Hardware

Diese Anleitung wurde aufgrund der vorhandenen Infrastruktur vor Ort erstellt. Konkret ist der Netzzugang hier über ein AON-ADSL-Modem realisiert, das als Gateway 10.0.0.138 fungiert.

Um nunmehr den VPN-Zugang ins Hamnet herzustellen, kam ein Mikrotik mAP-2n zum Einsatz und stellt Hamnet-Zugang sowohl für WLAN als auch LAN bereit. Alternativ sei auf das Mikrotik RouterBoard RB941-2nD um rund 30 EUR hingewiesen (natürlich geht jedes Routerboard für diesen Zweck, in größerem Rahmen zB das RB2011).

Grundsätzlich werden hier die Geräte (Laptops, Desktop, Tablets) über LAN bzw. WLAN an den Mikrotik angebunden und der Mikrotik entscheidet dann über das Routing ins Internet bzw. Hamnet. Dies stellt insoferne kein Problem dar, da das Hamnet den Netzbereich 44.0.0.0/8 exklusive zugewiesen bekommen hat und daher eine Routing-Regel hierfür ausreicht.

Der Mikrotik ist für das Beispiel über ETH1 Richtung AON-Modem/Router angebunden.



Registrierung eines VPN-Zuganges ins Hamnet

Für den VPN-Zugang ins Hamnet gibt es dankenswerterweise mehrere Einstiegspunkte:

DB0FHN – Nürnberg - http://db0fhn.efi.fh-nuernberg.de/doku.php?id=radio:db0fhn

DB0TV – Ennepetal http://www.ruhrlink.org/index.php?option=com_content&task=view&id=139&Itemid=250

DB0SDA – Aachen - https://www.afu.rwth-aachen.de/projekte/hamnet/anwendungen/vpn-zugang

Auf den o.a. Seiten wird auch beschrieben, wie man von einem Rechner aus eine VPN-Verbindung aufbaut. Grundsätzlich natürlich möglich, wir wollen hier nun aber dafür für unser ganzes lokales Netzwerk den Mikrotik verwenden.

Einrichtung VPN-Client

Wir melden uns mit der Winbox bei unserem Mikrotik an und stellen vorerst im QuickSet auf Routermode und aktivieren uns ein WLAN:

WISP AP 🗧 Quick	Set			
– Wireless –		- Configuration		ОК
Wireless Protocol:	€ 802.11 C nstreme C nv2	Mode:	Router C Bridge	Cancel
Network Name:	netz3	- Internet		Apply
Frequency:	2412 F MHz	Address Acquisition:	C Static C Automatic C PPPoE	
Band:	2GHz-B/G ∓	IP Address:	10.0.0.20 Renew Release	
Channel Width:	20MHz Ŧ	Netmask:	255.255.255.0 (/24)	
Country:	austria 🗧	Gateway:	10.0.0.138	
MAC Address:	4C:5E:00			
	Use Access List (ACL)	MAC Address:	4C:5E:0C:D0:B1:D2	
Security:	WPA WPA2	- Local Network		
Encryption:	✓ aes ccm tkip	IP Address:	10.10.10.1	
WiFi Password:	Hide	Netmask:	255.255.255.0 (/24)	
			✓ DHCP Server	
Wireless Clients		DHCP Server Range:	10.10.10.10.10.10.50	
MAC Address	✓ In ACL Last IP Uptime Sig ▼ no 10.10.10.48 12:17:31 -58 10.10.10.48		✓ NAT	

Das "Internet" kommt (hier) über Gateway 10.0.0.138 und wird vom AON-Modem/Router via Netrange 10.0.0.0/24 verteilt. Der Mikrotik hat die interne IP 10.10.10.1 zugewiesen und besitzt die Netrange 10.10.10.0/24, DHCP und NAT sind aufgedreht,

Anschließend wählen wir den Menüpunkt "Interfaces" aus:

🔏 Quick Set		Interf	ace Li	ist									
CAPsMAN		Inte	face	Ethemet	EoIP Tunnel	IP Tunnel	GRE 1	unne	I VLAN	VRRP	Bonding	LTE	
Interfaces						1							Conservation of the second
🔔 Wireless			-				121	1711	т.		D		T. D. J.
Bridge		R	Ivam 1-1b	ridge1	Bridge		LZIV	1598	IX	79.	0 kbps	8	4.0 kbps
E PPP		R	4 >	ether1	Etherr	net			1598		1680	bps	23.4 kbps
Switch	RS	4 >	ether2	Ether	net			1598		512	bps	0 bps	
°t <mark>8</mark> Mesh		RS		wlan I	VVirele	ss (Atheros	AR9		1600		/9.0 k	bps	4.0 Kbps
255 IP	1												
Ø MPLS	1												
😹 Routing	\uparrow												
💮 System	\uparrow												
Queues													
Files													
🗧 🗐 Log		•											+

Anschließend legen wir mit "+" ein neues Interface "PPTP-Client" an.

