KB 56852: OVPNIP8

IP-Tunnel mit OpenVPN einrichten auf Linux

Stand	24.09.2024, 16:52:44
Version	66f2d23c
Referenz-URL	https://www.internet-xs.de/kb/56852
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-56852-66f2d23c.pdf

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: OVPNIP8
- Hostname: ovpnip8.internet-xs.de
- IP-Adresse: 212.58.69.24
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.88.0/24 (212.58.88.1 - 212.58.88.254)
- Benutzername / Zugangskennung Format: ixs024-....-.....

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
```

root-Rechte erhalten

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

```
sudo -s
```

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/ovpnip8.internet-xs.de.conf --fail
"https://www.internet-xs.de/kb/file/download/00000/openvpn-2.5.udp0.ovpnip8.i
nternet-xs.de.ovpn"
```

OpenVPN **bis einschließlich Version 2.4**:

```
curl -o /etc/openvpn/client/ovpnip8.internet-xs.de.conf --fail
"https://www.internet-xs.de/kb/file/download/00000/openvpn-2.4.udp0.ovpnip8.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/ovpnip8.internet-xs.de.user`
2. Erste Zeile: *Ihr IP-Tunnel-Zugang Benutzername / Zugangskennung (z.B. ixs024-1234-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/ovpnip8.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 "ixs024-1234-a1b2c3d4\nXXXXXXXXXXXXXXXXXXXX" > /etc/openvpn/client/ovpnip8.internet-xs.de.user`
4. Dürcken Sie die Enter-Taste zum Ausführen des Befehls.

Bitte stellen Sie sicher, dass die Datei `/etc/openvpn/client/ovpnip8.internet-xs.de.user` nur aus genau zwei Zeilen besteht (`cat /etc/openvpn/client/ovpnip8.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/ovpnip8.internet-xs.de.user" >>
/etc/openvpn/client/ovpnip8.internet-xs.de.conf
```

Dienst starten

```
systemctl start openvpn-client@ovpnip8.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. **212.58.88.265**.

Externe Konnektivität prüfen

Um festzustellen, ob von extern, d.h. aus dem Internet, Kommunikation stattfinden kann empfiehlt es sich, z.B. mithilfe eines Smartphones aus dem LTE-Netz einen Ping an die feste IP-Adresse abzusetzen. Auf Android eignet sich dafür z.B. die App "PingTools". Es kann aber auch einfach ein Computer verwendet werden, der sich nicht im internen Netzwerk befindet.

`ping 212.58.88.265`

Setzen Sie für `212.58.88.265` die Ihrem IP-Tunnel-Zugang zugewiesene feste, öffentliche IPv4-Adresse ein. Als Ergebnis sollten Sie eine Ausgabe ähnlich dieser erhalten:

```
C:\Users\user>ping 212.58.88.265

Ping wird ausgeführt für 212.58.88.265 mit 32 Bytes Daten:
Antwort von 212.58.88.265: Bytes=32 Zeit=12ms TTL=62
Antwort von 212.58.88.265: Bytes=32 Zeit=12ms TTL=62
Antwort von 212.58.88.265: Bytes=32 Zeit=12ms TTL=62
Antwort von 212.58.88.265: Bytes=32 Zeit=13ms TTL=62

Ping-Statistik für 212.58.88.265:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 12ms, Maximum = 13ms, Mittelwert = 12ms
```

Fehlerdiagnose

Falls keine Verbindung zustande kommt, prüfen Sie das Syslog:

```
journalctl -n 20 -u openvpn-client@ovpnip8.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.

