KB 45793: OVPNIP3

Einrichtung feste, öffentliche IPv4-Adresse mit DD-WRT / Linksys E1200v2

Stand	24.02.2022, 12:57:06
Version	62177292
Referenz-URL	https://www.internet-xs.de/kb/45793
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-45793-62177292.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: OVPNIP3
- Hostname: ovpnip3.internet-xs.de
- IP-Adresse: 212.58.69.3
- Protokoll: OpenVPN / TAP / UDP
- Client IP-Adress-Bereich: 212.58.77.0/24 (212.58.77.1 - 212.58.77.254)
- Benutzernamen-Format: ixs003-....-.....

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.

Vorwort

Mittels dieser Anleitung kann der Tunnel-Zugang mit fester IP-Adresse auf einem DD-WRT Betriebssystem eingerichtet werden. Die feste IPv4-Adresse liegt auf dem Gerät an und kann von dort aus mittels Port-Weiterleitungen (“DNAT”) in Ihrem LAN weiter transportiert werden.

Anforderungen

1. DD-WRT-fähiger Router (z.B. Linksys E1200v2)
2. Test-Zugang oder permanenter Zugang auf dem Einwahlserver OVPNIP3 (ovpnip3.internet-xs.de / 212.58.69.3 / Benutzernamen mit ixs003-xxxx)
3. Funktionierender, stabiler, bestehender Internet-Zugang
4. Freier Switch-Port am Internet-Router oder Switch

Die Konfiguration wurde mit einem Linksys E1200 V2 Router mit Broadcom Chipsatz getestet. Andere Geräte verhalten sich möglicherweise anders. Bitte haben Sie Verständnis dafür, dass wir nur Support für exakt dieses Modell leisten können.

Vorbereitung

Dieser Teil der Anleitung bezieht sich größtenteils auf das exakte Modell “Linksys E1200 V2” mit der FCC ID “Q89-E1200V2” / IC-Nummer “3839A-E1200V2” mit Broadcom BCM5357 Chipsatz, für andere Modelle treffen einige Schritte nicht zu **und können im schlimmsten Fall zur Beschädigung des Geräts führen!** Diese Anleitung ist eine erweiterte Übersetzung des englischen Originals: http://www.dd-wrt.com/wiki/index.php/Linksys_E1200v2

Warnung: Ändern Sie Standard-Zugangsdaten umgehend ab. Das Gerät steht im öffentlichen Internet und wird damit sehr schnell automatisch Ziel von Angriffen! Im Idealfall deaktivieren Sie den Zugriff auf das Web-Interface / Telnet oder ändern den Port ab.

1. Laden Sie die sog. “mini”-Version für das Upgrade von Standard-Firmware -> DD-WRT herunter: https://download1.dd-wrt.com/dd-wrtv2/downloads/betas/2014/12-22-2014-r25697/broadcom_K26/dd-wrt.v24-25697_NEWD-2_K2.6_mini-e1200v2.bin
2. Laden Sie die sog. “mega”-Version für das Upgrade von DD-WRT “mini” auf DD-WRT “mega” herunter: https://download1.dd-wrt.com/dd-wrtv2/downloads/betas/2014/12-22-2014-r25697/broadcom_K26/dd-wrt.v24-25697_NEWD-2_K2.6_mega-nv64k.bin
3. Trennen Sie alle Netzwerkverbindungen am Konfigurations-Client (z.B. Windows PC oder Notebook), auch WLAN.
4. Ändern Sie die IP-Konfiguration (Windows: Systemsteuerung -> Netzwerk und Internet -> Netzwerk- und Freigabecenter -> Adaptereinstellungen ändern -> Rechtsklick auf Ihre Netzwerkkarte (z.B. Ethernet oder LAN-Verbindung) -> Eigenschaften -> Internetprotokoll Version 4 -> Eigenschaften):

```
IP: 192.168.1.10
Subnetzmaske: 255.255.255.0
Standardgateway: 192.168.1.1
DNS-Server: Leer oder 8.8.8.8 für Google DNS Server
```

