MikroTik hEX lite

Grundeinrichtung

1. Default config löschen (übers Terminal)

```
system reset-configuration skip-backup=yes no-default=yes
```

2. mittels Winbox verbinden
3. Internet an einen Port anschließen (eth1)
4. Rechner/Laptop an einem Port anschließen (eth2)
5. auf diesem Port muss ein DHCP Client eingerichtet werden, INterface (eth1), “Use Peer DNS”, “Use Peer NTP” und “Add default Route” ebenfalls aktivieren, vom Port kann nun ins Internet gepingt werden
6. NAT muss eingerichtet werden “IP” - “Firewall” - Reiter “NAT”, add new “Chain: srcnat”, out “eth1”, Action: “masquerade”, dann sollte ein Ping ins Internet vom Rechner aus bereits möglich sein.
7. DNS Relay müssen noch eintestellt werden, “IP” - “DNS” - “Allow remote DNS requests”
8. Portscan über nmap möglich zur Kontrolle, welche Ports offen sind. Von einem externen Client nmap auf die externe IP des Routers laufen lassen.
9. Firewall einrichten “IP” - “Firewall”, Achtung, wird von oben nach unten abgearbeitet, Reihenfolge beachten, sonst blockt man sich selbst aus. Für jede Regel kann ein Kommentar eingefügt werden.
    1. Chain: input, Connection state: established, Action: accept
    2. Chain: input, Connection state: related, Action: accept
    3. Chain: input, In. Interface: eth2, Action: accept (eth2 ist in dem Fall mein Laptop)
    4. Chain: input, Action: log
    5. Chain: input, Action: drop (jede weitere Information wird geblockt)
    6. Erneut nmap durchführen, (fast) keine Ports mehr offen
    7. Log deaktivieren (nicht löschen)
10. Firewall Forward einrichten
    1. Chain: forward, Connection State: established, Action: accept
    2. Chain: forward, Connection State: related, Action: accept
    3. Chain: forward, In. Interface: eth2, Dst. Address: !localnetwork, Protocol 6 (tcp), Dst. Port: 80, 443
        - Für andere Protokolle wird eine extra Regel benötigt
    4. Chain: forward, Action: drop
        - Somit geht nur lokaler Surf-Traffic raus, das interne Netz darf surfen, von außen kommt nichts rein.
11. Wenn man sehr viele Firewallregeln hat, kann gefiltert werden (rechts oben)
12. Interfaces können umbenannnt werden, Punkt “Interfaces”, z.b. eth1 auf e1wan und eth2 auf e2lan (später e3dmz, etc.)
13. Bridge muss angelegt werden, um die Ports zusammenzuführen
14. “Bridge”, neue Bridge anlegen “br-lan”, hier werden die Ports zusammengeführt, welche sich im LAN bewegen werden, auch virtuelle LANs können hier dann hinzugefügt werden.
15. Reiter “Ports”, hier neu anlegen “Interface: e10lan, Bridge: br-lan”
    - Achtung, Firewall muss angepasst werden, Winbox nicht schließen, sonst kein Zugriff mehr (jetzt noch möglich, da established zugelassen ist, Verbindung besteht bereits)

16. “IP” - “Firewall” - Input nicht mehr e2lan sondern die Bridge br-lan
17. “IP” - “Firewall” - die Forward Regel muss ebenfalls von e2lan auf br-lan geändert werden
18. “IP” - “Adress List” - hier ebenfalls von e2lan auf br-lan ändern (ist zwar möglich, aber sauberer mit der bridge)
19. Wenn das erweiterte Gerät vorhanden ist, kann ich die Hardware-Switchfunktion verwenden um CPU zu sparen. “Switch”, hier den korrekten Switch auswählen und “Switch all Ports” auswählen.
    1. “Interface” - Hier dann den ersten Port nehmen und auf Master umbenennen (z.B. sw1-e1-master), zweiten Port auswählen, sw1-e2-slave und einstellen “Master Port: sw1-e1-master”
    2. Der Switch ist allerdings isoliert, 2 PC am gleichen Switch erreichen untereinander, aber können nicht ins Internet.
    3. “Bridge” - “Ports” - neu anlegen “Interface: sw1-e1-master, Bridge: br-lan”
        1. Somit ist der Switch mit dem anderen Port verbunden und die Rechner können ins Internet.
20. DHCP Server einrichten (Später, je VLAN auch einen DHCP Server)
    1. “DHCP Setup”, Gatway ist der Router, DNS Server kann auch der Router sein, kann auch der vorgeschlagene verwendet werden. Range bsp. von .100 - .200, der rest kann reserviert werden.
21. So ist ein der Router erst einmal fertig konfiguriert

