversionen und Distributionen mit systemd 1:1 übertragbar)
- Die Anleitung nimmt keine Rücksicht auf bereits installierte Anwendungen. Es wird von einem frisch installierten, sich nicht im Produktivbetrieb befindlichen System ausgegangen.

root-Rechte erhalten

Alle weiteren Befehle benötigen root-Berechtigungen. Mittels dieses Befehls erhalten während Ihrer aktuellen Shell-Sitzung root-Berechtigungen:

```
sudo -s
```

System-Updates installieren

Debian / Ubuntu:

```
apt update && apt upgrade -y
```

RHEL / CentOS / Fedora:

```
yum update -y
```

Nach der Installation der Updates sollte das System neu gestartet werden:

```
reboot
```

OpenVPN installieren

Debian / Ubuntu:

```
apt install -y curl nano openvpn
```

RHEL / CentOS / Fedora:

```
yum install -y curl nano openvpn
```

Konfigurationsdatei herunterladen und platzieren

Ermitteln Sie zunächst die OpenVPN-Version mit diesem Befehl:

```
openvpn --version
```

OpenVPN **ab Version 2.5**:

```
curl -o /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.conf --fail
"https://www.internet-xs.de/kb/file/download/00000/udp0.ovpnip4.internet-xs.d
e.ovpn"
```

OpenVPN **bis einschließlich Version 2.4**:

```
curl -o /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.conf --fail
"https://www.internet-xs.de/kb/file/download/00000/openvpn-2.4.udp0.ovpnip4.i
nternet-xs.de.ovpn"
```

Datei mit Zugangsdaten erstellen

Damit die OpenVPN-Client-Verbindung automatisch gestartet werden kann, müssen die Zugangsdaten in einer Konfigurationsdatei hinterlegt werden.

Variante 1: nano

1. `nano /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user`
2. Erste Zeile: *Ihr IP-Tunnel-Zugang Benutzername / Zugangskennung (z.B. ixs004-1234-a1b2c3d4)*
3. Zweite Zeile: *Ihr IP-Tunnel-Zugang Passwort / Zugangspasswort*
4. `Strg+O` (“Write Out”, speichern)
5. `Strg+X` (“Exit”, schließen)

Variante 2: echo

Vorlage:

```
echo -e "[ip-tunnel-benutzername]\n[ip-tunnel-passwort]" >
/etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user
```

1. Kopieren Sie die Vorlage in die Befehlszeile
2. Ersetzen Sie `[ip-tunnel-benutzername]` **inklusive den eckigen Klammern** durch den Benutzernamen / Zugangskennung des IP-Tunnels, `[ip-tunnel-passwort]` **inklusive den eckigen Klammern** durch das Passwort des IP-Tunnel-Zugangs. Achten Sie darauf, dass Benutzername / Zugangskennung und Passwort durch ein `\n` getrennt sind (`\n` wird bei Ausführung des Befehls in eine neue Zeile umgewandelt)
3. Die Befehlszeile sollte danach beispielsweise so aussehen: `echo -e "ixs004-1234-a1b2c3d4\nXXXXXXXXXXXXXXXXXXX" > /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user`
4. Dürcken Sie die Enter-Taste zum Ausführen des Befehls.

Bitte stellen Sie sicher, dass die Datei `/etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user` nur aus genau zwei Zeilen besteht (`cat /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user`). Setzen Sie für “Benutzername” den individuellen Benutzernamen Ihres IP-Tunnel-Zugangs und für “Passwort” das Passwort zu Ihrem IP-Tunnel-Zugang ein.

OpenVPN Konfigurationsdatei ergänzen

Damit die Datei mit den Zugangsdaten beim starten der OpenVPN-Client-Verbindung auch berücksichtigt wird, muss der Konfigurationsdatei eine entsprechende Direktive angefügt werden:

```
echo "auth-user-pass /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.user" >> /etc/openvpn/client/udp0.ovpnip4.internet-xs.de.conf
```

Dienst starten

```
systemctl start openvpn-client@udp0.ovpnip4.internet-xs.de
```

Ausführung prüfen

```
curl http://checkip.amazonaws.com/
```

Hier sollte die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse ausgegeben werden, bspw. **212.58.82.265**.

Dienst bei Systemstart automatisch starten

```
systemctl enable openvpn-client@udp0.ovpnip4.internet-xs.de
```

Avahi-Daemon und rpcd deaktivieren

Der Avahi-Daemon stellt u.a. mDNS bereit, mittels rpcd können dynamisch Ports freigegen werden und sind auf vielen Distributionen leider standardmäßig an alle IP-Adressen des Systems gebunden. Diese Funktionen sollten auf einem Gerät / Server, das über eine feste, öffentliche IPv4-Adresse verfügt, jedoch nicht öffentlich zugänglich sein.

Hinweis: Möglicherweise verfügt Ihre Distribution nicht über einen der unten genannten Dienste. In dem Fall schlägt der Befehl fehl, was aber keine Rolle spielt.

```
systemctl stop avahi-daemon
systemctl disable avahi-daemon

systemctl stop rpcbind
systemctl disable rpcbind

systemctl stop portmap
systemctl disable portmap

systemctl stop cups
systemctl disable cups
```

Weitere Einstellungen, falls das Linux-Betriebssystem als Router / Gateway fungieren soll

Falls Sie das Linux-Betriebssystem als Router bzw. als Gateway für andere Netzwerkgeräte verwenden möchten, muss das IP-Forwarding aktiviert werden.

```
sysctl -w net.ipv4.ip_forward=1
```

Außerdem wird die Maskierung der Absender-IP-Adresse benötigt, da ausgehende Pakete sonst mit der LAN-IP-Adresse des absendenden Geräts (bspw. einer Webcam , Datenlogger o.Ä.) ins Internet gelangen und dort sofort verworfen werden:

```
iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE
```

`tun0` entspricht dem Interface-Namen des OpenVPN Interfaces. Sie können den Namen mittels `ip all show` ermitteln. Die Zeile, in der sich die Ihrem IP-Tunnel zugeteilte feste, öffentliche IPv4-Adresse befindet, ist der Interface-Name des Tunnel-Interfaces.

Fehlerdiagnose

Falls keine Verbindung zustande kommt, prüfen Sie das Syslog:

```
journalctl -n 20 -u openvpn-client@udp0.ovpnip4.internet-xs.de
```

In der letzten Zeile sollte **Initialization Sequence Completed** stehen. Falls dies nicht der Fall ist, können Sie uns das Syslog unter Angabe Ihrer Zugangskennung für eine Analyse zusenden.

Impressum

Verantwortlich für die Inhalte in diesem Dokument:

Internet XS Service GmbH
Internetagentur
Heßbrühlstr. 15
70565 Stuttgart

Telefon: 07 11/78 19 41 - 0
Telefax: 07 11/78 19 41 -79
E-Mail: info@internet-xs.de
Internet: www.internet-xs.de

Geschäftsführer: Helmut Drodofsky
Registergericht: Amtsgericht Stuttgart
Registernummer: HRB 21091
UST.IdNr.: DE 190582774

Alle Preise, sofern nicht ausdrücklich anders gekennzeichnet, inkl. gesetzlich geldender deutscher MwSt.

Angebote, sofern nicht ausdrücklich anders gekennzeichnet, gültig bis 4 Wochen nach Zusendung / Abruf.