Installation von DD-WRT (am Beispiel des Routers E1200v2)

1. Öffnen Sie in einem Internet-Browser Ihrer Wahl die Adresse http://192.168.1.1
2. Klicken Sie auf “Mit öffentlich zugänglichem und ungesichertem Netzwerk fortfahren (nicht empfohlen)”. Aktivieren Sie das Kontrollkästchen “*Mir ist bewusst, dass mein Netzwerk momentan öffentlich zugänglich und nicht sicher ist. Ich möchte die Sicherheitseinstellungen meines Routers manuell konfigurieren.*” und klicken Sie anschließend auf “Fortfahren”.
3. Melden Sie sich mit den Standard-Zugangsdaten an: Benutzer: **admin** Passwort: **admin**
4. Als nächstes erscheint eine Warnung. Aktivieren Sie das Kontrollkästchen “Diese Meldung nicht mehr anzeigen.” und klicken Sie dann auf “OK”.
5. Navigieren Sie zum Punkt Verwaltung > Firmware-Aktualisierung.
6. **(Nur Linksys E1200v2)** Wählen Sie die Datei “dd-wrt.v24-25697_NEWD-2_K2.6_**mini**-e1200v2.bin” von Ihrem Computer aus.
7. Der Aktualisierungsvorgang dauert etwa 2-3 Minuten. Bitte trennen Sie das Gerät in dieser Zeit auf keinen Fall vom Strom. Klicken Sie nach der Wartezeit von 80 Sekunden auf “Fortfahren”.
8. Falls das Gerät nicht reagiert schalten Sie es kurz aus und wieder ein. Warten Sie 2-3 Minuten und rufen Sie das Web-Interface erneut unter http://192.168.1.1 auf.
9. Sie werden erneut zur Eingabe eines Benutzernamens und Passworts aufgefordert. Melden Sie sich mit den DD-WRT-Standardzugangsdaten an: Benutzer: **root** Passwort: **admin**
10. **Hinweis:** Sollten Sie einen “404 Not Found”-Fehler erhalten leeren Sie bitte Ihren Browsercache oder verwenden Sie ein privates Fenster oder einen anderen Browser.
11. Navigieren Sie zu “Administration” -> “Firmware Upgrade”. Wählen Sie jetzt die Datei “dd-wrt.v24-25697_NEWD-2_K2.6_**mega**-nv64k.bin” aus. Wählen Sie für “After flashing, reset to” die Einstellung “Reset to Default Settings” aus. Klicken Sie anschließend auf “Upgrade”.
12. Warten Sie **mindestens** 5 Minuten.
13. Schalten Sie das Gerät aus.
14. Schalten Sie das Gerät ein.
15. Das Web-Interface sollte nach 1-2 Minuten unter http://192.168.1.1 erreichbar sein.
16. Falls das Web-Interface nach 1-2 Minuten noch nicht erreichbar ist, drücken Sie die Reset-Taste des Routers für mindestens 30 Sekunden mit einer Büroklammer oder einem kleinen Schraubenzieher (bitte keinen Kugelschreiber verwenden). Warten Sie danach nochmal mindestens 5 Minuten und schalten Sie das Gerät dann aus und wieder ein.
17. **Ändern Sie die Standard-Zugangsdaten unter Administration > Management umgehend ab. Vergeben Sie eine eigene, sichere Benutzername-Passwort-Kombination.**

Grundkonfiguration

Dieser Abschnitt widmet sich der grundlegenden Konfiguration von DD-WRT inklusive einigen sicherheitsrelevanten Einstellungen. Alle Einstellungen sind als Empfehlungen zu verstehen - falls Sie z.B. die WLAN-Funktion benötigen können Sie diese natürlich nutzen. Die genannten IP-Adressen sind als Beispiel zu verstehen - Sie müssen die IP-Adressen an Ihr bestehendes LAN anpassen.

