KB 87962: OVPNIP8

IP-Tunnel mit OpenVPN einrichten auf Linksys WRT3200 ACM

Stand	24.09.2024, 16:29:19
Version	66f2ccbf
Referenz-URL	https://www.internet-xs.de/kb/87962
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-87962-66f2ccbf.pdf

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

Zielgruppe:
Administratoren eines Linksys WRT3200ACM, die eine feste, öffentliche IPv4-Adresse mittels OpenVPN-Tunnel (IP-Tunnel) in das LAN transportieren 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: 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.

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

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.

Es gibt zwei Konfigurationsvarianten:

Konfiguration als IP-Client

Diese Konfigurationsvariante eignet sich besonders für die Integration in ein bestehendes Netzwerk. Der Linksys WRT3200ACM befindet sich dabei nur im bestehenden LAN und öffnet selbst kein neues Netzwerk. Es wird nur die **ETHERNET**-Buchse verwendet, die **INTERNET**-Buchse (“WAN”) bleibt ungenutzt.

Beispiele für die Verwendung dieser Variante:

- IP-Kameras, Webcams, Datenlogger, die sich bereits im LAN befinden

Konfiguration als DMZ-Router / kaskadierter Router

Mit dieser Konfigurationsvariante eröffnet der Linksys WRT3200ACM neben dem bestehenden LAN ein neues LAN, fortan “DMZ” genannt. Alle Geräte, die über die feste IP-Adresse kommunizieren und / oder mittels Port-Weiterleitungen (DNAT) über die feste IP-Adresse des IP-Tunnels aus dem Internet erreichbar gemacht werden sollen, befinden sich in einem neuen, abgetrennten Netzwerk. Die Nutzung dieser Variante ist auch erforderlich, wenn Sie dem Linksys WRT3200ACM einen Firewall-Router (cisco ASA, Fortigate usw.) nachschalten möchten. Der Router ist mit der **INTERNET**-Buche mit dem bestehenden Router verbunden, die Buchsen **ETHERNET 1** - **ETHERNET 4** können für den Anschluss von DMZ-Geräten oder einem Switch genutzt werden.

- Aufbau eines neuen Server-Netzwerks
- DSL-Backup-Leitung (z.B. mit einem dem Linksys WRT3200ACM vorgeschalteten LTE-Router und einem dem Linksys WRT3200ACM nachgeschalteten Firewall-Router mit mehreren WAN-Ports)

Anforderungen

- Linksys WRT3200ACM
- Test-Zugang oder permanenter Zugang auf dem Einwahlserver OVPNIP8 (ovpnip8.internet-xs.de / 212.58.69.24 / Benutzernamen mit ixs024-xxxx)
- Funktionierender, stabiler, bestehender Internet-Zugang
- Freier Switch-Port am Internet-Router oder Switch

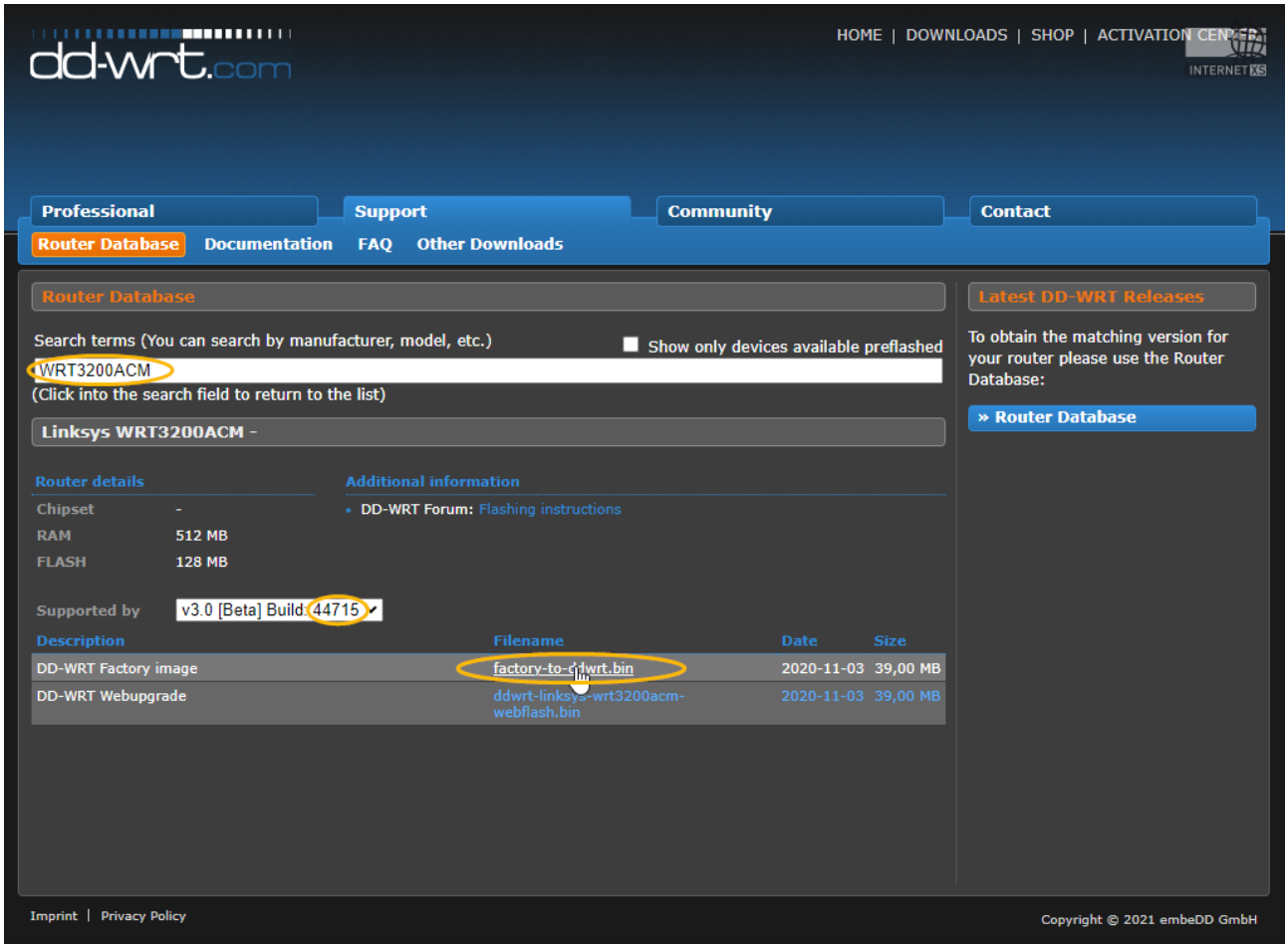
Konfigurations-PC vorbereiten

Suchen und laden Sie hier eine DD-WRT-Version größer oder gleich **44715**, Image-Typ **factory-to-ddwrt.bin** herunter:

https://dd-wrt.com/support/router-database/

(Suchbegriff = WRT3200ACM)

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.



Geben Sie Ihrem Konfigurations-PC eine statische IP-Konfiguration, z.B.

