

KB 15765: OVPNIP8

IP-Tunnel mit OpenVPN einrichten auf MikroTik RouterOS (Konfiguration als IP-Client zur Integration in ein bestehendes LAN)

 Stand
 25.10.2024, 15:09:22

 Version
 671b9882

 Referenz-URL
 https://www.internet-xs.de/kb/15765

 PDF-URL
 https://www.internet-xs.de/kb/Internet-XS_KB-15765-671b9882.pdf

Vorwort	4
Voraussetzungen	4
Router mit dem Netzwerk verbinden	4
WinBox mit dem Router verbinden	4
Firmware-Update durchführen	5
Administrator-Passwort vergeben	6
Nicht benötigte Dienste deaktivieren	6
DHCP-Server deaktivieren	7
FastTrack deaktivieren	7
LAN konfigurieren	8
Standard-Route erstellen	8
DNS-Server einstellen	9
Prüfen der Internet-Verbindung	10
NTP-Server und Zeitzone einstellen	10
OpenVPN-Client hinzufügen	11
Weitere Routen hinzufügen	12
Interface der Liste WAN zuordnen	13
Port-Weiterleitungen / DNAT einrichten	14
Standard-Gateway auf den Zielen von Port-Weiterleitungen umstellen	16
Port-Weiterleitungen testen	16
Optional: Remote-Zugriff auf den Router per Winbox oder Web-Oberfläche	16
Optional: Source-NAT (SNAT) bspw. für Port-Weiterleitungen zum Standard-Gateway	18
Zu erwartender Durchsatz	19
Backup erstellen	19
Konfiguration als Script	19

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.

Vorwort

Mittels dieser Anleitung kann der Tunnel-Zugang mit fester IP-Adresse auf einem MikroTik RouterOS 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.

Die Konfiguration des Routers erfolgt als IP-Client, d.h. der Router verliert seine Routing-Funktion und erhält stattdessen eine LAN-IP-Adresse aus dem Netzwerk eines vorhandenen Internet-Routers. Diese Konfigurationsvariante eignet sich optimal zur einfachen Integration in ein bestehendes Netzwerk.

Voraussetzungen

- Test-Zugang oder bezahlter Zugang auf dem Server OVPNIP8
- MikroTik Router (getestet mit MikroTik RB750Gr3)
- RouterOS Version 6.49.8 (Long Term) bis 6.99.99
- MikroTik Standardkonfiguration ("default configuration")
- WinBox Konfigurationssoftware (https://mt.lv/winbox64)
- Netzwerk mit einem Internet-Router (z.B. FRITZ!Box, Speedport, Gigacube ...)

Diese Anleitung nimmt an, dass die LAN-IP-Adresse des bestehenden Internet-Routers <u>192.168.178.1</u> lautet, und dass die LAN-IP-Adresse <u>192.168.178.254</u> aus diesem Netzwerk unbelegt ist. Diese Angaben müssen Sie an Ihr LAN anpassen.

Router mit dem Netzwerk verbinden

Verbinden Sie den MikroTik-Router mit dem ersten **LAN-Port** (MikroTik RB750Gr3: **Port 2**) mit dem Netzwerk oder direkt mit einem Konfigurations-PC.

WinBox mit dem Router verbinden

Für die Konfiguration wird eine Software namens WinBox eingesetzt, die vom Hersteller des Routers bereitgestellt wird. Mittels Wine kann die Software auch problemlos unter Linux oder mac OS ausgeführt werden.

- 1. Laden Sie die WinBox-Software beim Hersteller herunter: https://mt.lv/winbox64
- 2. Öffnen Sie die WinBox-Software.
- 3. Falls ein Windows-Sicherheitshinweis der Windows Defender Firewall angezeigt wird, erlauben Sie die Kommunikation.
- 4. Klicken Sie auf den Reiter **Neighbors**. Nach wenigen Sekunden sollte in der Liste der zu konfigurierende Router erscheinen.
- 5. Klicken Sie in der Spalte **MAC Address** auf die MAC-Adresse des zu konfigurierenden Routers. Daraufhin wird im Feld **Connect To:** die gewählte MAC-Adresse eingetragen.
- Geben Sie als Login: (d.h. Benutzernamen) den Standard-Benutzernamen admin ein und lassen Sie das Feld Password: leer.
- 7. Klicken Sie auf Connect.
- Bei der ersten Verbindung sollte ein Hinweis angezeigt werden, dass auf dem Gerät die default configuration angewendet wurde. Diesen Hinweis können Sie mit OK schließen.

Firmware-Update durchführen

Laden Sie die aktuelle, für die Prozessorarchitektur des Routers passende Firmware bei MikroTik herunter.

https://mikrotik.com/download

- Spalte: Long-term
- Zeile: Main package
- RB750Gr3: MMIPS: https://download.mikrotik.com/routeros/6.49.8/routeros-mmips-6.49.8.npk
- RB4011iGS+RM: ARM (32 bit): https://download.mikrotik.com/routeros/6.49.8/routeros-arm-6.49.8.npk
- 1. Navigieren Sie zu **Files**
- 2. Klicken Sie auf Upload...
- 3. Suchen Sie die zuvor heruntergeladene Datei auf Ihrem Computer
- 4. Der Upload dauert einige Sekunden.
- 5. Achten Sie darauf, dass sich die Datei im obersten Verzeichnis befindet bei Routern mit **flash**-Verzeichnis auf einer Ebene mit dem **flash**-Verzeichnis, **nicht im flash-Verzeichnis**.