Dienst bei Systemstart automatisch starten

```
systemctl enable openvpn-client@ovpnip8.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.

Port-Weiterleitungen / NAT oder Reverse Proxy

Falls eine eigene virtuelle Maschine oder einen eigenen Server (z.B. Raspberry Pi) als Endpunkt für die IP-Tunnel-Verbindung eingerichtet wurde, sollen die Daten, die an die feste IP-Adresse des IP-Tunnel-Zugangs gesendet werden, häufig an andere virtuellen Maschinen / Servern / Geräten weitergeleitet werden.

Dafür gibt es zwei Optionen:

1. Port-Weiterleitungen / NAT

Wenn Sie beliebige Netzwerk-Dienste in Ihrem LAN mittels z.B. TCP / UDP-Anfragen aus dem Internet erreichbar machen möchten, bieten sich Port-Weiterleitungen / NAT als Lösungsoption an. Hierbei spielt es keine Rolle, was genau Sie anbinden möchten (eine Web-Oberfläche, RDP / Remote-Desktop, VNC, RTSP…). Jeder netzwerkfähige Dienst kann damit transparent erreichbar gemacht werden.

Dieses Vorgehen entspricht dem eintragen von Port-Weiterleitungen in einem Internet-Router.

Beispiel für Port-Weiterleitungen / NAT mit `iptables`:

```
iptables -t nat -I PREROUTING -p tcp --dport 80 -j DNAT --to
192.168.178.123:5000
```

Ersetzen Sie im Muster folgende Eigenschaften:

1. `-p tcp`: Setzen Sie hier `tcp` oder `udp` ein, je nachdem, welche Art von Netzwerk-Dienst Sie erreichbar machen möchten.
2. `--dport 80`: 80 ist der häufig als “Externer Port” bezeichnete Port, also der Port, den Sie für die Kommunikation später an Ihre feste, öffentliche IPv4-Adresse anfügen müssen (bspw. http://212.58.88.265:80). Dieser kann oft vom “Ziel Port” abweichend sein.

3. `--to 192.168.178.123:5000`: Setzen Sie hier die LAN-IP-Adresse des Servers / Geräts ein, zu dem die Daten geleitet werden sollen.

Sie müssen anschließend auf dem LAN-Gerät / Server mit der Beispiel-IP-Adresse `192.168.178.123` als **Standard-Gateway** (**Default Gateway**) die LAN-IP-Adresse des Linux-Systems eintragen, auf dem Sie den OpenVPN-Client zum Bezug der festen, öffentlichen IPv4-Adresse eingerichtet haben.

Bitte beachten Sie, dass die mittels `iptables` eingestellte Port-Weiterleitung mit einem Neustart des Systems verschwinden. Wie Sie iptables-Regeln dauerhaft speichern und sie beim Systemstart laden, ist von Distribution zu Distribution unterschiedlich (z.B. in /etc/sysconfig/iptables für RHEL-basierte Distributionen). Bitte konsultieren Sie die Dokumentation Ihrer Distribution für weitere Informationen.

2. Reverse Proxy

Falls Sie nur Web-Oberflächen wie bspw. ERP-Systeme, Samrt-Home-Steuerungen, Webmail, Cloud-Speichersystem wie Next Cloud etc. mittels der festen, öffentlichen IPv4-Adresse erreichbar machen möchten, kann das Problem mithilfe eines sog. **Reverse Proxys** gelöst werden, der im ersten Schritt die Daten-Verbindung annimmt, dann basierend auf dem angefragten Host-Namen (z.B. cloud.ihre-domain.tld, webmail.ihre-domain.tld, erp.ihre-domain.tld) die Verbindung in das LAN weiter vermittelt und die Antwort des angefragten Systems an den anfragenden Nutzer zurück vermittelt.

Um diese Lösungsmöglichkeit sinnvoll zu nutzen, sollten Sie über eine eigene Domain verfügen.

Installieren Sie dafür auf der virtuellen Maschine / dem Server, auf dem Sie auch den OpenVPN-Client für die IP-Tunnel-Verbindung eingerichtet haben einen **Web-Server** wie z.B. **Apache** und konfigurieren Sie diesen als Reverse-Proxy in Richtung der anzubindenden Web-Oberfläche.

Beispiel (bitte beachten Sie, dass die genaue Konfiguration von Distribution zu Distribution unterschiedlich sein kann und dass möglicherweise die Installation weiterer Webserver-Module wie bspw. `mod_proxy` für Apache erforderlich sein kann. Es gibt im Internet zahlreiche Schritt-für-Schritt-Anleitungen für nahezu alle Distributionen):

```
# Reverse-Proxy für cloud.ihre-domain.tld
<VirtualHost *:80>
    ServerAdmin ihre-email-adresse@ihre-domain.tld
    ProxyRequests off
    DocumentRoot /var/www
    SSLProxyEngine on
    ProxyPreserveHost on