1. IP-Adresse: 192.168.1.50
2. Subnetzmaske: 255.255.255.0
3. Standard-Gateway: 192.168.1.1
4. DNS 1: 192.168.1.1

(https://support.microsoft.com/de-de/windows/%C3%A4ndern-der-tcp-ip-einstellungen-bd0a07af-15f5-cd6a-363f-ca2b6f391ace)

Erste Anmeldung am Standard Web-Interface

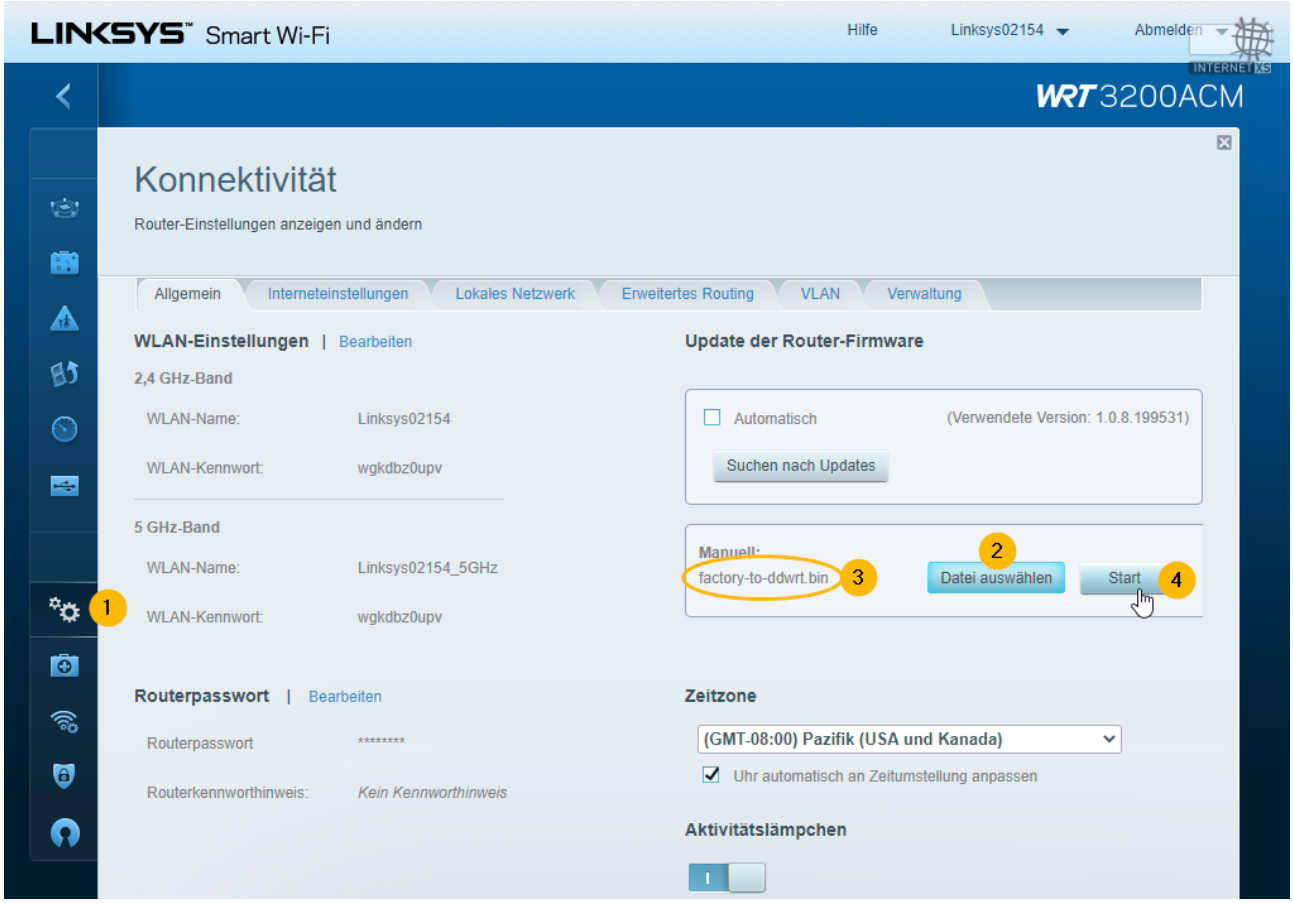
Öffnen Sie die Web-Oberfläche des Linksys WRT3200ACM. Die Standard-Zugangsdaten lauten:

1. URL: http://192.168.1.1/
2. Ich habe die Lizenzvereinbarung gelesen und akzeptiere sie.: Aktiviert
3. Ich möchte dazu beitragen, zukünftige Verbesserungen zu ermöglichen, indem ich Linksys über Router-Fehler und Diagnosen informiere.: Deaktiviert
4. Klicken Sie auf **Manuelle Konfiguration**
5. Nach wenigen Sekunden erscheint eine Meldung **Internetverbindung ist inaktiv**.
6. Klicken Sie auf **Anmelden**
7. Routerpasswort: **admin**

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

Upgrade auf DD-WRT

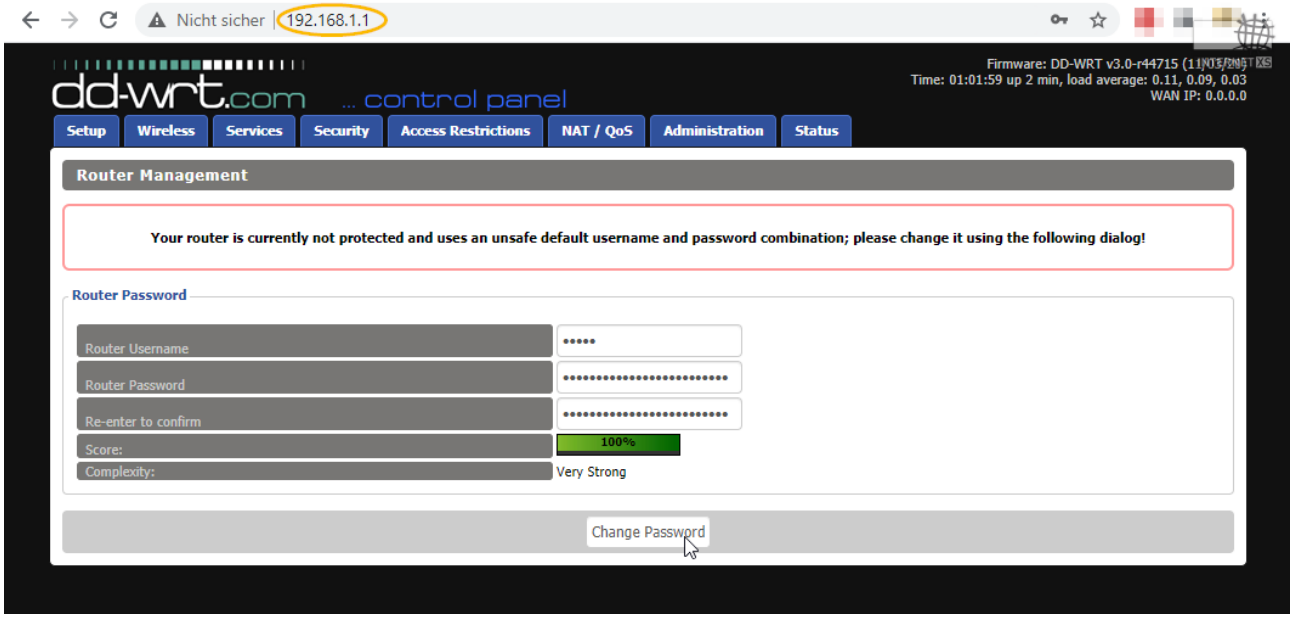
1. Navigieren Sie zu **Konnektivität**
2. Im Bereich **Update der Router-Firmware** im Abschnitt **Manuell** klicken Sie auf **Datei auswählen** und wählen die zuvor heruntergeladene DD-WRT Firmware (factory-to-ddwrt.bin) auf dem Computer aus.
3. Klicken Sie auf **Start**
4. Bestätigen Sie die Meldung **Nicht erkannter Dateiname** mit **Ja**
5. Bestätigen Sie die Meldung **Firmware aktualisieren** mit **Ja**
6. Nach einigen Sekunden erscheint die Meldung **Ihr Router wird neu gestartet**. Bestätigen Sie mit **OK**.
7. Warten Sie 5 Minuten.