File List				×
🗕 🍸 🖹 🔒 Bac	kup Restore U	lpload		Find
File Name	∠ Type	Size		Creation Time
📴 flash	disk			Jun/09/2021 12:09:32
lash/pub	directory			Jan/02/1970 01:20:18
📔 flash/skins	directory			Jan/01/1970 01:00:08
💗 routeros-mmips-6.48.5.npk	package		10.0 MiB	Nov/03/2021 17:52:24
		Ŀ	20	
4 items (1 selected)	11.3 MiB of 16.3 MiB	used	30	% free

Wenn der Upload abgeschlossen ist, muss der Router neu gestartet werden.

- 1. Navigieren Sie zu System > Reboot
- 2. Bestätigen Sie mit OK

Der Router erkennt automatisch, dass sich im obersten Verzeichnis eine neue Firmware-Version befindet und installiert die Firmware. Das Update kann mehrere Minuten dauern. Der Router sollte in diesem Zeitraum nicht vom Stromnetz getrennt werden.

Klicken Sie nach entsprechender Wartezeit auf **Reconnect**. Sie können die installierte Firmware-Version im Fenstertitel von WinBox ablesen (z.B. WinBox (64bit) **6.49.8** on hEX (mmips))

Administrator-Passwort vergeben

- 1. Navigieren Sie zu System > Users
- 2. Doppelklicken Sie die Zeile mit dem Namen admin
- 3. Klicken Sie rechts auf Password...
- 4. Vergeben Sie ein neues, sicheres Passwort
- 5. Klicken Sie auf \mathbf{OK}
- 6. Schließen Sie alle weiteren, noch geöffneten Fenster.

User List		
Users Groups SSH Keys SSH Private	Keys Active Users	
		Find
Name / Group Allowed Address	Last Logged In	Comment
admin full	Jan/02/1970 00:17:05	5 system default user
	User <admin></admin>	
	Name: admin	ок
	Group: full	Cancel
	Allowed Address:	Apply
	Last Logged In: Jan/02/1970 00:17	:05
	Change Password	× Disable
	New Password:	Comment
	Confirm Password:	Сору
	Apply	Remove
	7450	Password
	enabled	
1 item (1 selected)		

Nicht benötigte Dienste deaktivieren

- 1. Navigieren Sie zu IP > Services
- Deaktivieren Sie diese Dienste durch klick auf die Zeile und anschlie
 ßendes Klicken auf das rote "X"-Symbol:
- api
- api-ssl
- ftp
- ssh
- telnet

IP S	IP Service List								
 Image: A start of the start of									
	Name 🗠	Port	Available From	Certificate	TLS Ver				
X	🛛 api	8728							
X	api-ssl	8729		none	any				
X	● ftp	21							
X	ssh	22							
X	telnet	23							
	winbox	8291							
	www	80							
X	www-ssl	443		none	any				
					Ş				
8 ite	ems								

DHCP-Server deaktivieren

Im Rahmen der Standard-Konfiguration wird ein DHCP-Server auf dem Router aktiviert. Da sich der MikroTik-Router im selben Netzwerk wie Ihr Internet-Router befinden soll, sollte der DHCP-Server deaktiviert werden (in jedem Netzwerk darf nur einen DHCP-Server IP-Adressen vergeben, um Konflikte zu vermeiden):

- 1. Navigieren Sie zu IP > DHCP Server
- 2. Klicken Sie einmal auf die Zeile mit dem Namen defconf
- 3. Klicken Sie auf das rote "-"-Symbol zum löschen
- 4. Der Eintrag sollte aus der Liste verschwunden sein
- 5. Wählen Sie den Reiter Networks
- 6. Klicke Sie einmal auf die Zeile mit der Address 192.168.88.0/24
- 7. Klicken Sie auf das rote "X"-Symbol zum deaktivieren
- 8. Schließen Sie das Fenster DHCP Server.

FastTrack deaktivieren

FastTrack ist eine Funktion von MikroTik-Routern, mit der die Last auf dem Router reduziert werden kann. Die positiven Auswirkungen sind beim gegebenen Anwendungsfall jedoch nicht messbar, dafür kann FastTrack bei VPN und Verschlüsselung nicht reproduzierbare Nebeneffekte nach sich ziehen. Deshalb sollte FastTrack deaktiviert werden.

- 1. Navigieren Sie zu IP > Firewall > Reiter Filter Rules
- 2. Markieren Sie die Zeile mit der Action "fasttrack connection" durch anklicken
- 3. Klicken Sie oben auf das rote "X"-Symbol zum deaktivieren der Regel.
- 4. Schließen Sie das Fenster Firewall.

