KB 33493: OVPNIP5

IP-Tunnel mit OpenVPN einrichten auf OPNSense

Stand	24.02.2022, 12:51:26
Version	6217713e
Referenz-URL	https://www.internet-xs.de/kb/33493
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-33493-6217713e.pdf

Einleitung

Mithilfe dieser Anleitung kann ein IP-Tunnel-Zugang von unseren Einwahlserver OVPNIP5 (ovpnip5.internet-xs.de / 212.58.69.9) auf einer OPNSense-Installation in Betrieb genommen werden. Sie erläutert außerdem, wie ICMP aktiviert werden kann und wie Ports mittels DNAT an andere Netzwerkgeräte (z.B. Server, IP-Kameras, Smart-Home…) weitergeleitet werden können.

Zielgruppe:
Administratoren von OPNSense, die mittels einer IP-Tunnel-Verbindung von Internet XS eine feste, öffentliche IPv4-Adresse auf einer OPNSense-Installation nutzen möchten.

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: OVPNIP5
- Hostname: ovpnip5.internet-xs.de
- IP-Adresse: 212.58.69.9
- Protokoll: OpenVPN / TUN / UDP oder TCP
- Client IP-Adress-Bereich: 212.58.84.0/24 (212.58.84.1 - 212.58.84.254)
- Benutzername / Zugangskennung Format: ixs009-....-.....

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

1. OPNSense-Grundinstallation
2. Kostenloser Test-Zugang oder ein bezahlter Zugang auf unserem IP-Tunnel-Server OVPNIP5 (ovpnip5.internet-xs.de / 212.58.69.9)

CA-Zertifikat importieren

Zunächst muss das CA-Zertifikat unseres OpenVPN-Servers in die OPNSense-Installation importiert werden. Dazu gehen Sie wie folgt vor:

Download “ovpnip5.internet-xs.de.ca.crt.txt”

1. Navigieren Sie zu **System > Trust > Authorities**
2. Klicken Sie auf **+ Add**
3. Descriptive name: ovpnip5.internet-xs.de
4. Method: Import an existing Certificate Authority
5. Certificate data: Inhalt der Datei ovpnip5.internet-xs.de.ca.crt.txt inklusive `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`
6. Certificate Private Key: *leer*
7. Serial for next certificate: *leer*
8. Klicken Sie auf **Save**

OpenVPN Client-Verbindung konfigurieren

1. Navigieren Sie zu **VPN > OpenVPN > Clients**
2. Klicken Sie auf + Add
3. Disabled: *deaktiviert*
4. Description: z.B. **ixs009-1234-a1b2c3d4** (Ihr Benutzername auf dem IP-Tunnel-Server)
5. Server Mode: Peer to Peer (SSL/TLS)
6. Protocol: *UDP*
7. Device mode: **tun**
8. Interface: *any*
9. Remote Server: Host or address: **212.58.69.9**
10. Remote Server: Port: **1194**
11. Retry DNS resolution > Infinitely resolve remote server: **aktiviert**
12. Proxy host or address: *leer*
13. Proxy port: *leer*
14. Proxy authentication extra options > Authentication method: *none*
15. Local port: *leer*
16. User name/pass > Username: Ihr Benutzername auf dem IP-Tunnel-Server (z.B. **ixs009-1234-a1b2c3d4**)
17. User name/pass > Password: Das zum IP-Tunnel-Zugang zugehörige Passwort, das Sie von uns erhalten haben
18. Renegotiate time: 0
19. TLS Authentication > Enable authentication of TLS packets.: **deaktiviert**
20. TLS Authentication > Automatically generate a shared TLS authentication key.: **deaktiviert**