Setup > Basic Setup > WAN-Setup

1. Stellen Sie “Connection Type” auf “Disabled”.
2. Optional Settings: Vergeben Sie einen individuellen Router Name und einen Hostname.

Setup > Basic Setup > Network Setup

1. Local IP Adress: Unter dieser IP-Adresse ist der E1200 zukünftig im LAN erreichbar. Tragen Sie eine freie IP-Adresse aus dem Netz ein, das Ihr Internet-Router zur Verfügung stellt und die der E1200 erhalten soll, z.B. 192.168.178.254 (AVM Fritz!Box), 192.168.2.254 (Telekom Speedport), 192.168.0.254 (Netgear-Geräte), 192.168.1.254 (z.B. TP-Link). Die gewählte IP-Adresse sollte nicht im DHCP-Bereich Ihres Internet-Routers liegen.
2. Subnet Mask: In der Regel 255.255.255.0
3. Gateway: IP-Adresse Ihres Internet-Routers, z.B. 192.168.178.1 (AVM Fritz!Box), 192.168.2.1 (Telekom Speedport), 192.168.0.1 (Netgear-Geräte), 192.168.1.1 (z.B. TP-Link)
4. Local DNS: LAN-IP-Adresse eines DNS-Servers, i.d.R. dieselbe IP-Adresse wie “Gateway”
5. Klicken Sie auf “Save” (die Einstellungen werden jetzt nur zwischengespeichert).
6. DHCP Type: DHCP Server
7. DHCP Server: Disable (wichtig, sonst stört sich der DHCP-Server des DD-WRT-Routers mit dem DHCP-Server des Internet-Routers)
8. Klicken Sie auf “Save” (die Einstellungen werden jetzt nur zwischengespeichert).

Wireless > Basic Settings

1. Falls die WLAN-Funktion nicht benötigt wird sollte diese deaktiviert werden.
2. “Wireless Mode”: “Client”
3. “Wireless Network Mode”: “Disabled”
4. Klicken Sie auf “Save” (die Einstellungen werden jetzt nur zwischengespeichert).

Administration > Management

1. Info Site Passwort Protection: Enabled
2. Enable Info Site: Disable
3. Klicken Sie auf “Save” (die Einstellungen werden jetzt nur zwischengespeichert).

Administration > Keep Alive

Verwenden Sie am besten die Funktion “Schedule Reboot” mit einem “Interval”. Damit wird das Gerät auch regelmäßig neu gestartet wenn keine aktuelle Uhrzeit zur Verfügung steht.

1. Schedule Reboot: Enable
2. Interval (in seconds): Gewünschter Intervall, z.B. 43200 für alle 12 Stunden, 86400 für alle 24 Stunden
3. Klicken Sie auf “Save” (die Einstellungen werden jetzt nur zwischengespeichert).

Für eine schnellere Reaktion bei Abbrüchen oder Ausfällen sowie in ruhigen Netzwerken, in denen nur wenige Clients die IP-Verbindung verwenden, aktivieren Sie zusätzlich die Funktion “WDS/Connection Watchdog”:

1. WDS/Connection Watchdog: Enable
2. Interval (in seconds): 100
3. IP Addresses: 212.58.77.1

Speichern und neu starten

Klicken Sie nun auf “Apply Settings”. Jetzt werden die zuvor zwischengespeicherten Einstellungen angewendet und permanent gespeichert.

Das Gerät ist nun unter der IP-Adresse erreichbar, die Sie als “Local IP Address” festgelegt haben.

Verbinden Sie den E1200 mittels eines Netzwerk-Kabels am Port 1 (“Ethernet”, blau) mit einem freien Switch-Port Ihres Internet-Routers.

Schalten Sie den E1200 kurz aus und wieder ein.

IP-Konfiguration des Computers wiederherstellen

Stellen Sie die in Schritt 3 umgestellte IP-Konfiguration Ihres Computers wieder auf die zuvor verwendete (i.d.R. “IP-Adresse automatisch beziehen” oder “DHCP”) um.