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer 7 Process 	Firew	all										
Image: Construction of the section	Filte	r Rul	es	NAT	Mangle	Raw	Service P	orts	Connectio	ons Add	ress Li	ists Layer7 Protocol
# Action Chain Src. Address Dst. Address Protocol 0 D passthrough forward 1 ✓ accept input 2 X drop input 1 (icmp) 3 ✓ accept input 127.0.0.1 5 X drop input 127.0.0.1 6 ✓ accept forward 1 7 ✓ accept forward 1 9 ✓ accept forward 1 10 X drop forward 1	÷	-	2	×	0	7 0	Reset Cou	inters	(O Res	et All Cour	nters	INTERNETXS
0 D passthrough forward 1 Imput input input 2 Imput input 1 (icmp) 3 Imput Imput 1 (icmp) 4 Imput Imput 1 (icmp) 5 Imput Imput 127.0.0.1 5 Imput Imput Imput 6 Imput Imput Imput 7 Imput Imput Imput 8 Imput Imput Imput 9 Imput Imput Imput 10 Imput Imput Imput 11 Imput Imput Imput	#		Actio	on	5		Chain	Src	. Address	Dst. Add	ress	Protocol
1 ✓ accept input 2 X drop input 1 (icmp) 3 ✓ accept input 127.0.0.1 4 ✓ accept input 127.0.0.1 5 X drop input 1 6 ✓ accept forward 1 7 ✓ accept forward 1 9 ✓ accept forward 1 9 ✓ accept forward 1 10 X drop forward 1	0	D	P	bassthro	ough		forward					
2 X drop input 1 (icmp) 3 ✓ accept input 127.0.0.1 4 ✓ accept input 127.0.0.1 5 X drop input 1 6 ✓ accept forward 1 7 ✓ accept forward 1 8 X Input 1 9 ✓ accept forward 1 10 X drop forward 1	1		🔶 a	accept			input					
3 Imput 1 (icmp) 4 Imput 127.0.0.1 5 Imput 127.0.0.1 6 Imput Imput 7 Imput Imput 8 Imput Imput 9 Imput Imput 10 Imput Imput	2		* d	drop			input					
4 ✓ accept input 127.0.0.1 5 ¥ drop input 6 ✓ accept forward 7 ✓ accept forward 8 X Image: Accept forward 9 ✓ accept forward 10 ¥ drop 11 Image: Accept forward	3		💙 a	accept			input					1 (icmp)
5 X drop input 6 Implementation of accept forward 7 Implementation of accept Implementation of accept 8 X Implementation of accept Implementation of accept 9 Implementation of accept Implementation of accept 10 X drop Implementation of accept	4		🔶 a	accept			input			127.0.0.1	1	
6 ✓ accept forward 7 ✓ accept forward 8 X forward 9 ✓ accept forward 10 # drop	5		X d	lrop			input					
7 ✓ accept forward 8 X > fasttrack connection forward 9 ✓ accept forward 10 X drop forward	6		💙 a	accept			forward					
8 X Image: Second sec	7		💙 a	accept			forward					
9 ✓ accept forward 10 X drop forward 11 M drop forward	8	Х	₩ fi	asttrac	k connect	ion	forward			1		
10 X drop forward	9		💙 a	accept			forward					
11 🔲 dana Ganuard	10		* d	lrop			forward					
rorward	11		* d	drop			forward					

LAN konfigurieren

- 1. Navigieren Sie zu IP > Addresses
- 2. Doppelklicken Sie die Zeile mit der **Address** 192.168.88.1/24 (192.168.88.1 ist die im Rahmen der Standardkonfiguration des Herstellers eingestellte LAN-IP-Adresse des Routers)
- Address: Geben Sie hier eine freie LAN-IP-Adresse aus Ihrem bestehenden Netzwerk ein, z.B. 192.168.178.254/24 (der MikroTik-Router erhält damit die LAN-IP-Adresse 192.168.178.254)
- 4. Network: Geben Sie hier die Netzadresse Ihres LAN ein i.d.R. 192.168.xxx.0, z.B. 192.168.178.0

Add	ress List						×
÷	- 🗸 🗶 🍸					Fin	
	Address	Network	Interface	Comment		1011300131 X	-
	÷ 192.168.88.1/24	192.168.88.0	bridge	defconf			
		Address <192.16 Address: 192.1 Network: 192.1 Interface: bridge	8.88.1/24> 168.178.254/24 168.178.0 2 e	1 OF Cano Total Disa	Del		
1 1 () 2	= Eine freie LAN-IP-Adress 92.168.178.254) gefolgt vo 255.255.255.0 = /24) = Netz-Adresse des besteh	se aus dem beste on der Anzahl de nenden LAN - i.d	ehenden LAN (z. r 1-Bits der Subr .R. 192.168.xxx	.B. netzmaske des LAN 0	y y ve		
1 ite	em (1 selected)	enabled					

Standard-Route erstellen

Für die Kommunikation mit dem Internet wird eine sog. Standard-Route benötigt.

- 1. Navigieren Sie zu IP > Routes (nicht Routing!)
- 2. Klicken Sie auf das blaue "+"-Zeichen zum hinzufügen eines neuen Eintrags
- 3. Klicken Sie in das Feld **Gateway** und geben Sie dort die **LAN-IP-Adresse Ihres Internet-Routers** ein, bspw. **192.168.178.1**

- 4. **Dinstance**: 10
- 5. Klicken Sie auf OK

Nach kurzer Zeit sollte in der neuen Zeile mit dem Flag **AS** (Spalte ganz links) in der Spalte **Gateway** neben der LAN-IP-Adresse des Internet-Routers das Wort **reachable** und **bridge** angezeigt werden.

Route <0.0.0/0>	,			
General Attribu	tes			ок
Dst. Address:	0.0.0.0/0			Cancel
Gateway:	192.168.178.1	Setzen Sie hier die LAN-IP-Adresse I Internet-Routers ein (z.B. 192.168.17	8.1). ♦	Apply
Check Gateway:				Disable
Туре:	unicast		Ŧ	Comment
Distance:	10			Сору
Scope:	30			Remove
Target Scope:	10			
Routing Mark:			•	
Pref. Source:			~	Ν
				<i>μ</i> ζ ⁴
enabled		active	static	

DNS-Server einstellen

- 1. Navigieren Sie zu IP > DNS
- Geben Sie im Feld Servers mindestens einen DNS-Server ein. I.d.R. bietet sich hier die LAN-IP-Adresse des Internet-Routers (bspw. 192.168.178.1) an. Alternativ kann auch bspw. Google DNS (8.8.8.8) oder Cloudflare DNS (1.1.1.1) oder Quad9 (9.9.9.9) verwendet werden.