Backup & Restore

1. “File” - “Backup” - “Backup” - Name eingeben, backup wird am lokalen flashspeicher vom Router erstellt.
2. Das ist ein Fullbackup zum zurückspielen am gleichen Gerät. Auf einem anderen Gerät nicht möglich. Einstellungen, User, Passwörter.
3. ssh admin@ipadresse
4. /export compact
    1. Alle Änderungen in der Sprache. Kann angepasst werden und kann eingefügt werden, auch auf einem anderen Gerät.
5. /export compact file=test
    1. auf dem Flashspeicher wird eine Datei “Test” erzeugt, welche wieder kopiert werden kann. Keine User, keine Passwörter

Loggin & Syslog

1. Zeitstempel muss korrekt sein, deswegen Zeit / Datum korrekt konfigurieren. “System” - “SNTP” enabled, Unicast, DNS-Name kann eingetragen werden, wird automatisch auf IP aufgelöst. Infos dazu werden unten reingeschrieben.
2. “System” - “Clock” - Check. Hier wird die Zeit noch falsch sein, da die falsche Zeitzone ausgewählt ist. Für Deutschland/Österreich - Europe/Berlin
3. “Log” hier wird alles angezeigt, begrenzte Zeilenazahl, zum Nachvolziehen schwierig (z. B. Hackattacke)
4. Firewall - Logregel - ganz nach oben schieben damit alles geloggt wird. Je weiter sie nach unten geschoben wird, um so wenig wird geloggt.
5. “System” - “Logging” hier wird das Default-Setup angezeigt. Um alles, außer Firewall zu loggen zweite Bedingung anwählen “!Firewall” (! zum ausschließen“. Somit sehe ich aber Firewall

nirgends.
6. Syslogserver soll aktiviert sein, Port 514 üblicherweise.
7. “System” - “Loggin” - Reiter “Actions” - neue Action “name: syslog1, type: remote, Remote Adress: syslogserverIP”, Reiter “Rules” Topics: firewall, Action: syslog1”
8. Somit sehe ich am Mikrotik selbst nur die Änderungen, die gemacht werden, alles was die Firewall betrifft ist ausgelagert und kann gesichert werden. Wenn WLAN angeboten wird, müssen auch Daten gespeichert werden.

QOS

SSH Verkehr soll separiert werden und soll Vorrang erhalten gegenüber anderen Verbindungen. Dazu muss der Traffic erst markiert werden.

1. “IP” - “Firewall” - Reiter “Mangle” für die Markierung
    1. neue Regel “Chain: prerouting, Protocol: 6(tcp), Dst. Port: 22, Action: mark connection, New Connection mark: ssh*con” - neue Regel “Chain: prerouting, Connection Mark: ssh*con, Action: mark packet, New Packet Mark: ssh*pkt” * Alle Pakete die zu dieser Verbdindung gehören, werden mit ssh*pkt markiert.
2. Queue - Reiter “Simple Queue”
    1. Reiter “Simple Queues” - “Name: wan1, Target: e1wan”, Target Upload: Max Limit 1M“
    2. Reiter “Advanced” - “Packet Marks: no-mark, priority 8, Queue Type: default (ist eine FIFO Regel)
    3. Reiter “Simple Queues” - “Name: wan-hi, target: e1wan, Target Upload: Max Limit 1M”
    4. Reiter “Advanced” - “packet Marks: ssh_pkt, priority: 2”
3. Firewall, Regel für Internet, Port 22 muss hinzugefügt werden
4. Eine extra Regel kann z.B. auch für VoIP angelegt werden.

SSH

Über Telnet und SSH möglich, wobei SSH sicherer ist. Über Windows über putty möglich, über Linux direkt übers Terminal (ssh admin@ip).