Konfiguration Tunnel-Zugang mit fester IP über OpenVPN

Öffnen Sie das Web-Interface des E1200 unter der IP-Adresse, die Sie unter “Local IP Address” festgelegt haben. Navigieren Sie zu “Services > VPN”. Nehmen Sie die folgenden Einstellungen vor:

1. OpenVPN Client > Start OpenVPN Client: Enable
2. Server IP/Name: 212.58.69.3 (setzen Sie hier **NICHT** Ihre persönliche feste IP-Adresse ein!)
3. Port: 1194
4. Tunnel Device: TAP
5. Tunnel Protocol: UDP
6. Encryption Cipher: None
7. Hash Algorithm: None
8. User Pass Authentication: Enable
9. Username: Der Benutzername, den Sie von uns erhalten haben (z.B. ixs003-xxxx-yyyyyyyy)
10. Password: Das Passwort, das Sie von uns erhalten haben
11. Advanced Options: Enable
12. TLS Cipher: None
13. LZO Compression: **Disable**
14. NAT: Enable
15. (Bridge TAP to br0: Disable, falls sichtbar)
16. Firewall Protection: Enable
17. IP Address: *Leer*
18. Subnet Mask: *Leer*
19. Tunnel MTU setting: 1500
20. Tunnel UDP Fragment: *Leer*
21. Tunnel UDP MSS-Fix: Disabled
22. nsCertType verification: *Nicht aktivieren*
23. Additional Config: **Siehe unten**
24. Policy based Routing: Leer (für erfahrene Benutzer: Hier können Sie in Abhängigkeit der Quell-LAN-IP-Adresse den zugehörigen Tunnel-Zugang als Gateway setzen bzw. mehrere Zugänge mit festen IPs auf einem Gerät einrichten.)
25. PKCS12 Key: *Leer*
26. Static Key: *Leer*
27. CA Cert: **Siehe unten**
28. Public Client Cert: *Leer*
29. Private Client Key: *Leer*

Inhalt für das Feld “**Additional Config**”:

```
sndbuf 0
rcvbuf 0
keepalive 20 120
nobind
route-delay 5
verb 4
mute 5
explicit-exit-notify
auth-retry nointeract
resolv-retry infinite
persist-key
persist-tun
reneg-sec 0
reneg-bytes 0
setenv CLIENT_CERT 0
```

Inhalt für das Feld “**CA Cert**”:

Inhalt aus dieser Datei kopieren:

Download “ovpnip3.internet-xs.de.ca.crt.txt”

Inklusive `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`

```
-----BEGIN CERTIFICATE-----
MIIFVjCCAz6gAwIBAgIJAL0tW3TnzaoOMA0GCSqGSIb3DQEBCwUAMCExHzAdBgNV

<<<weitere Zeilen aus der Datei ovpnip3.internet-xs.de.ca.crt.txt>>>

s8KKM/zKbK6A+3eZ75XFbBju7iC4Bc5ycvtIr/wIlJyb300vXOmIGgjCAkm1W1Bb
7iVaAlNqbNqbmoRu6pyaodCuPa9ifAb+YFI=
-----END CERTIFICATE-----
```

Klicken Sie anschließend auf “Save” und dann auf “Apply Settings” und schalten Sie den Router aus.

Verbinden Sie nun einen LAN-Port (nicht *Internet* oder *WAN*!) des DD-WRT-Routers mithilfe eines Ethernet-Kabels mit einem freien LAN-Switch-Port Ihres Internet-Routers und schalten Sie den DD-WRT-Router ein.

Der DD-WRT-Router sollte sich nun mit unserem Einwahlserver verbinden. **Sie können die Funktion testen, indem Sie die Ihnen von uns zugeteilte feste, öffentliche IPv4-Adresse z.B. von einem Smartphone aus aufrufen. Es sollte eine Anmeldeaufforderung erscheinen. Sie können sich dann mit den zuvor eingestellten Geräte-Zugangsdaten anmelden.**

7. Port-Weiterleitungen zu IP-Kameras, Datenloggern, Servern…

1. Navigieren Sie zu Administration -> Commands
2. Dort befindet sich ein großes Textfeld. Passen Sie die unten stehende Regel nach Ihren Anforderungen an und kopieren Sie sie in das Textfeld.
3. Klicken Sie anschließend auf “**Save Firewall**”
4. Starten Sie den Router neu.