Anmelden am DD-WRT Web-Interface

1. Schließen Sie das Browser-Fenster, mit dem Sie mit dem Standard-Web-Interface verbunden waren.
2. Öffnen Sie das DD-WRT-Web-Interface unter http://192.168.1.1
3. Vergeben Sie einen Router Username und ein Router Passwort. Bitte wählen Sie ein sicheres Passwort.
4. Klicken Sie auf **Change Password**

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.



Basis-Netzwerkkonfiguration

Navigieren Sie zu **Setup** (Sie werden jetzt zur Eingabe des zuvor festgelegten Benutzernamens und Passworts aufgefordert)

Abschnitt WAN Connection Type

Falls Sie den Linksys WRT3200ACM als **IP-Client** konfigurieren möchten, wählen Sie hier **Disabled**. Diese Variante eignet sich für die Integration des Routers in ein bestehendes Netzwerk.

Falls Sie den WRT3200ACM als **DMZ-Router** bzw. kaskadierten Router konfigurieren möchten, wählen Sie entweder **Automatic Configuration - DHCP** oder Static IP und vergeben Sie eine IP-Konfiguration, die zum vorgeschalteten Router passt. Diese Variante eignet sich, wenn Sie Server, Datenlogger, Webcams usw. in einem vom vorgeschalteten Router getrennten Netzwerk betreiben möchten.

Beispiel:

- WAN IP Address: 192.168.178.254
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.178.1
- Static DNS 1: 192.168.178.1

Wobei 192.168.178.254 eine beliebige freie IP-Adresse außerhalb des DHCP-Bereichs aus dem Netzwerk des vorgeschalteten Routers ist und 192.168.178.1 der LAN-IP-Adresse des vorgeschalteten Routers entsprechen muss.

Abschnitt Optional Settings

1. Router Name: Vergeben Sie einen Namen oder behalten Sie den Standard-Wert (DD-WRT) bei.
2. Hostname: Vergeben Sie einen Namen oder behalten Sie den Standard-Wert (leer) bei.

Abschnitt Network Setup > Router IP

Falls Sie den Router als IP-Client konfigurieren

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

1. Local IP Address: Eine beliebige freie IP-Adresse außerhalb des DHCP-Bereichs Ihres bestehenden Internet-Routers (bspw. 192.168.178.254)
2. Subnet Mak: I.d.R. 255.255.255.0
3. Gateway: LAN-IP-Adresse des bestehenden Internet-Routers (z.B. 192.168.178.1)
4. Local DNS: LAN-IP-Adresse des bestehenden Internet-Routers (z.B. 192.168.178.1)

Falls Sie den Router als DMZ-Router / kaskadierten Router konfigurieren

1. Local IP Address: Eine beliebige IP-Adresse aus einem Netz, das **nicht** der vorgeschaltete Router verwendet (bspw. 192.168.179.1)
2. Subnet Mask: I.d.R. 255.255.255.0
3. Gateway: 0.0.0.0
4. Local DNS: 0.0.0.0

Abschnitt Network Address Server Settings (DHCP)

Der DHCP-Server sollte in jedem Fall deaktiviert werden.

1. DHCP Server: **Disable**

Abschnitt Time Settings

1. NTP Client: Enable
2. Time Zone: I.d.R. Europe/Berlin
3. Server IP/Name: **de.pool.ntp.org**

Zwischenspeichern

1. Klicken Sie auf **Save**
2. Klicken Sie auf **Apply Settings**.
3. Stellen Sie die LAN-IP-Konfiguration des Konfigurations-PCs wieder auf “Automatisch” (Konfiguration als IP-Client) oder geben Sie dem Konfigurations-PC eine LAN-IP-Adresse aus dem DMZ-Netzwerk (bspw. 192.168.179.50)
4. Der Router ist nach wenigen Sekunden unter seiner neuen LAN-IP-Adresse erreichbar.

- Konfiguration als IP-Client: z.B. http://192.168.178.254
- Konfiguration als DMZ-Router / kaskadierter Router: z.B. http://192.168.179.1

Verkabelung

Konfiguration als IP-Client

1. Die Buche **INTERNET** ist nicht verbunden
2. Die Buchse **ETHERNET 1** ist mit dem bestehenden Internet-Router verbunden
3. Der Konfigurations-PC ist mit dem bestehenden Internet-Router verbunden
4. Die Buchse **ETHERNET 2** bis **ETHERNET 3** sind nicht verbunden

Konfiguration als DMZ-Router / kaskadierter Router

1. Die Buchse **INTERNET** ist mit dem bestehenden Internet-Router verbunden

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

2. Die Buchsen **ETHERNET 1** bis **ETHERNET 4** ist mit dem Konfigurations-PC und / oder einem Switch verbunden, an dem die Geräte der DMZ angeschlossen sind. Alternativ können die DMZ-Geräte auch direkt am Linksys WRT3200 ACM angeschlossen werden.

Uhrzeit prüfen

Oben rechts sollte bei **Time:** eine aktuelle Uhrzeit angezeigt werden:

Firmware: DD-WRT v3.0-r44715 std (11/03/20) **Time: 12:31:16** up 6 min, load average: 0.00, 0.01, 0.00

So lange dies nicht der Fall ist, hat der Router keine Internet-Verbindung. Bitte prüfen Sie in dem Fall die zuvor vorgenommenen Einstellungen.

Internet-Verbindung prüfen

Navigieren Sie zu **Administration** > **Commands**. Kopieren Sie diesen Befehl in das Textfeld **Commands**:

```
ping -c 5 ovpnip8.internet-xs.de
```

Klicken Sie anschließend auf **Run Commands**. Nach einigen Sekunden sollte eine Ausgabe ähnlich dieser angezeigt werden:

```
PING ovpnip8.internet-xs.de (212.58.69.24): 56 data bytes
64 bytes from 212.58.69.24: seq=0 ttl=63 time=0.604 ms
64 bytes from 212.58.69.24: seq=1 ttl=63 time=0.575 ms
64 bytes from 212.58.69.24: seq=2 ttl=63 time=0.602 ms
64 bytes from 212.58.69.24: seq=3 ttl=63 time=0.623 ms
64 bytes from 212.58.69.24: seq=4 ttl=63 time=0.685 ms

--- ovpnip8.internet-xs.de ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.575/0.617/0.685 ms
```