Interface	Ethemet	EoIP Tunnel	IP T	Funnel	GRE Tunne	VLAN	VRRP	Bond	ling L	TE	
Traf	fic Eng Int	te <mark>r</mark> face								F	Find
PPP	Server				L2 MTU	Tx		1	Rx		Tx Pac
PPP	Client				1598		54.	1 kbps		2.4 kbps	
DDT		inding						0 bps		0 bps	
PPI	P Server b	inuing			1598		2.	1 kbps		12.5 kbps	
PPT	P Client				1598		16	96 bps		512 bps	
SST	P Server B	indina		os AR9.	. 1600		54.	1 kbps		2.4 kbps	
CCT	D Client										
331	PClient										
L2T	P Server B	inding									
L2T	P Client										
				1							

Die Konfiguration des VPN-Clients ist relativ einfach, anbei die entsprechenden Screenshots (je nach VPN-Zugang anpassen):

Interface <db0fhn></db0fhn>	
General Dial Out Status Traffic	ОК
Name: db0fhn	Cancel
Type: PPTP Client	Apply
L2 MTU:	Disable
Max MTU: 1450	Comment
Max MRU: 1450	Сору
MRRU: 1600	Remove
	Torch

Interface <db0fhn></db0fhn>			
General Dial Out State	us Traffic		ОК
Connect To:	db0fhn.efi.fh-nuemberg.de		Cancel
User:	oe7bsh		Apply
Password:			Disable
Profile:	default-encryption	₹	Comment
Keepalive Timeout:	180		Сору
	Dial On Demand		Remove
	Add Default Route		Torch
Default Route Distance:	0		
Allow:	✓ mschap2 ✓ mschap1 ✓ chap ✓ pap		

Man beachte das deaktivierte "add default route". Ansonsten versucht der Mikrotik **alle** Verbindungen über Hamnet zu führen. "Dial on demand" macht natürlich Sinn, damit nicht durchgehend eine VPN-

Verbindung steht. Die unter "allow" angeführten Verschlüsselungen sind eigentlich nicht erforderlich, da im Hamnet als Teil des Amateurfunks keine Verschlüsselung erfolgt.

Nach erfolgreicher Konfiguration finden wir nunmehr ein neues PPTP-Interface, das das VPN abbildet und wie jedes Interface angesprochen/geroutet werden kann:

Interfa	ace List							
Inter	face Ethemet E	oIP Tunnel IP Tunnel (GRE Tunnel	VLAN	VRRP Bond	ling LTE		
+ -	×						F	ind
	Name	∆ Туре	L2 MTU	Tx		Rx		Tx Pac 🔻
R	1 ⊐tbridge1	Bridge	1598		41.8 kbps		2.9 kbps	
R	<-⊳db0fhn	PPTP Client			0 bps		0 bps	
R	ether1	Ethernet	1598		2.1 kbps		23.9 kbps	
RS	♦ether2	Ethernet	1598		0 bps		0 bps	
RS	wlan1	Wireless (Atheros AR9	1600		41.8 kbps		3.1 kbps	

Einrichtung Routing 44er-Netzwerk

Soweit so gut – zum "grande finale" müssen wir dem Mikrotik noch beibringen, dass er zwischen Internet und Hamnet unterscheidet und unterschiedlich routet.

Hamnet: Alles was für 44.0.0.0/8 bestimmt ist, soll an den PPTP-Client (hier: Interface "db0fhn") weiter geleitet werden

Internet: Alles andere (default route 0.0.0.0/0) soll an den AON-Router als gateway 10.0.0.138 gehen

Wie erklären wir dem Mikrotik den Unterschied zwischen Internet und Hamnet? Wir benutzen hierzu eine Mangle-Rule. Diese erstellen wir mit "+" unter IP – Firewall – Mangle:

Firewall				×□
Filter Rules NAT Mangle	Service Ports Connections	Address Lists Layer7 Protocols		
+ -	T 00 Reset Counters	00 Reset All Counters	Find	all 🔻
# Add Action Chain	Src. Address Dst. Address	s Proto Src. Port Dst. Port	In. Inter Out. Int Bytes Packets	; T

Vor dem eigentlichen Routing ("prerouting") soll die Mangle rule alles aus dem Mikrotik-Netzwerk (10.10.10.0/24) auf ein Ziel im Hamnet (44.0.0.0/8) überprüfen:

Mangle Rule <10.10.10.0/24->44.0.0.0/8>	
General Advanced Extra Action Statistics	ОК
Chain: prerouting	Cancel
Src. Address: 10.10.10.0/24	Apply
Dst. Address: 44.0.0.0/8	Disable
Protocol:	Comment
Src. Port:	Сору
Dst. Port:	Remove
Any. Port:	Reset Counters
P2P:	Reset All Counters

Trifft die o.a. Regel zu, (aus Mikrotik-Netz zu Hamnet) dann soll das Paket entsprechend markiert werden mit dem Zusatz "mitvpn":

Mangle Rule <10.10.10.0/24->44.0.0.0/8>	
General Advanced Extra Action Statistics	ОК
Action: mark routing	Cancel
🗌 Log	Apply
Log Prefix:	Disable
New Routing Mark: mitvpn 🛛 🔻	Comment
Passthrough	Сору
	Remove
	Reset Counters
	Reset All Counters

Advanced, Extras und Statistics werden nicht benötigt.