5. **(Wichtig!)** Auf dem Gerät mit der LAN-IP-Adresse CCC.CCC.CCC.CCC (= IP-Kamera, Datenlogger, Server…) müssen Sie anschließend das Standard-Gateway auf die LAN-IP-Adresse des E1200 umstellen. Wie das genau funktioniert entnehmen Sie bitte der Bedienungsanleitung Ihrer Kamera, Datenlogger… . I.d.R. ist diese Einstellung bei folgenden Menüpunkten zu finden: “TCP/IP Configuration”, “Static IP Setup”, “Disable DHCP”…
6. Sie können mittels der Regel-Vorlage beliebig viele Ports freischalten
7. Jede Regel muss in genau einer Zeile stehen, also quasi **iptables** beginnen und **DDDD** enden.
8. Wenn Sie vorhandene Regeln bearbeiten wollen, klicken Sie auf “Edit” unter dem Feld “Firewall”.

Regel-Vorlage:

```
iptables -t nat -A PREROUTING -i tap1 -p AAA --dport BBBB -j DNAT --to
CCC.CCC.CCC.CCC:DDDD
```

1. AAA: Protokoll, tcp oder udp
2. BBBB: Eingehender Port (Remote-Port, Zugriff später mit z.B. http://Ihre.feste.IP:BBBB)
3. CCC.CCC.CCC.CCC: LAN-IP-Adresse des Geräts, auf das Sie den Port weiterleiten wollen (z.B. IP-Kamera, Datenlogger, Server…)
4. DDDD: Ziel-Port auf dem LAN-Gerät, kann von BBBB verschieden sein oder auch gleich, z.B. 8080 oder 8081 oder 80, vorgegeben durch Dienst auf dem LAN-Gerät bzw. Konfiguration

Beispiele:

```
iptables -t nat -A PREROUTING -i tap1 -p tcp --dport 80 -j DNAT --to
192.168.178.50:80
```

Leitet http://Ihre-feste-IP an das Gerät mit der LAN-IP 192.168.178.50 weiter.

```
iptables -t nat -A PREROUTING -i tap1 -p tcp --dport 81 -j DNAT --to
192.168.178.51:80
```

Leitet http://Ihre-feste-IP:81 an das Gerät mit der LAN-IP 192.168.178.51:80 weiter.

```
iptables -t nat -A PREROUTING -i tap1 -j DNAT --to 192.168.178.54
```

Leitet den **gesamten Traffic** inklusive GRE (PPTP), AH, ESP (IPsec), ICMP (Ping) an 192.168.178.54 weiter (auch “Exposed Host” oder “DMZ” genannt)

8. Speziallfall: Port-Weiterleitung an das Webinterface des Internet-Routers

Nutzen Sie diese Regel zusätzlich zur in 6.) erstellten Port-Weiterleitung um das Web-Interface z.B. einer FRITZ!Box erreichbar zu machen:

```
iptables -t nat -A PREROUTING -i tap1 -p AAA --dport BBBB -j DNAT --to
CCC.CCC.CCC.CCC:DDDD iptables -t nat -A POSTROUTING -d CCC.CCC.CCC.CCC -j SNAT -
-to ZZZ.ZZZ.ZZZ.ZZZ
```

1. AAA: Protokoll, tcp oder udp (meist TCP)
2. BBBB: Eingehender Port (z.B. 8080)

3. CCC.CCC.CCC.CCC: LAN-IP-Adresse des Geräts, auf das Sie den Port weiterleiten wollen, z.B. 192.168.178.1, 192.168.0.1, 192.168.1.1, 192.168.2.1 usw.
4. DDDD: Port des Router-Webinterfaces (meist 80)
5. ZZZ.ZZZ.ZZZ.ZZZ = LAN-IP des E1200