DNS Settings			
Servers:	192.168.178.1	\$	ок
Dynamic Servers:			Cancel
Use DoH Server:		-	Apply
	Verify DoH Certificate		Static
	✓ Allow Remote Requests		Cache
Max UDP Packet Size:	4096		
Query Server Timeout:	2.000	s	
Query Total Timeout:	10.000	S	
Max. Concurrent Queries:	100		
Max. Concurrent TCP Sessions:	20		
Cache Size:	2048	КiВ	
Cache Max TTL:	7d 00:00:00		
Cache Used:	29 KiB		

Prüfen der Internet-Verbindung

- 1. Navigieren Sie zu Tools > Ping
- 2. Geben Sie im Feld **Ping To** diese IP-Adresse ein: 212.58.69.24 (setzen Sie hier **nicht** die Ihrem IP-Tunnel zugeteilte feste, öffentliche IPv4-Adresse ein!)
- 3. Klicken Sie auf Start.
- 4. Warten Sie 5-10 Sekunden
- 5. Klicken Sie auf Stop.
- 6. Wenn eine Ausgabe ähnlich der unten stehenden angezeigt wird, besteht eine funktionsfähige Internet-Verbindung:

Ping General Pir Inte Packet (Tir	I Ad ng To erface Coun meour	dvanced : 212.58.69. : ARP Ping t: t: 1000					▼	Start Stop Close New Window
See # /	Heat		Time	Peoply Size	тті	Status		
0	212	58.69	1ms	50 Theply 512e	63	Jidius		
1	212	58.69	Oms	50	63			
2	212	58.69	Oms	50	63			
3	212	58.69	Oms	50	63			
4	212	58.69.	Oms	50	63			
5 items		5 of 5 packets received	0% pack	et loss	Min: (0 ms	Avg: 0 ms	Max: 1 ms

NTP-Server und Zeitzone einstellen

- 1. Navigieren Sie zu System > SNTP Client
- 2. Enabled: Aktiviert
- 3. Server DNS Names: de.pool.ntp.org
- 4. Klicken Sie auf **Apply**

Nach einem Augenblick sollte im Feld **Active Server** eine IP-Adresse angezeigt werden. Nach einigen Sekunden sollte im Feld **Last Update** eine Zeit wie z.B. *00:00:17 ago* angezeigt werden.

SNTP Client		
	✓ Enabled	ок
Mode:	unicast	Cancel
Primary NTP Server:	0.0.0.0	Apply
Secondary NTP Server:	0.0.0.0	2
Server DNS Names:	de.pool.ntp.org	
Dynamic Servers:		
Poll Interval:	256 s	
Active Server:	80.151.186.5	
Last Update From:	80.151.186.5	
Last Update:	00:00:10 ago	
Last Adjustment:	136 us	
Last Bad Packet From:		
Last Bad Packet:		
Last Bad Packet Reason:		

Zum einstellen der Zeitzone:

- 1. Navigieren Sie zu System > Clock
- 2. Time Zone Name: Europe/Berlin
- 3. Klicken Sie auf OK

Nach Abschluss der Einstellungen können Sie die Fenster Clock und SNTP Client schließen.

OpenVPN-Client hinzufügen

- 1. Navigieren Sie zu Interfaces
- 2. Klicken Sie unter dem Reiter Interface auf das blaue "+"-Symbol.
- 3. Wählen Sie OVPN Client aus der Liste
- 4. Name: ovpn-out1-ixs-ovpnip
- 5. Wechseln Sie in den Reiter Dial Out
- 6. Connect To: 212.58.69.24 (setzen Sie hier nicht die feste IP-Adresse Ihres IP-Tunnel-Zugangs ein!)
- 7. **User**: ixs024-1234-a1b2c3d4 (setzen Sie hier den **Benutzernamen** zu Ihrem IP-Tunnel-Zugang ein, den Sie von uns erhalten haben)
- 8. **Password**: XXXXXXXX (setzen Sie hier das **Passwort** zu Ihrem IP-Tunnel-Zugang ein, das Sie von uns erhalten haben)
- 9. Auth.: null
- 10. Cipher: null
- 11. Use Peer DNS: no
- 12. Add Default Route: Deaktiviert
- 13. Klicken Sie auf Apply
- 14. Nach wenigen Augenblicken sollte der Status (unten rechts) auf connected wechseln.

Interface <ovpn-c< th=""><th>out 14</th><th>ixs-ovpnip</th><th>></th><th></th><th></th></ovpn-c<>	out 14	ixs-ovpnip	>		
General Dial	Dut	Status	Setzen Sie hier d des OVPNIP-Se dem sich Ihr Zug	ie IP-Adresse rvers ein, auf ang befindet	
Connect To:	212	.58.69.1	Setzen Sie hier N	NICHT die IP-	Cancel
Port:	119	4	Adresse Ihres Zugangs	IP-Tunnel- ein!.	Apply
Mode:	ip			,	Disable
User:	ixs0				Comment
Password:				^	Сору
Profile:	defa	ault		•	Remove
Certificate:	non	е		₹	Torch
	<u> </u>	/erify Serv	er Certificate		
Auth.:	null			₹	
Cipher:	null			₹	
Use Peer DNS:	no			₹	6
	A	Add Defau	lt Route		
enabled			running	slave	Status: connected

Weitere Routen hinzufügen

Damit ausgehender Traffic inkl. Antwort-Pakete auf eingehende Anfragen (wie bspw. Port-Weiterleitungen / DNAT) über die feste, öffentliche IPv4-Adresse transportiert werden, müssen zwei weitere Routen hinzugefügt werden. Auf anderen Betriebssystemen wie bspw. Windows oder Linux werden diese Routen automatisch beim Aufbau der IP-Tunnel-Verbindung hinzugefügt. Auf MikroTik RouterOS ist die dafür benötigte Funktion jedoch leider nicht implementiert, weshalb die Routen manuell hinzugefügt werden müssen.

Die erste Route sorgt dafür, dass der getunnelte Traffic über den Internet-Router zum IP-Tunnel-Server gesendet wird.