Gut, alles Richtung Hamnet trägt nun also die Markierung "mitvpn". Davon ausgehend können wir nun unter IP – Routes die Routen eintragen für Internet Richtung 10.0.0.138 und Hamnet Richtung Interface "db0fhn":

Route <0.0.0.0/0>			
General Attribut	IS .		ОК
Dst. Address:	0.0.0/0		Cancel
Gateway:	10.0.138	•	Apply
Check Gateway:		•	Enable
Type:	unicast	Ŧ	Comment
Distance:	1		Сору
Scope:	30		Remove
Target Scope:	10		
Routing Mark:			
Pref Source:		.	
isabled	active static		
Route <44.0.0.0/8	>		
General Attribut	35		ОК
Dst. Address:	44.0.0.0/8		Cancel
Gateway:	db0fhn 🔻 reachable	\$	Apply
Check Gateway:			Disable
Type:		•	Disable
	unicast	▼ ₹	Commen
Distance:	unicast	▼ ∓ ▲	Commen
Distance: Scope:	1 30	▼ ▼	Commen Copy Remove
Distance: Scope: Target Scope:	unicast 1 30 10	▼ ▼ ▼	Commen Copy Remove
Distance: Scope: Target Scope: Routing Mark:	unicast 1 30 10 mitvpn		Commer Copy Remove

44.0.0.0/8 wird wie bereits ausgeführt zum Gateway db0fhn geroutet – anhand der Routing Mark "mitvpn".

Weiters wurden noch die entsprechenden NAT-Rules angelegt:

Firewall														
Filter F	lules 1	TAV	Mangle	Service Ports	Connections	s Ado	dress Lists	s Layer7 F	rotocols					
+ -	- 🗸	×	:	7 00 Res	set Counters	00	Reset A	Counters				Find	all	₹
#	Actio	n I	Chain	Src. Address	s Dst. Ad	dress	Proto	Src. Port	Dst. Port	In. Inter	Out. Int	Bytes	Packets	-
0	≓ll m	as i	srcnat	10.10.10.0/2	24						db0fhn	361.7 KiB	6 904	
1	≓∥m	as :	sronat								ether1	20.0 MiB	311 956	

NAT-Rule für Hamnet:

NAT Pulo 210 10 10 0/245			
NAT NUE <10.10.0/242		NAT Rule <10.10.10.0/24>	
General Advanced Extra Action	ОК	Advanced Extra Action Statistics	ок
Chain: srcnat	Cancel	Action: masquerade	Cancel
Src. Address: 10.10.10.0/24	Apply		Carloci
			Apply
Dst. Address:	Disable		
		Log Prefix:	Disable
Protocol:	Comment		
			Comment
Src. Port:	Сору		
Det Det	Remove		Сору
Dst. Port:	Tiemove		
Any Port	Reset Counters		Remove
			Devel Counters
In. Interface:	Reset All Counters		Reset Counters
Out. Interface: db0fhn ∓ 🔺		1	Reset All Counters

Nat-Rule für Internet:

NAT Rule <>				
General Advanced Extra Action		ОК	NAT Rule <>	
Chain: srcnat	Ŧ	Cancel	Advanced Extra Action Statistics	ОК
Src. Address:	•	Apply	Action: masquerade 🔻	Cancel
Dst. Address:	•	Disable		Apply
Protocol:	•	Comment	Log Prefix:	Disable
Src. Port:	-	Сору		Comment
Dst. Port:	-	Remove		Сору
Any. Port:	•	Reset Counters		Remove
In. Interface:	•	Reset All Counters		Reset Counters
Out. Interface: ether1 Ŧ	•		6	Reset All Counters

Damit sollte nunmehr der Traffic der via WLAN bzw. LAN beim Routerboard "aufschlägt" entsprechend Richtung Internet bzw. Hamnet geroutet werden.

Disclaimer: Hat hier einwandfrei funktioniert, wir sind aber im Experimentalfunk, also alles auf eigene Gefahr und Risiko [©] (heißt: Mikrotik davor mit Backup versehen).

Bernd, OE7BSH oe7bsh@oevsv.at

22.1.2016 – V 1.0