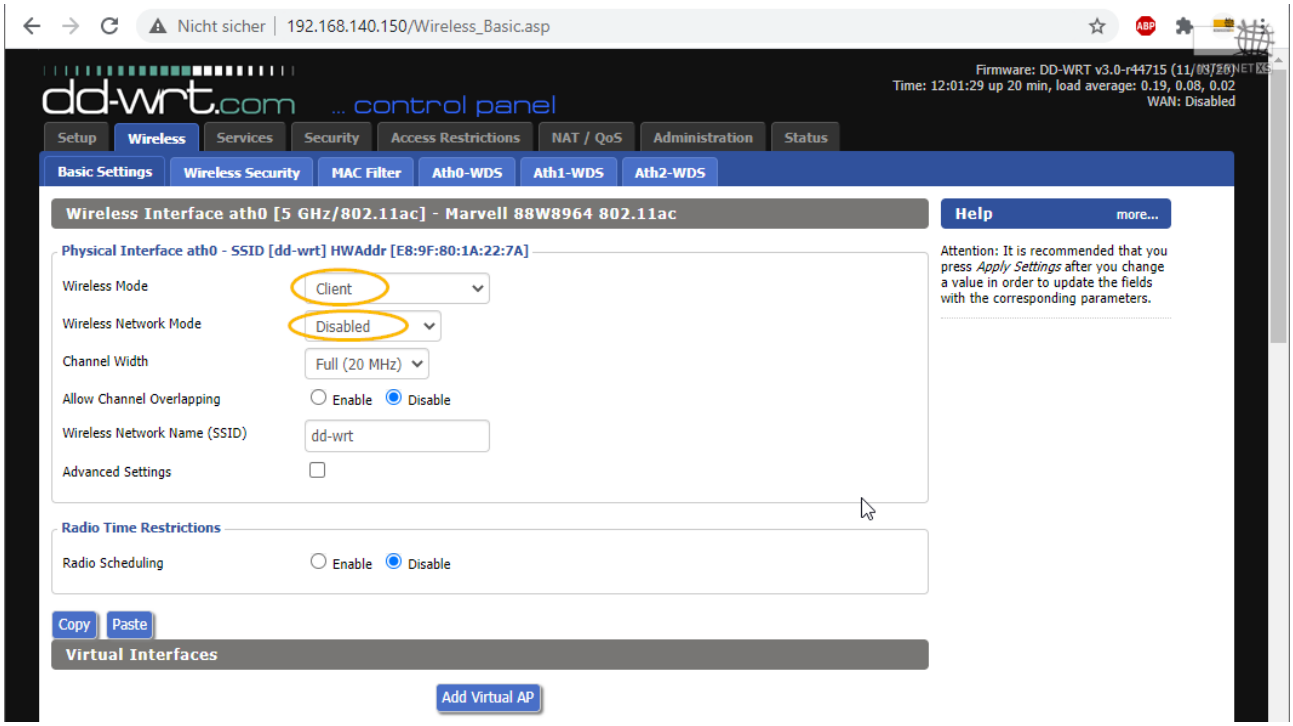
0% packet loss ist erforderlich, um mit der Konfiguration fortzufahren. Falls eine andere Ausgabe erscheint wie z.B. `ping: bad address 'ovpnip8.internet-xs.de'` oder `100% packet loss`, prüfen Sie die Basis-Netzwerkkonfiguration und die Verkabelung.

Wireless deaktivieren

I.d.R. benötigt das IP-Gateway kein WLAN. Deshalb sollte WLAN / Wifi deaktiviert werden.

1. Navigieren Sie zu **Wireless** > **Basic Settings**
2. Stellen Sie bei allen Interfaces den Wireless Mode auf **Client** und **Wireless Network Mode** auf **Disabled**.
3. Klicken Sie auf **Save** und dann auf **Apply Settings**
4. Prüfen Sie z.B. mit einem Smartphone, ob die Wireless-Funktion des Routers wirklich deaktiviert wurde.

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.



Status-Seite deaktivieren

Damit die Status-Seite nicht öffentlich eingesehen werden kann, sollte die Passwort-Abfrage für die Status-Seite aktiviert und die Status-Seite deaktiviert werden.

1. Navigieren Sie zu **Administration** > **Management**
2. Info Site Password Protection: Enabled
3. Enable Info Site: Disable
4. Klicken Sie auf **Save**
5. Klicken Sie auf **Apply Settings**

nvram Einstellungen vornehmen

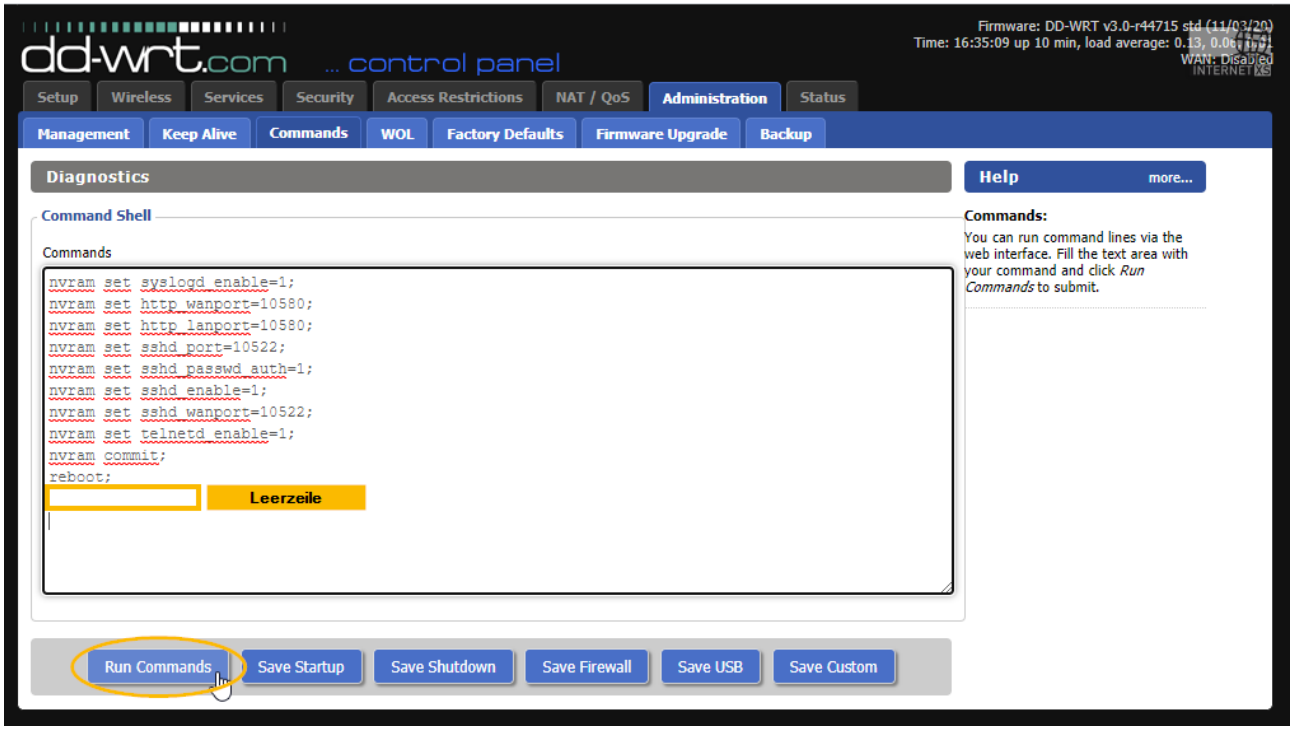
Zur deaktivierung von Telnet, Aktivierung von SSH mit Passwort-Authentifizierung und zur Änderung des Web-Interface Ports können diese nvram-Befehle verwendet werden. Die Eignabe ist alternativ über telnet möglich.

1. Navigieren Sie zu **Administration** > **Commands**
2. Kopieren Sie diese Befehle **inkl. der Leerzeile** am Ende in das Textfeld **Commands**:

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

```
nvram set syslogd_enable=1;
nvram set http_wanport=10580;
nvram set http_lanport=10580;
nvram set sshd_port=10522;
nvram set sshd_passwd_auth=1;
nvram set sshd_enable=1;
nvram set sshd_wanport=10522;
nvram set telnetd_enable=0;
nvram commit;
reboot;
```

3. Klicken Sie auf **Run Commands**
4. Der Befehlsblock beinhaltet einen `reboot`, der einige Sekunden dauert.
5. Danach ist das Web-Interface unter http://192.168.178.254:10580 (Konfiguration als IP-Client) bzw. http://192.168.179.1:10580 (Konfiguration als DMZ-Router / kaskadierter Router) erreichbar. Die Kommandozeile ist per SSH unter 192.168.178.254:10522 (Konfiguration als IP-Client) bzw. 192.168.179.1:10522 (Konfiguration als DMZ-Router / kaskadierter Router) erreichbar.