- 1. Navigieren Sie zu IP > Routes
- 2. Klicken Sie auf das blaue "+"-Symbol
- 3. **Dst. Address**: 212.58.69.24 (IP-Adresse des Servers, auf dem sich Ihr IP-Tunnel-Zugang befindet. Setzen Sie hier nicht die IP-Adresse Ihres IP-Tunnel-Zugangs ein!)
- 4. Gateway: LAN-IP-Adresse Ihres Internet-Routers, bspw. 192.168.178.1
- 5. Distance: 1
- 6. Klicken Sie auf OK

Route <212.58.69	. >			
General Attribu	ites II	P-Adresse des OVPNIP-Servers (z.B. 212.58.69.9). Setzen Sie hier NICHT IP-Adresse Ihres IP-Tunnel-Zugangs ein.	die	OK KA
Dst. Address:	212.58.69.			Cancel
Gateway:	192.168.178.10	Setzen Sie hier die LAN-IP-Adresse Ihres Internet-Routers ein (z.B. 192.168.178.1).	\$	Apply
Check Gateway:			•	Disable
Туре:	unicast		Ŧ	Comment
Distance:	1		•	Сору
Scope:	30			Remove
Target Scope:	10			
Routing Mark:			•	
Pref. Source:			•	\square
enabled		active static		

Die zweite Route sorgt dafür, dass jeglicher Internet-Traffic zum virtuellen Netzwerk-Interface des IP-Tunnel-Zugangs gesendet wird.

1. Navigieren Sie zu IP > Routes

2. Klicken Sie auf das blaue "+"-Symbol

- 3. Dst. Address: 0.0.0.0/0
- 4. Gateway: Wählen Sie ovpn-out1-ixs-ovpnip aus der Liste der Gateways aus
- 5. Distance: 5
- 6. Klicken Sie auf OK

Route <0.0.0.0/0>								
General Attributes				ок				
Dst. Address: 0.0.0.0/0				Cancel				
Gateway: ovpn-out1-ixs-ov	vpnip 두 read	chable	\$	Apply				
Check Gateway:				Disable				
Type: unicast	Type: unicast							
Distance: 5			▲	Сору				
Scope: 30				Remove				
Target Scope: 10								
Routing Mark:			•					
Pref. Source:			₹	B				
enabled		active	static					

Interface der Liste WAN zuordnen

Das im Rahmen der Konfiguration des OpenVPN-Clients erstellte virtuelle Netzwerkinterface sollte noch der Interface Liste **WAN** zugeordnet werden, damit die richtigen Firewall-Regeln auf das Interface angewendet werden.

- 1. Navigieren Sie zu Interfaces > Reiter Interface List
- 2. Klicken Sie auf das blaue "+"-Symbol

- 3. List: WAN
- 4. Interface: ovpn-out1-ixs
- 5. Klicken Sie auf **OK**

Interface Lis	st										
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN VRRP	Bonding LTE				
+ -	<pre></pre>	7	ists		Interface List Member <wan ovpn-out1-ixs-ovpnip=""></wan>						
List		∆ Int	terface		Comment	List: WA	N	Ŧ	ОК		
LAN	LAN bridge			defconf							
WAN		et	ther1		defconf	Interface: ovpr	nterface: ovpn-out1-ixs-ovpnip 🗧				
WAN	N ovpn-out 1-ixs-ovpnip					<u> </u>					
									Apply		
									Disable		
							Comment				
									Сору		
									Remove		
						enabled					
3 items	3 items										

Port-Weiterleitungen / DNAT einrichten

- 1. Navigieren Sie zu IP > Firewall > Reiter NAT
- 2. Klicken Sie auf das blaue "+"-Symbol zum hinzufügen einer neuen Regel
- 3. Wechseln Sie zum Reiter General
- 4. Chain: dstnat
- 5. Protocol: z.B. 6 (tcp) oder 17 (udp)
- 6. Dst. Port: Tragen Sie hier den gewünschten eingehenden Port ein. Dieser Port kann vom To Ports (siehe unten) abweichend definiert werden, sollte aber wenn möglich gleich sein wie der To Ports. Der Dst. Port darf nur einmal pro Protokoll (TCP/UDP) vergeben werden. Falls Sie bspw. zwei IP-Kameras erreichbar machen möchten, die beide intern (= To Ports) den Port 80 verwenden, muss als Dst. Port bspw. für die erste Kamera 80/TCP und für die zweite Kamera bspw. 81/TCP angegeben werden.
- 7. In. Interface List: WAN
- 8. Wechseln Sie zum Reiter Action
- 9. Action: dst-nat
- 10. **To Addresses**: Geben Sie hier die Ziel-LAN-IP-Adresse ein, zu der dieser Port weitergeleitet werden soll, also bspw. eine IP-Kamera, Datenlogger, NAS, Server ...
- To Ports: Geben Sie hier den Port ein, auf dem das Gerät mit der zuvor festgelegten Ziel-LAN-IP-Adresse (also bspw. eine IP-Kamera, Datenlogger, NAS, Server …) einen Dienst bereitstellt, z.B. 80 für HTTP, 443 für HTTPS usw.
- 12. Klicken Sie auf OK