21. Peer Certificate Authority: **ovpnip5.internet-xs.de** (das im Abschnitt “CA-Zertifikat importieren” importierte CA-Zertifikat)
22. Client Certificate: *None (Username and Passwort required)*
23. Encryption algorithm: **None (No Encryption)**
24. Auth Digest Algorithm: **SHA1**
25. Hardware Crypto: *No Hardware Cryption Acceleration* oder eine zur Verfügung stehende Hardwarebeschleunigung
26. IPv4 Tunnel Network: *leer*
27. IPv6 Tunnel Network: *leer*
28. IPv4 Remote Network: *leer*
29. IPv6 Remote Network: *leer*
30. Limit outgoing bandwidth: *leer*
31. Compression: *No Preference*
32. Type-of-Service: *deaktiviert*
33. Don’t pull routes: *deaktiviert*
34. Don’t add/remove routes: *deaktiviert*
35. Kopieren Sie diese Einstellungen in das Feld **Advanced**:

```
sndbuf 0
rcvbuf 0
keepalive 20 120
nobind
route-delay 5
mute 5
explicit-exit-notify
auth-retry nointeract
persist-key
persist-tun
reneg-bytes 0
setenv CLIENT_CERT 0
```

36. Verbosity level: **3 (recommended)**
37. Klicken Sie auf Save, um die Konfiguration abzuspeichern.

Ausführung prüfen

1. Navigieren Sie zu VPN > OpenVPN > Connection Status
2. In der Zeile mit dem Namen z.B. **ixs009-1234-a1b2c3d4** in der Spalte **Status** sollte nun **up** stehen.
3. Navigieren Sie zu VPN > OpenVPN > Log File
4. Die oberste Zeile sollte einen Inhalt ähnlich **openvpn[64476]: Initialization Sequence Completed** haben

Interface Assignment konfigurieren

Damit das neue OpenVPN-Client-Interface `ovpnc1` über die OPNSense-Web-Oberfläche konfiguriert werden kann, muss das Interface dem System bekannt gemacht werden.

1. Navigieren Sie zu **Interface > Assignments**
2. New Interface: Spalte Network port: *ovpnc1 (XX:XX:XX:XX:XX:XX)*
3. New Interface: Description: z.B. **ixs009-1234-a1b2c3d4** (z.B. Benutzername Ihres IP-Tunnel-Zugangs)

4. Auf das **+** klicken, um zu speichern

Maskierung

Damit Traffic, der die OPNSense über den IP-Tunnel verlässt mit der korrekten Absender-IP-Adresse versehen wird, ist die Einrichtung einer Maskierung (Masquerading) notwendig:

1. Navigieren Sie zu Firewall > NAT > Outbound
2. Mode: Hybrid outbound NAT rule generation
3. Save
    - Add
5. Interface: z.B. **ixs009-1234-a1b2c3d4** (bzw. der Name, der über das Interface-Assignment festgelegt wurde)
6. Save

ICMP erlauben

Es wird empfohlen, ICMP-Anfragen (z.B. Ping) auf dem virtuellen Netzwerk-Interface (z.B. ovpnc1) zu erlauben.

1. Navigieren Sie zu Firewall > Rules > OpenVPN
2. Klicken Sie auf + Add
3. Action: *Pass*
4. Disabled: *deaktiviert*
5. Quick: *aktiviert*
6. Interface: *OpenVPN*
7. Direction: *in*
8. TCP/IP Version: *IPv4*
9. Protocol: **ICMP**
10. ICMP type: *any*
11. Source / Invert: *deaktiviert*
12. Source > Advanced: *keine Einstellungen*
13. Destination / Invert: *deaktiviert*
14. Destination: **Single host or Network**
15. Destination > Single host or Network > Netzwerk: **Die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse (z.B. 212.58.84.XXX)**
16. Destination > Single host or Network > CIDR-Angabe: *32*
17. Destination port range > from: *any*
18. Destination port range > to: *any*
19. Log > Log packets that are handled by this rule: Nach Belieben
20. Category: Nach Belieben
21. Description: z.B. **Allow ICMP on 212.58.84.XXX**
22. Source OS: *Any*
23. No XMLRPC Sync: Nach Belieben
24. Schedule: *none*
25. Gateway: *Nothing selected*
26. Advanced Options: *keine Einstellungen*
27. Klicken Sie auf **Save**

28. Klicken Sie auf **Apply changes**

ICMP testen

Sie können nun von einem externen Gerät, z.B. von einem Smartphone, das im LTE eingebucht ist, die Ihrem IP-Tunnel-Zugang zugewiesene feste, öffentliche IPv4-Adresse pingen.

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.