Konfiguration OpenVPN Client

Navigieren Sie zu **Services** > **VPN**. Suchen Sie den Abschnitt OpenVPN **Client**. Nehmen Sie die folgenden Einstellungen vor:

1. Start OpenVPN Client: Enable
2. CVE-2019-14899 Mitigation: Enable
3. Server IP/Name: 212.58.69.24 (setzen Sie hier **nicht** die Ihrem IP-Tunnel-Zugang zugeteilte feste IP-Adresse ein!)
4. Port: 1194
5. Tunnel Device: TUN
6. Tunnel Protocol: UDP

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

7. Encryption Cipher: None
8. Hash Algorithm: SHA1
9. First Data Cipher: Not set
10. Second Data Cipher: Not set
11. Third Data Cipher: Not set
12. User Pass Authentication: Enable
13. Username: Benutzername / Zugangskennung Ihres IP-Tunnel-Zugangs (bspw. ixs024-1234-a1b2c3d4)
14. Passwort: Das dem IP-Tunnel-Zugang zugeteilte Passwort
15. Advanced Options: Enable
16. TLS Cipher: None
17. Compression: Disabled
18. NAT: Enable
19. Inbound Firewall on TUN: Deaktiviert
20. IP Address: leer
21. Subnet Mask: leer
22. Tunnel MTU setting: 1500
23. Tunnel UDP Fragment: leer Tunnel UDP MSS-Fix: Disable
24. Verify Server Cert.: Aktiviert
25. TLS Key choice: TLS Auth
26. TLS Key: leer
27. Additional Config:

```
reneg-bytes 0
reneg-sec 0
explicit-exit-notify
txqueuelen 1000
float
keepalive 20 120
fast-io
data-ciphers-fallback none
```

28. Policy based Routing: leer
29. PKCS12 Key: leer
30. Static Key: leer
31. CA Cert:

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

```
-----BEGIN CERTIFICATE-----
MIIFWDCCA0CgAwIBAgIJAM6lHqecPPDWMA0GCSqGSIb3DQEBCwUAMCExHzAdBgNV
BAMMFm92cG5pcDguaW50ZXJuZXQteHMuZGUwIBcNMjQwOTI0MTEzMzIxWhgPMjEw
MTA1MjQxMTMzMjFaMCExHzAdBgNVBAMMFm92cG5pcDguaW50ZXJuZXQteHMuZGUw
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDEQ+LMHtB7BtX1tXB66r9b
+wD93ZSy2Grquv4xweCkeF8ttSJq7pS7Vt+goGFqAS4fOtqofs6iDgliEs/luWQW
lzmW+HgDzni8DZkWFdnSbGc8pMCp1HrQSlJm3NXPc+jUVIOeWy8gPed2WP92aJs2
x1oWFgSD7FvFkDgWMCXsVYZOMCzSc0+55zY8cB/BYYATlSCG4CZ9NJtw/JVecIFa
CaYyMPN8bpbdYW+OrBApbsfDJqICX6iIoC7owyKMOy6/LSluSrUYzVLoHV0JG7kP
5VGhEEA4F926z7shJSNzVSZWUE7CRueKRm+QlSAiloiASSI02jCwy4tmSRaEriEL
pA/kWTnJF+61bsKorkGinkWqksiYokZo0diXqThDV/0C3P0eKgX1AtR2WhoQr9ke
A7IvLdDtAxYKDr9DBNgfL5f/MdJcD17TBj8PzDNdh1W5kSLuYMwzxW/bScBpgfro
KIn2jKtMEbFl+qBmzu3cWttMkCIoKPKO+Pr9ZGsvYzcOvxsCxWEG5/PgZjL3Sf/B
4Pa7bQSyTbQOdocxjRs8qmrt58DFBoCOc3db3OD6BqQ35e9AMUgx0R7CxbsNrGXf
qSnyg9HvI7bSWxDVm4bzpw29lTk6dshDHtwXrDUlOzgmho0S6yWljykV9kJLRTT/
O9AZvYs6rB5fSWVfOSvzUwIDAQABo4GQMIGNMB0GA1UdDgQWBBQ/aVQtQzAloOGh
6DGWPgwG7hqBCTBRBgNVHSMESjBIgBQ/aVQtQzAloOGh6DGWPgwG7hqBCaElpCMw
ITEfMB0GA1UEAwwWb3ZwbmlwOC5pbnRlcm5ldC14cy5kZYIJAM6lHqecPPDWMAwG
A1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQCGa+jS
Vj3Zgmtqvdb5K+ufAPU00ude2BlgA2v3waNB1uXsvA5d7O21HfaBrtYobVewQ1FH
00Xm8skxrV3fwdeTs1GBQ7Sy95TuKER1FOMnRGLiJJQOmsvkyQkuopQW2q4Aon5h
rdhQIim4hmutiNK/LtLcePe/D8pVSn8CxZ0h8M7WYfp2yqEOOwcXAEk2VIW03YcE
z4pVEuwEkJT1Pha6KVXcVmYsvknACqm6hneaexZXHIrSNbDtm0Ap2GSzG/nLlKr6
E30UlZB7hsAjBmM0TxF8HS6g6npzhxeANqy3Zst+vBomfbJI6AmWQn3kvWkZS8V/
ZxhDptR7Cp14OtIN0VNvBR7DZzNbgNUs23wDGEqLUqlHVFciiIzipSOXxICJGfbr
bwABBi5KSQWokluMR4kyhWJb7e3Kv88HPGhaIDyQkemF4qKx4T0RN9vYxwDoErXp
AI7gqXSmJ8v/5PgRvZ2Hm+bN2HYB369JsF2TcngctIQGv91SIaPTOSveeVmDLoan
4MpgTa0NVwcoO/qzXFH4kMskcmAKJ9ZZIDAKiZ1VTprUz/2ua56cAo1a9HCwTeoD
1yA3uuKtGQS7hqfCW00ZoKAWG7xl8a1Sk460GcN5trABc7d817nbHr3dn+WcGlW
g4yUi2HNRaZt2VMGp3FJpPLdxxhLCJXh+RQCxg==
-----END CERTIFICATE-----
```


32. Public Client Cert: leer
33. Private Client Key: leer
34. Klicken Sie auf **Save**
35. Klicken Sie auf **Apply Settings**

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

OpenVPN Client

OpenVPN Client

Start OpenVPN Client	(●) Enable ( ) Disable
CVE-2019-14899 Mitigation	(●) Enable ( ) Disable
Server IP/Name	212.58.69.4
Port	1194 (Default: 1194)
Tunnel Device	TUN
Tunnel Protocol	UDP
Encryption Cipher	None
Hash Algorithm	SHA1
First Data Cipher	Not set
Second Data Cipher	Not set
Third Data Cipher	Not set
User Pass Authentication	(●) Enable ( ) Disable
Username	[redacted]
Password	[redacted]
Advanced Options	(●) Enable ( ) Disable
TLS Cipher	None
Compression	Disabled
NAT	(●) Enable ( ) Disable
Inbound Firewall on TUN	[x]
IP Address	
Subnet Mask	
Tunnel MTU setting	1500 (Default: 1500)
Tunnel UDP Fragment	(Default: Disable)
Tunnel UDP MSS-Fix	( ) Enable (●) Disable
Verify Server Cert.	[x]
TLS Key choice	( ) TLS Crypt (●) TLS Auth

TLS Key

Additional Config

```
reneg-bytes 0
reneg-sec 0
```

Policy based Routing

PKCS12 Key

Static Key

CA Cert

```
-----BEGIN CERTIFICATE-----
MIIFVjCCAz6gAwIBAgIJAJdvGtb8dDNOMA0GCSqGSIb3DQEBCwUAMCExHzAdBgNV
```