NAT Rule <80>	
General Advanced Extra Action Statistics	OK SHE
Chain: dstnat	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Protocol: 6 (tcp) ∓ 🔺	Comment
Src. Port:	Conv
Dst. Port: 80	Remove
Any. Port:	Reset Counters
In. Interface:	Reset All Counters
Out. Interface:	Heset Air Counters
In. Interface List: WAN 🗧 🔺	
Out. Interface List:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Routing Table:	
Connection Type:	
enabled	
NAT Rule <80>	
NAT Rule <80> General Advanced Extra Action Statistics	
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat The state of the	OK Cancel
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Log	OK Cancel Apply
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log	Cancel Disable
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log Log ▼ To Addresses: 192.168.178.20 ▲	Cancel Disable Comment
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Image: Constraint of the state	Cancel Cancel Disable Comment Copy
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Image: Constraint of the state	Cancel Cancel Disable Comment Copy Remove
NAT Rule <80> General Advanced Extra Action: dst-nat Image: Deg Defix: To Addresses: 192.168.178.20 To Ports: 80	OK Cancel Apply Disable Comment Copy Remove Reset Counters
NAT Rule <80> General Advanced Extra Action: dst-nat Image: Constraint of the second se	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log Log Log Prefix: ▼ To Addresses: 192.168.178.20 ▲ To Ports: 80 ▲	OK OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log Log Log Prefix: ▼ To Addresses: 192.168.178.20 ▲ To Ports: 80	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat ▼ Log Log ▼ To Addresses: 192.168.178.20 ▲ To Ports: 80 ▲	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Image: Constraint of the state	Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Log Log Prefix: To Addresses: 192.168.178.20 To Ports: 80	Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Image: Constraint of the state	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters
NAT Rule <80> General Advanced Extra Action Statistics Action: dst-nat Image: Constraint of the second seco	OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Diese Schritte sind für alle gewünschten Port-Weiterleitungen zu wiederholen. Der Übersichtlichkeit halber sollte die Standard *masquerade*-Regel immer ganz unten stehen. Sie können die Regeln mit Drag & Drop verschieben.

Häufig verwendete Ports:

- HTTP: 80/TCP
- HTTPS: 443/TCP
- HTTP alternativ: 8080/TCP
- HTTPS alternativ: 8443/TCP
- SMTP (Mail-Server): 25/TCP
- Remote-Desktop-Verbindung: 3389/TCP und 3389/UDP (es sind zwei Regeln notwendig, eine für TCP und eine für UDP)
- RTSP (häufig für IP-Kameras benötigt): 554/UDP

Standard-Gateway auf den Zielen von Port-Weiterleitungen umstellen

Auf allen LAN-Geräten, die Ziel einer Port-Weiterleitung sind (d.h. deren LAN-IP-Adresse in einem **To Addresses**-Feld einer NAT-Regel steht), muss das so genannte *Standard-Gateway* oder *Default Gateway* oder *Default Route* auf die LAN-IP-Adresse des MikroTik-Routers umgestellt werden (bspw. **192.168.178.254**. Wie das genau funktioniert ist von Hersteller zu Hersteller und Gerät zu Gerät unterschiedlich. Bitte konsultieren Sie dafür die Bedienungsanleitung des Geräts. Häufig sind diese Einstellungen im Bereich der Netzwerk- oder LAN-Konfiguration zu finden und erfordern die Verwendung einer *Statischen* oder *Static* LAN-Konfiguration, **nicht** *Dynamic* oder *DHCP*.

Dieser Schritt ist unbedingt erforderlich. So lange das Standard-Gateway der IP-Kamera / Datenlogger / NVR / Server / NAS nicht auf die LAN-IP-Adresse des MikroTik-Routers umgestellt wurde, funktionieren die Port-Weiterleitungen nicht!

Port-Weiterleitungen testen

Testen Sie Port-Weiterleitungen immer aus dem Internet, d.h. nicht aus dem Iokalen Netzwerk. Verwenden Sie dafür bspw. ein Smartphone, das ins LTE-Netz eingebucht ist.

Sie erreichen nach Abschluss der Konfiguration die festgelegten Ports nach diesem Schema aus dem Internet:

- http://(lhre.feste.IP):(Dst. Port) -> (To Addresses):(To Ports)
- http://212.58.88.256:80 -> 192.168.178.20:80
- http://212.58.88.256:81 -> 192.168.178.21:80
- http://212.58.88.256:12345 -> 192.168.178.21:12345

Optional: Remote-Zugriff auf den Router per Winbox oder Web-Oberfläche

Achtung: Die Einschränkung auf eine feste Absender-IP-Adresse wird dringend empfohlen. Falls die Einschränkung auf eine feste Absender-IP-Adresse nicht möglich ist, sollten zumindest die Standard-Ports der Dienste unter **IP** > **Services** geändert werden.

- 1. Navigieren Sie zu IP > Firewall > Reiter Filter Rules
- 2. Klicken Sie auf das blaue +-Symbol
- 3. Chain: input
- 4. Src. Address: Eine feste IPv4-Adresse, z.B. von einem Büro-Internet-Anschluss. Diese Einstellung ist optional, wird jedoch empfohlen.
- 5. Protocol: 6 (tcp)
- 6. Dst. Port: Port, der erreichbar gemacht werden soll (z.B. 8291 für Winbox)
- 7. In. Interface List: WAN
- 8. Klicken Sie auf OK
- 9. Im Fenster Firewall erscheint die neu angelegte Regel nun ganz unten.
- 10. Schieben Sie die Regel per Drag & Drop **über** die "drop input"-Regel. Die "drop input"-Regel sollte immer die letzte Regel im "input"-Chain sein.