Beispiel für Fritz!Box:

VORAUSGESETZT DER E1200 HAT DIE LAN-IP-ADRESSE 192.168.178.254

```
iptables -t nat -A PREROUTING -i tap1 -p tcp --dport 8080 -j DNAT --to
192.168.178.1:80
iptables -t nat -A POSTROUTING -d 192.168.178.1 -j SNAT --to 192.168.178.254
```

Damit wird das Webinterface Ihrer Fritz!Box unter

http://Ihre.feste.IP:8080

---

erreichbar.

Hinweis: Die zusätzliche SNAT-Regel ist nur notwendig, falls Sie Dienste Ihres Standardgateways nutzen möchten wie z.B. das Webinterface der Fritz!Box o.Ä. Falls Sie nur Server / Dienste hinter Ihrem Standardgateway nutzen möchten sind diese Regeln nicht erforderlich!

Hintergrund

Beispiel-Aufbau:

1. Internet-Router: Fritz!Box. IP: 192.168.178.1
2. Linksys E1200: IP 192.168.178.254
3. Externer Zugriff von 85.25.258.123 auf Web-Interface der Fritz!Box

Ohne SNAT-Regel:

1. Paket aus dem Internet: Absender-IP-Adresse 85.25.258.123
2. Linksys E1200
3. Port-Weiterleitung an Fritz!Box
4. Fritz!Box: Antwort an 85.25.258.123
5. IP liegt nicht im Subnetz der Fritz!Box
6. Fritz!Box schickt Antwort an Standard-Gateway (Provider-Router)
7. Kann das Paket keiner Verbindung zuordnen
8. — Paket wird spätestens hier verworfen —

Mit SNAT-Regel:

1. Paket aus dem Internet: Absender-IP-Adresse 85.25.258.123
2. Linksys E1200
3. Port-Weiterleitung an Fritz!Box
4. SNAT: 85.25.258.123 wird durch 192.168.178.254 ersetzt
5. Fritz!Box: Antwort an 192.168.178.254
6. IP liegt im Subnetz der Fritz!Box
7. Fritz!Box schickt antwort an E1200

8. SNAT: 192.168.178.254 wird durch 85.25.258.123 ersetzt
9. Zuordnung kann stattfinden
10. — Antwort an 85.25.258.123 wird zugestellt. —

Hinweis: Dieser Vorgang hat zur Folge, dass die z.B. Fritz!Box als Absender-IP nicht mehr eine öffentliche IP-Adresse sondern eine LAN-IP-Adresse “sieht”. Pakete, die mittels SNAT modifiziert wurden behandelt die Fritz!Box also als LAN-Pakete, nicht als Internet-Pakete. Daher greifen in diesem Fall alle Einstellungen nicht mehr, die sich ausschließlich auf Internet-Pakete beziehen. Eine andere Konfiguration ist an dieser Stelle aber leider nicht möglich, dafür sind die Konfigurationsmöglichkeiten der meisten Provider- bzw. Consumer-Geräte zu begrenzt.

9. Zugriff auf Web-Interface und Telnet beschränken

Nach Abschluss der Konfiguration ist der Linksys E1200 weltweit aus dem Internet mittels seiner festen, öffentlichen IPv4-Adresse erreichbar. Sie können den Zugriff auf das Web-Interface und den Telnet-Zugang mithilfe dieser Regeln beschränken:

1. Falls Sie bereits eigene Firewall-Regeln verwenden, bitte zunächst auf “Edit” unter dem Textbereich “Firewall” klicken, da sonst die vorhandenen Regeln überschrieben werden.
2. Unter Administration > Commands in das Feld “Commands” kopieren und dann auf “Save Firewall” klicken.
3. Falls Sie Port 80 oder Port 23 bereits an ein anderes Gerät weiterleiten, sind die Regeln nicht notwendig.

```
# Telnet nur von lokal oder IXS Netz erlauben

 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 23 -s 10.0.0.0/8 -j ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 23 -s 172.16.0.0/12 -j
ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 23 -s 192.168.0.0/16 -j
ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 23 -s 212.58.67.1/24 -j
ACCEPT
 iptables -A INPUT -i tap1 -p tcp -m tcp --dport 23 -j DROP

 # Web-Interface nur von lokal oder IXS Netz erlauben

 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 80 -s 10.0.0.0/8 -j ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 80 -s 172.16.0.0/12 -j
ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 80 -s 192.168.0.0/16 -j
ACCEPT
 iptables -I INPUT -i tap1 -p tcp -m tcp --dport 80 -s 212.58.67.1/24 -j
ACCEPT
 iptables -A INPUT -i tap1 -p tcp -m tcp --dport 80 -j DROP
```

Fehlerbehebung / Fehlerdiagnose

Falls Ihr DD-WRT-Router keine Verbindung zu unserem VPN-Service mit fester, öffentlicher IP-Adresse aufbaut nutzen Sie bitte unsere Tipps zur Fehlerbehebung und Diagnose.

Die Fehlerdiagnose kann nicht über das Webinterface von DD-WRT durchgeführt werden. Bitte verbinden Sie sich mit Telnet oder SSH mit Ihrem DD-WRT-Gerät. Nutzen Sie hierfür eine Software wie Putty unter Windows oder diesen Befehl unter

Linux:

`telnet 123.456.789.0`

Windows:

1. Öffnen Sie “putty.exe”
2. Host Name (or IP address): `123.456.789.0 (LAN-IP des Geräts)`
3. Port: `23`
4. Connection type: `Telnet`

Wobei `123.456.789.0` der IP-Adresse Ihres DD-WRT Routers entspricht.

Falls Sie Putty nicht kennen oder die Linux-Kommandozeile noch nie verwendet haben, haben wir hier eine Kurzanleitung für Sie bereitgestellt:

Putty verwenden

Standardzugangsdaten:

Benutzer: `root` Passwort: `admin`

Ping / DNS-Auflösung testen

Bevor überhaupt eine VPN-Verbindung hergestellt werden kann muss Ihr DD-WRT-Router auf jeden Fall eine primitive Verbindung mit Internet XS herstellen können bzw. Ihr lokales Netz muss fehlerfrei funktionieren. Zur Diagnose setzen Sie einen Ping-Befehl ab.

`ping -c 3 ovpnip3.internet-xs.de`

Sie erhalten eine ähnliche Ausgabe wie

```
[root@ddwrt ~]# ping -c 3 ovpnip3.internet-xs.de
PING ovpnip3.internet-xs.de (212.58.69.3) 56(84) bytes of data.
64 bytes from ovpnip3.internet-xs.de (212.58.69.3): icmp_seq=1 ttl=64
time=2.14 ms
64 bytes from ovpnip3.internet-xs.de (212.58.69.3): icmp_seq=2 ttl=64
time=0.808ms
64 bytes from ovpnip3.internet-xs.de (212.58.69.3): icmp_seq=3 ttl=64
time=1.06 ms
--- ovpnip3.internet-xs.de ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2082ms
rtt min/avg/max/mdev = 0.808/1.336/2.142/0.580 ms
```

Falls Sie die folgende Meldung erhalten:

```
[root@ddwrt ~]# ping -c 3 ovpnip3.internet-xs.de
ping: unknown host ovpnip3.internet-xs.de
```

Funktioniert die DNS-Auflösung in Ihrem lokalen Netzwerk nicht. Bitte prüfen Sie die Konfiguration oder ersetzen Sie die Zeile

```
remote ovpnip3.internet-xs.de 1194
```

durch

```
remote 212.58.69.3 1194
```

Wichtig: So lange der Ping-Befehl nicht funktioniert bzw. unser VPN-Server für Sie nicht erreichbar ist, wird auch keine VPN-Verbindung herstellt werden können. Bitte prüfen Sie Ihre lokale Netzwerkkonfiguration.

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.