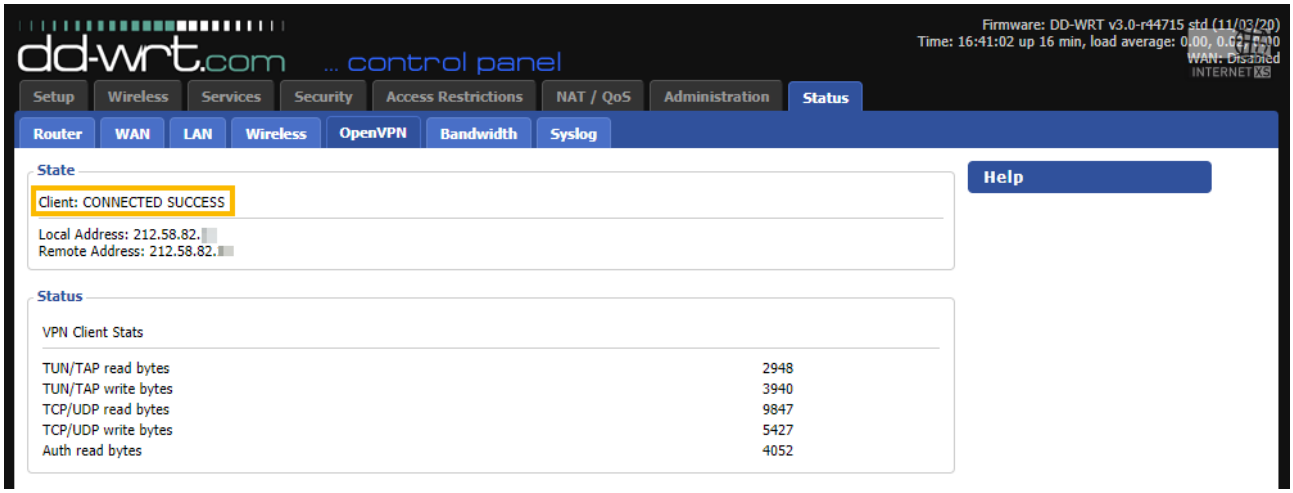
Public Client Cert

Private Client Key

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

Ausführung des OpenVPN Clients prüfen

Navigieren Sie zu **Status** > **OpenVPN**. Im Bereich **State** sollte in der Zeile **Client: CONNECTED SUCCESS** stehen. Bei **Local Address** sollte die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse angezeigt werden.



Konnektivität prüfen

Öffnen Sie das Web-Interface des Routers über die Ihrem IP-Tunnel-Zugang zugeteilte feste, öffentliche IPv4-Adresse von einem Gerät aus, das sich nicht im lokalen Netzwerk befindet (z.B. mit einem Smartphone, das nur im mobilen Datennetz / LTE / 4G / 5G angemeldet ist):

http:*//Ihre feste IP-Adresse*:10580

Es sollte eine Anmeldeabfrage (Nutzername / Passwort) erscheinen.

Falls dies nicht der Fall ist, prüfen Sie alle Einstellungen aus dem Abschnitt **Konfiguration OpenVPN Client** sorgfältig. Jede kleinste Abweichung von den hier genannten Einstellungen führt dazu, dass die Verbindung fehlschlägt oder nicht nutzbar ist.

Keep-Alive und Auto-Reboot (optional, empfohlen)

Falls das Gerät an einem entlegenen Ort betrieben wird, an dem ein manueller Neustart nur schwer möglich ist empfiehlt es sich, einen regelmäßigen, geplanten Neustart zu aktivieren.

Navigieren Sie zu **Administration** > **Keep Alive**.

Abschnitt Schedule Reboot

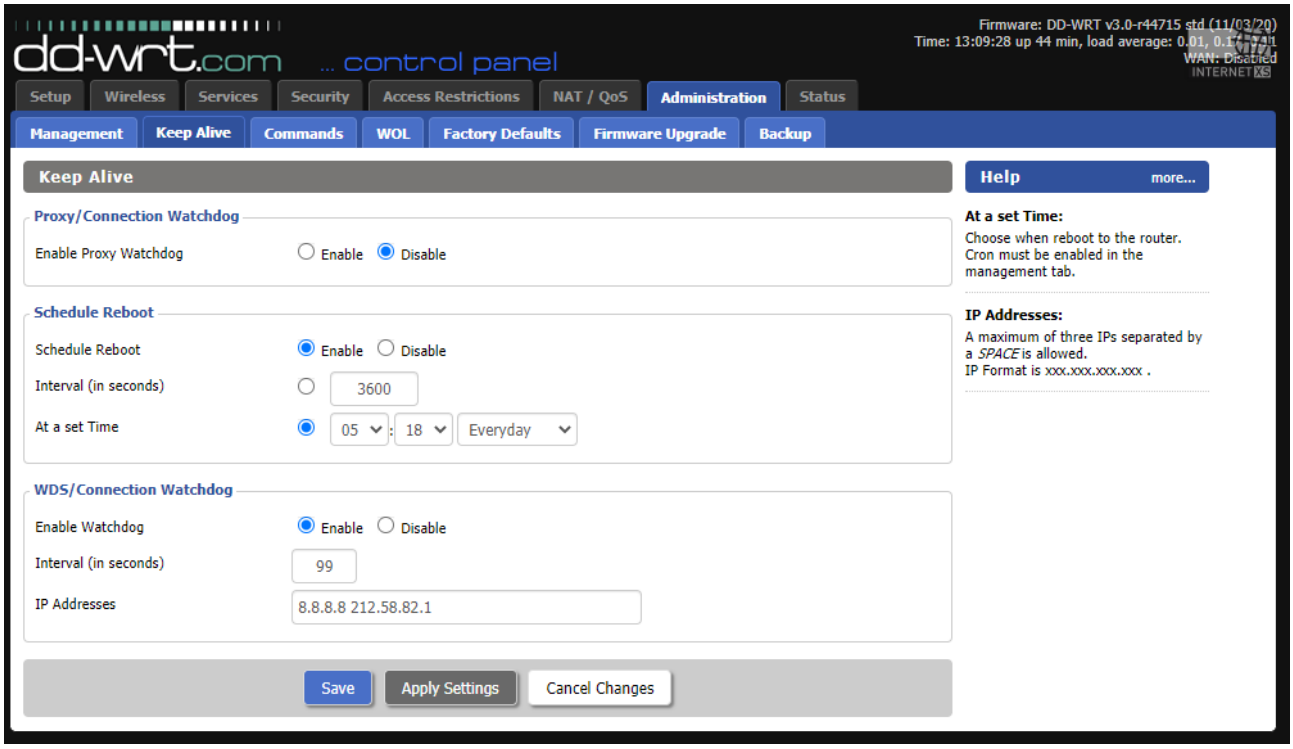
1. Schedule Reboot: Enable
2. Interval (in seconds): Deaktiviert
3. At a set Time: Aktiviert
4. Wählen Sie eine Uhrzeit, zu der der Anschluss i.d.R. nicht genutzt wird, bspw. 05:18
5. Wählen Sie als Wochentage **Everyday**

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

Abschnitt WDS/Connection Watchdog

1. Enable Watchdog: Enable
2. Interval (in seconds): Eine Zahl zwischen 90 und 110 (z.B. 99)
3. IP Adresses: `8.8.8.8 212.58.82.1`

Klicken Sie auf **Save**, danach auf **Apply Settings**.



Firewall und Port-Weiterleitungen

Die Firewall und Port-Weiterleitungen können für die per IP-Tunnel bereitgestellte feste IP leider nicht direkt über die Eingabefelder der Web-Oberfläche konfiguriert werden, da die dafür vorgesehenen Eingabefelder für die Anwendung nicht flexibel genug sind.