Firewall Rule <84.122.32.143->8291>	
General Advanced Extra Action Statistics	
Chain: input	Cancel
Src. Address: 84.122.	Apply
Dst. Address:	Disable
Protocol: 6 (tcp)	Comment
Src. Port:	Сору
Any Port:	Remove
In. Interface:	Reset Counters
Out. Interface:	Reset All Counters
In. Interface List: WAN	
Out. Interface List:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Routing Table:	
Connection Type:	
Connection State:	
Connection NAT State:	
enabled	

Firewall												٦×
Filter Rule	es NAT Mangle Raw	Service Ports	Conne	ections Addr	ess Lists	Layer7 Proto	cols				Ţ	鞋
+ -	X	Reset Counter	rs (O F	Reset All Count	ters				[Find	all	TXS ₹
#	Action	Chain S	Src. Ad	Dst. Address	Protocol		Src. Port	Dst. Port	In. Inter	Out. Int	In. Inter	0
0 D	🗅 passthrough	forward										
1	🔶 accept	input										
2	🗱 drop	input										
3	🔶 accept	input			1 (icmp)							
4	< accept	input		127.0.0.1								
5	✓ accept	input 8	4.122		6 (tcp)			8291			WAN	
6	😫 drop	input									!LAN	
7	🔶 accept	forward	-									
8	✓ accept	forward										
9	fasttrack connection	forward										
10	✓ accept	forward										
11	X drop	forward										
12	🗱 drop	forward									WAN	
Alle Regeln im "input" Chain			Die	e Standard-D st die letzte "input" Cl	Prop-Reg Regel im hain	el	Die bef Sta	neu erste indet sicl andard-Dr	llte Regel i über der op-Regel			
•												•
13 items (1 selected)											

Optional: Source-NAT (SNAT) bspw. für Port-Weiterleitungen zum Standard-Gateway

Wenn auf einen Port-Weiterleitungs-Ziel / DNAT-Ziel das Standard-Gateway nicht geändert werden kann (z.B. weil es sich um den Internet-Router handelt oder das Ziel-System per Firewall Zugriffe von externen IP-Adressen ausschließt), ist eine so genannte Source-NAT / SNAT-Regel erforderlich, die die Absender-IP-Adresse in eingehenden, per DNAT weitergeleiteten Paketen durch die LAN-IP-Adresse des MikroTik-Routers ersetzt.

Bitte beachten Sie, dass dadurch die reale Absender-IP-Adresse der eingehenden Datenpakete verschleiert wird. Dadurch können Sicherheitsmechanismen der Ziel-Systeme außer Funktion gesetzt werden.

- 1. Navigieren Sie zu IP > Firewall > Reiter NAT
- 2. Klicken Sie auf das blaue "+"-Symbol
- 3. Wählen Sie den Reiter **General**
- 4. Chain: srcnat
- 5. Dst. Address: Geben Sie hier die interne IP-Adresse des Port-Weiterleitungs-Ziels / DNAT-Ziels ein, bspw. 192.168.178.1
- 6. Sie können bei Bedarf die Regel weiter Einschränken, z.B. per Protocol und Dst. Port
- 7. Wählen Sie den Reiter Action
- 8. Action: src-nat
- 9. **To Addresses**: Geben Sie hier die interne IP-Adresse des MikroTik-Routers ein, bspw. 192.168.178.254
- 10. Klicken Sie auf OK
- 11. Platzieren Sie die Regel per Drag & Drop ganz oben im Chain srcnat

Zu erwartender Durchsatz

Unter Laborbedingungen kann mit einem MikroTik RB750Gr3 dieser Durchsatz erzielt werden:

- Download: Max. 107,64 Mbit/s
- Upload: Max. 97,51 Mbit/s

Der Durchsatz wird durch die Prozessorleistung des Geräts begrenzt.

×

https://www.speedtest.net/result/12277359651

Backup erstellen

Nach erfolgreicher Konfiguration sollte ein Backup erstellt werden. Bitte beachten Sie, dass die Wiederherstellung des Backups nur auf demselben Gerät mit derselben Firmware-Version möglich ist.

- 1. Navigieren Sie zu Files
- 2. Klicken Sie auf Backup
- 3. Name: Vergeben Sie einen Dateinamen, z.B. mein-backup
- 4. Password: Versehen Sie das Backup mit einem Passwort
- 5. Encryption: aes-sha256
- 6. Don't Encrypt: Deaktiviert
- 7. Klicken Sie auf **Backup**
- 8. Nach einigen Sekunden befindet sich im Speicher des Geräts eine Backup-Datei mit dem Namen mein-backup.backup
- 9. Klicken Sie mit der rechten Maustaste auf das Backup und wählen Sie **Download**, um die Datei vom Router herunterzuladen.
- 10. Falls im Dateisystem ein Verzeichnis mit dem Namen flash vorhanden ist und Sie das Backup auf dem Router liegen lassen möchten, schieben Sie das Backup in den Ordner flash. Dateien, die außerhalb des flash-Verzeichnisses liegen, werden bei einem Router-Neustart gelöscht. Geräte, die kein flash-Verzeichnis haben, behalten alle Dateien im Dateisystem auch bei einem Router-Neustart im Speicher.

Konfiguration als Script

Alle hier dargestellten Schritte können auch mittels eines Konfigurations-Scripts durchgeführt werden.

- Kopieren Sie das unten stehende Konfigurations-Script in einen Texteditor wie bspw. Notepad oder Notepad++ (nicht Word oder WordPad)
- 2. Passen Sie die Variablen an Ihre Wünsche und Ihr Netzwerk an
- 3. Verbinden Sie sich mit der WinBox-Software mit dem MikroTik-Router
- 4. Falls Sie bereits manuelle Einstellungen vorgenommen haben, Setzen Sie den Router zunächst auf Werkseinstellungen zurück:
- 5. Navigieren Sie zu System > Reset Configuration
- 6. Keep User Configuration: Deaktiviert
- 7. CAPS Mode: Deaktiviert
- 8. No Default Configuration: Deaktiviert