    # Vergeben einen Server-Namen. Sie muessen diesen Server-Namen
    # in der DNS-Verwaltung Ihres Domain-Anbieters einrichten
    ServerName cloud.ihre-domain.tld

    # Eigene Log-Dateien pro angebundener Web-Oberflaeche
    ErrorLog /var/log/apache2/cloud-error.log
    CustomLog /var/log/apache2/cloud-access.log combined

    LogLevel error

    <Location />
        # Setzen Sie hier die HTTP-Adresse ein, mit der Sie die
        # anzubindende Web-Oberflaeche aus dem lokalen Netzwerk
        # erreichen koennen:
        ProxyPass http://192.168.178.123:5000/
```

```
        # Setzen Sie hier dieselbe HTTP-Adresse nochmal ein:
        ProxyPassReverse http://192.168.178.123:5000/

        Order allow,deny
        Allow from all
    </Location>

</VirtualHost>

# Ein weiterer Reverse-Proxy fuer webmail.ihre-domain.tld
<VirtualHost *:80>
    ServerAdmin ihre-email-adresse@ihre-domain.tld
    ProxyRequests off
    DocumentRoot /var/www
    SSLProxyEngine on
    ProxyPreserveHost on

    # Vergeben einen Server-Namen. Sie muessen diesen Server-Namen
    # in der DNS-Verwaltung Ihres Domain-Anbieters einrichten
    ServerName webmail.ihre-domain.tld

    # Eigene Log-Dateien pro angebundener Web-Oberflaeche
    ErrorLog /var/log/apache2/webmail-error.log
    CustomLog /var/log/apache2/webmail-access.log combined

    LogLevel error

    <Location />
        # Setzen Sie hier die HTTP-Adresse ein, mit der Sie die
        # anzubindende Web-Oberflaeche aus dem lokalen Netzwerk
        # erreichen koennen:
        ProxyPass http://192.168.178.124:80/

        # Setzen Sie hier dieselbe HTTP-Adresse nochmal ein:
        ProxyPassReverse http://192.168.178.124:80/

        Order allow,deny
        Allow from all
    </Location>

</VirtualHost>
```

In die Direktiven `ProxyPass` bzw. `ProxyPassReverse` tragen Sie die HTTP-Adresse (i.d.R. eine LAN-IP-Adresse) inklusive Port ein, über die Sie die anzubindende Web-Oberfläche (= ERP-System, Smart-Home-Steuerung, Webmail, Cloud-Speichersystem wie Next Cloud oder Synology DSM…) aus dem **lokalen Netzwerk** erreichen.

Tragen Sie anschließend in der DNS-Verwaltung Ihres Domain-Anbieters eine neue Subdomain ein:

cloud.ihre-domain.tld: A-Record auf 212.58.88.265 (= die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse) webmail.ihre-domain.tld: A-Record auf 212.58.88.265 (= die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse) erp.ihre-domain.tld: A-Record auf 212.58.88.265 (= die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse)

usw.

Der Zugriff aus dem Internet erfolgt dann mittels den entsprechenden Subdomains:

http://cloud.ihre-domain.tld
http://webmail.ihre-domain.tld
http://erp.ihre-domain.tld

Der angebundenen Web-Oberfläche (= ERP-System, Smart-Home-Steuerung, Webmail, Cloud-Speichersystem wie Next Cloud oder Synology DSM…) muss häufig mitgeteilt werden, dass sie sich hinter einem Reverse Proxy befindet. Wie das genau funktioniert entnehmen Sie der Dokumentation der angebundenen Web-Oberfläche.

Sie können mit diesem Schema eine beliebige Zahl Web-Oberflächen mit einer einzelnen festen, öffentlichen IPv4-Adresse aus dem Internet erreichbar machen.

Ein Reverse Proxy kann auch die Terminierung von verschlüsselten Verbindungen mit z.B. Let's Encrypt / `certbot` zentral übernehmen. Bitte konsultieren Sie die Dokumentation Ihres Web-Servers für weitere Informationen zur Konfiguration von SSL-Verbindungen.

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.