1. Navigieren Sie zu **Administration** > **Commands**
2. Geben Sie im Textfeld **Commands** Firewall-Regeln und Port-Weiterleitungen ein (siehe unten)
3. Klicken Sie auf **Save Firewall**
4. Zum Bearbeiten der Firewall klicken Sie im Abschnitt **Firewall** unten auf den Button **Edit**. Die derzeit aktive Firewall wird dann wieder in das Textfeld **Commands** kopiert, kann dort bearbeitet und mit **Save Firewall** wieder gespeichert werden.

Falls Sie Hilfe bei der Erstellung von passenden Firewall-Regeln haben, kontaktieren Sie uns bitte.

In der PDF-Version dieser Anleitung können Zeilen an anderen Stellen umgebrochen sein. Bitte prüfen Sie nach dem einfügen, ob unerwünschte Zeilenumbrüche mit kopiert / eingefügt wurden. Sie können dafür das Textfeld “Commands” im Browser etwas größer ziehen.

Passen Sie das Beispiel unten gemäß Ihren Anforderungen an:

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

```
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 443 -j DNAT --to
192.168.178.60:443
                                          ---         ---              -------
------- ---
                                           A           B
C        D
```

- A = Protokoll = `tcp` oder `udp`
- B = Eingehender Port, d.h. 212.58.82.X:8443; 8443 = Eingehender Port
- C = Ziel-LAN-IP-Adresse
- D = Ziel-Port

Der Eingehende Port (B) kann vom Ziel-Port (D) abweichen, falls benötigt. Somit lassen sich z.B. 5 Webcams, die alle den Port 443 erfordern, konfigurieren:

```
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8443 -j DNAT --to
192.168.178.60:443
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8444 -j DNAT --to
192.168.178.61:443
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8445 -j DNAT --to
192.168.178.62:443
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8446 -j DNAT --to
192.168.178.63:443
iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8447 -j DNAT --to
192.168.178.64:443
```

Sie können diesen Abschnitt als Vorlage verwenden. Abgesehen von den Beispielen sind dort folgende Einstellungen vorgenommen:

1. SSH (Port 10522) und Web-Interface (Port 10580) sind nur vo Internet XS aus erreichbar, d.h. aus dem öffentlichen Internet kann nicht auf SSH bzw. Web-Interface des Routers zugegriffen werden. Sie können die Regel weiter einschränken (z.B. auf einen eigenen IP-Bereich) oder entfernen (nicht empfohlen).
2. Forwarding von vlan2 <-> tun1 erlauben (erforderlich)
3. Forwarding von vlan2 <-> br0 erlauben (erforderlich)
4. ICMP immer erlauben (es ist nicht sinnvoll, ICMP zu sperren, da damit z.B. Path MTU Discovery funktionsunfähig wird)
5. Alle Pakete an die feste IP-Adresse, die nicht von vorhergehenden Regeln erfasst wurden, werden verworfen.

Um die Beispiele zu aktivieren, entfernen Sie das `#`-Symbol am Anfang der Zeile. Jede Zeile muss entweder leer sein, mit einem `#`-Symbol (Kommentar) oder dem Wort `iptables` beginnen. Umlaute und andere Sonderzeichen sollten vermieden werden.

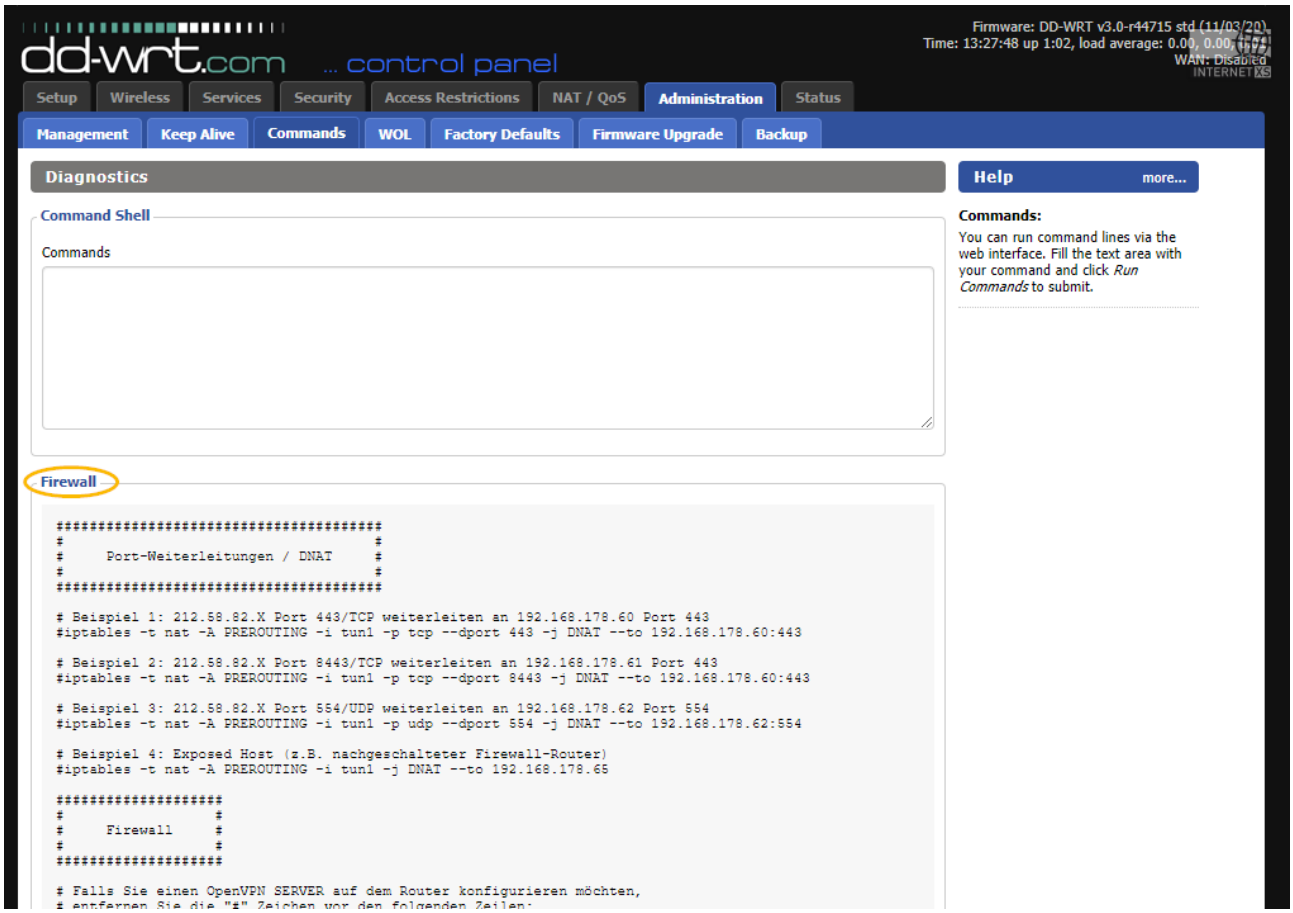
```
#########################################
#                                       #
#     Port-Weiterleitungen / DNAT       #
#                                       #
#########################################

# Beispiel 1: 212.58.82.X Port 443/TCP weiterleiten an 192.168.178.10 Port
443
#iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 443 -j DNAT --to
192.168.178.10:443
```