- 9. Do Not Backup: Aktiviert
- 10. Run After Reset: leer
- 11. Klicken Sie auf Reset Configuration
- 12. Der Router wird daraufhin neu gestartet und auf Werkseinstellungen mit der vom Hersteller vorgesehenen Standard-Konfiguration zurücksetzt. WinBox verliert in diesem Zuge die Verbindung zum Router. Klicken Sie nach 2-3 Minuten auf **Reconnect**.
- 13. Klicken Sie in der WinBox-Software links auf **New Terminal**. Daraufhin öffnet sich ein Kommandozeilenfenster innerhalb der WinBox-Software.
- 14. Kopieren Sie das gesamte, an Ihr Netzwerk angepasste Konfigurations-Script aus Ihrem Texteditor (inkl. Kommentare, diese werden vom Router ignoriert)
- 15. Klicken Sie mit der rechten Maustaste in das zuvor geöffnete Terminal-Fenster in der WinBox-Software
- 16. Klicken Sie auf Paste

Wenn die im Konfigurations-Script hinterlegten IP-Adressen, Netzwerkangaben und OpenVPN-Zugangsdaten korrekt waren, ist der Router nun - bis auf Ihre individuellen Port-Weiterleitungen, die Sie gemäß der Anleitung vornehmen müssen - fertig konfiguriert.

```
###
#
#
# Bitte passen Sie die nachfolgenden Variablen an Ihr Netzwerk an.
#
#
###
# Administrator-Passwort
:global ixsAdminPassword "meinsicherespasswort"
# Freie LAN-IP-Adresse, die der MikroTik-Router erhalten soll
# (z.B. 192.168.178.254)
:global ixsLanIpAddress "192.168.178.254"
# Netz-Adresse. Endet i.d.R. mit ".0"
# (z.B. 192.168.178.0)
:global ixsLanNetwork "192.168.178.0"
# LAN-IP-Adresse des Internet-Routers (z.B. 192.168.178.1)
:global ixsLanGateway "192.168.178.1"
# LAN-IP-Adresse des DNS-Servers
# (i.d.R. der Internet-Router, z.B. 192.168.178.1)
:global ixsDnsServers "192.168.178.1"
# Anzahl der Bits der LAN-Netzwerkmaske. 255.255.255.0 = 24
:global ixsLanMaskBits "24"
# IP-Adresse des Internet XS OVPNIP Servers
:global ixs0vpnipServerIpAddress "212.58.69.24"
# Port des Internet XS OVPNIP Servers
:global ixsOvpnipServerPort "1194"
# Benutzername Ihres IP-Tunnel-Zugangs auf dem Internet XS OVPNIP Server
```

```
:global ixsOvpnipUsername "ixs024-XXXX-XXXXXXXXXX"
# Passwort zu Ihrem IP-Tunnel-Zugangs auf dem Internet XS OVPNIP Server
###
#
#
# Ab hier keine Änderungen mehr vornehmen
#
#
###
/user set [/user find name=admin] password="$ixsAdminPassword"
/ip service set [/ip service find name=telnet] disabled=yes
/ip service set [/ip service find name=ftp] disabled=yes
/ip service set [/ip service find name=api] disabled=yes
/ip service set [/ip service find name=api-ssl] disabled=yes
/ip service set [/ip service find name=ssh] disabled=yes
/ip dhcp-server disable [/ip dhcp-server find disabled=no]
/ip address set [/ip address find comment=defconf]
address="$ixsLanIpAddress/$ixsLanMaskBits" network="$ixsLanNetwork"
/ip firewall filter disable [/ip firewall filter find action=fasttrack-
connection]
/system ntp client set enabled=yes server-dns-names=de.pool.ntp.org
:if ([/interface find name=ovpn-out1-ixs-ovpnip]) do={ /interface ovpn-client
set [/interface ovpn-client find name=ovpn-outl-ixs-ovpnip] use-peer-dns=no
connect-to="$ixs0vpnipServerIpAddress" port="$ixs0vpnipServerPort" auth=null
cipher=null user="$ixs0vpnipUsername" password="$ixs0vpnipPassword" }
else={/interface ovpn-client add name=ovpn-out1-ixs-ovpnip use-peer-dns=no
connect-to="$ixsOvpnipServerIpAddress" port="$ixsOvpnipServerPort" auth=null
cipher=null user="$ixsOvpnipUsername" password="$ixsOvpnipPassword" }
:if ([/interface list member print count-only where interface=ovpn-out1-ixs-
ovpnip list=WAN] = 0) do={ /interface list member add interface=ovpn-out1-
ixs-ovpnip list=WAN }
:if ([/ip route find dst-address=0.0.0.0/0 distance=10]) do={ /ip route set
[/ip route find dst-address=0.0.0.0/0 distance=10] dst-address=0.0.0.0/0
gateway="$ixsLanGateway" distance=10 } else={ /ip route add dst-
address=0.0.0.0/0 gateway="$ixsLanGateway" distance=10 }
:if ([/ip route print count-only where gateway=ovpn-out1-ixs-ovpnip] = 0)
do={ /ip route add dst-address=0.0.0.0/0 distance=5 gateway=ovpn-out1-ixs-
ovpnip }
:if ([/ip route print count-only where dst-
address="$ixs0vpnipServerIpAddress/32"] = 0) do={ /ip route add dst-
address="$ixs0vpnipServerIpAddress/32" distance=1 gateway="$ixsLanGateway" }
/ip dns set servers="$ixsDnsServers"
# Umgebungsvariablen loeschen
:set ixsAdminPassword
:set ixsLanIpAddress
:set ixsLanNetwork
:set ixsLanGateway
:set ixsLanMaskBits
:set ixs0vpnipServerIpAddress
:set ixsOvpnipServerPort
:set ixs0vpnipUsername
:set ixs0vpnipPassword
```

 $\ensuremath{\mathbb{C}}$ 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.