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

```
# Beispiel 2: 212.58.82.X Port 8443/TCP weiterleiten an 192.168.178.11 Port
443
#iptables -t nat -A PREROUTING -i tun1 -p tcp --dport 8443 -j DNAT --to
192.168.178.11:443

# Beispiel 3: 212.58.82.X Port 554/UDP weiterleiten an 192.168.178.12 Port
554
#iptables -t nat -A PREROUTING -i tun1 -p udp --dport 554 -j DNAT --to
192.168.178.12:554

# Beispiel 4: 192.168.178.13 ist Exposed Host (z.B. nachgeschalteter
Firewall-Router)
#iptables -t nat -A PREROUTING -i tun1 -j DNAT --to 192.168.178.13

####################
#                  #
#     Firewall     #
#                  #
####################

# Falls Sie einen OpenVPN SERVER auf dem Router konfigurieren möchten,
# entfernen Sie die "#" Zeichen vor den folgenden Zeilen:
#iptables -I INPUT -i tun1 -p tcp -m tcp --dport 443 -j ACCEPT
#iptables -t nat -A POSTROUTING -s 172.19.154.0/24 -o br0 -j MASQUERADE

# SSH an oeffentliche IP nur von Internet XS erlauben
# Bei Bedarf anpassen, auskommentieren oder loeschen
iptables -t nat -I PREROUTING -i tun1 -p tcp -m tcp --dport 10522 -s
212.58.67.1/24 -j ACCEPT
iptables -I INPUT -i tun1 -p tcp -m tcp --dport 10522 -s 212.58.67.1/24 -j
ACCEPT
iptables -A INPUT -i tun1 -p tcp -m tcp --dport 10522 -j DROP

# SSH an oeffentliche IP nur von Internet XS erlauben
# Bei Bedarf anpassen, auskommentieren oder loeschen
iptables -t nat -I PREROUTING -i tun1 -p tcp -m tcp --dport 10580 -s
212.58.67.1/24 -j ACCEPT
iptables -I INPUT -i tun1 -p tcp -m tcp --dport 10580 -s 212.58.67.1/24 -j
ACCEPT
iptables -A INPUT -i tun1 -p tcp -m tcp --dport 10580 -j DROP

##################################################
#                                                #
#     Forwarding, ICMP und Standard-Regel        #
#                                                #
##################################################

# Traffic von vlan2 <--> tun1 erlauben
iptables -I FORWARD -i vlan2 -o tun1 -j ACCEPT
iptables -I FORWARD -i tun1 -o vlan2 -j ACCEPT

# Traffic von br0 <--> tun1 erlauben
iptables -I FORWARD -i br0 -o tun1 -j ACCEPT
iptables -I FORWARD -i tun1 -o br0 -j ACCEPT

# ICMP erlauben
iptables -t nat -I PREROUTING -p icmp -j ACCEPT
iptables -I INPUT -p icmp -j ACCEPT
iptables -I FORWARD -p icmp -j ACCEPT
iptables -I OUTPUT -p icmp -j ACCEPT
```

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

```
# Alle anderen an oeffentliche IP verwerfen
iptables -A INPUT -i tun1 -j DROP
```



Statische LAN-IP-Konfiguration für mittels Port-Weiterleitungen / DNAT angesprochene Geräte

Bei Konfiguration als IP-Client

Auf alle Geräten (Datenlogger, Server, NAS, Alarmanlagen, Webcams etc.), die mittels Port-Weiterleitungen angesprochen werden, muss das Standard-Gateway die LAN-IP-Adresse des Linksys WRT3200 ACM (Beispiel: 192.168.178.254) umgestellt werden. Alle IP-fähigen Geräte haben dafür eine entsprechende Einstellungsmöglichkeit. Häufig ist diese unter TCP/IP Konfiguration oder Static IP Configuration zu finden. Synonyme für Standard-Gateway sind Default Gateway, Next Hop oder Router. Für weitere Informationen ziehen Sie die Bedienungsanleitung des jeweiligen Geräts zu Rate.

So lange das Standard-Gateway nicht auf die LAN-IP-Adresse des Linksys WRT3200 ACM eingestellt ist, funktionieren die Port-Weiterleitungen nicht.

Beispiel:

Datenlogger:

- IP-Adresse: 192.168.178.10
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.178.254
- DNS 1: 192.168.178.1

Kamera 1:

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

- IP-Adresse: 192.168.178.11
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.178.254
- DNS 1: 192.168.178.1

Kamera 2:

- IP-Adresse: 192.168.178.12
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.178.254
- DNS 1: 192.168.178.1

usw.

Bei Konfiguration als DMZ-Router / kaskadierter Router

Geräte, die sich im DMZ-Netz befinden, werden jeweils mit einer statischen LAN-IP aus dem DMZ-Netz konfiguriert. Beispiele:

Server 1:

- IP-Adresse: 192.168.179.10
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.179.1
- DNS 1: 192.168.179.1

Server 2:

- IP-Adresse: 192.168.179.11
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.179.1
- DNS 1: 192.168.179.1

Firewall-Router (“Exposed Host”)

- IP-Adresse: 192.168.179.13
- Subnetzmaske: 255.255.255.0
- Standard-Gateway: 192.168.179.1
- DNS 1: 192.168.179.1

usw.

Port-Weiterleitungen testen

Testen Sie die eingestellten Port-Weiterleitungen von einem externen Gerät (z.B. einem Smartphone, das nur mit dem mobilen Datennetz verbunden ist).

Beispiel:

https://*Ihre feste IP-Adresse*:8443

Wobei 8443 dem in der Port-Weiterleitung festgelegten, externen Port (B) entspricht.

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

Falls Sie Unterstützung bei der Erstellung von Firewall-Regeln / Port-Weiterleitungen benötigen, kontaktieren Sie uns bitte. Uns ist bewusst, dass diese Art der Konfiguration im Vergleich zu Consumer-Routern ungewohnt ist, jedoch ist sie deutlich flexibler und transparenter.

Konfigurationsbackup erstellen

Es ist ratsam, nach erfolgreicher Konfiguration ein Backup zu erstellen.

1. Navigieren Sie zu **Administration** > **Backup**
2. Klicken Sie auf **Backup**
3. Der Browser lädt eine Datei mit einem Dateinamen wie z.B. **nvrambak_r44715_DD-WRT_Linksys WRT3200ACM.bin** herunter.
4. Speichern Sie diese Datei an einem sicheren Ort ab.

Konfigurationsbackup einspielen

Falls eine Fehlkonfiguration vorgenommen oder das Gerät zurückgesetzt wurde, kann ein zuvor erstelltes Konfigurationsbackup so zurückgespielt werden:

1. Navigieren Sie zu **Administration** > **Backup**
2. Im Bereich **Restore Settings** wählen Sie das zuvor erstellte Konfigurationsbackup aus
3. Klicken Sie auf **Restore**

Fehlerdiagnose

Falls trotz penibler Prüfung aller vorgegebenen Einstellungen - besonders im Bereich OpenVPN-Client - keine Verbindung mit dem Einwahlserver zustande kommt, schicken Sie uns bitte das Syslog für eine weitere Analyse zu:

1. Starten Sie den Router neu
2. Warten Sie 5 Minuten
3. Navigieren Sie bitte zu **Status** > **Syslog**
4. Kopieren Sie alle Seiten (Navigation mit Next/Prev) in eine E-Mail
5. Geben Sie den IP-Tunnel-Zugang Benutzernamen / Zugangskennung und die zugeteilte IP-Adresse an
6. Schicken Sie uns das Syslog per E-Mail an info@internet-xs.de.

© 2024 Internet XS Service GmbH. Alle Rechte vorbehalten.

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.

Die Weiterverbreitung dieses Dokuments, der darin befindlichen Inhalte, auch nur Auszugsweise, ist nur mit ausdrücklicher Genehmigung der Internet XS Service GmbH gestattet.