[Worklog] - [User Review]

VPN Gateway Enigmabox - virtualisiert auf dem Prüfstand

Einleitung:

Hi

Ich bin schon einige Jahre mit Firewalls und Netzwerktechnik am experimentieren. Ich bin allerdings kein Profi. Angefangen hatte ich mit einer virtuellen Endian auf dem ESXi, welche hinter einem Router hing (doppeltes NAT). Damals schon suchte ich eine Möglichkeit, einen eigenen virtuellen Gateway auf dem ESXi zur Verfügung zu haben. Ich wurde dann auf die Enigmabox aufmerksam gemacht. Die Enigmabox (ALIX Board mit openWRT) hatte ich zuerst ein Jahr als Hardware in Betrieb. Später gab es die Box wie gewünscht virtuell. Allerdings wollte ich sie nicht ungeschützt in mein LAN hängen. Ich kaufte mir dann eine Zywall 110, seither läuft das Cablemodem im bridged mode. Bis vor kurzem hatte ich da zwei fixe IP's am Cablemodem.

Ich bekam dann drei Zertifikate für einige Monate zur Verfügung gestellt, um das Ganze auf verschiedenen Virtualisierungsplattformen zu testen. Ich habe die virtualisierte Box neben vSphere auch auf vmware Workstation und Oracle VirtualBox getestet, was so für die meisten User praktikabel wäre. Auf den Desktop Systemen (Typ-2-Hypervisor) hat man am Host das Internet des Providers, und in einem host-only vmnet das VPN für die Gäste anliegen. Die Enigmabox läuft in einer separaten VM.

Allerdings hat der Entwickler wohl kein Interesse daran, dass man Unterstützung für die virtuelle Version bietet. Ich hätte da sonst Anleitungen für alle Plattformen geschrieben. Das war aber nicht wirklich gewünscht, und so ist das Thema für mich vorerst auch gegessen. Trotzdem wollte ich Euch ein Review der virtualisierten Box nicht vorenthalten.

Auch die Version mit Hardwarebox und an den Gast durchgereichter USB NIC am Typ-2-Hypervisor ist noch eine Option. Das hatte ich so getestet, als ich die Box noch nicht virtuell am Laufen hatte.

Ich bin kein Mitglied im Enigmabox Verein, ich bin lediglich Benutzer. Daher biete ich nur hier Support an, und das nur im Bezug der hier im Artikel beschriebenen Aspekte. Ich mache kein Support für Box Images, Box Updates oder Zertifikate.

Die offizielle Website des Vereins Enigmabox:

https://enigmabox.net/

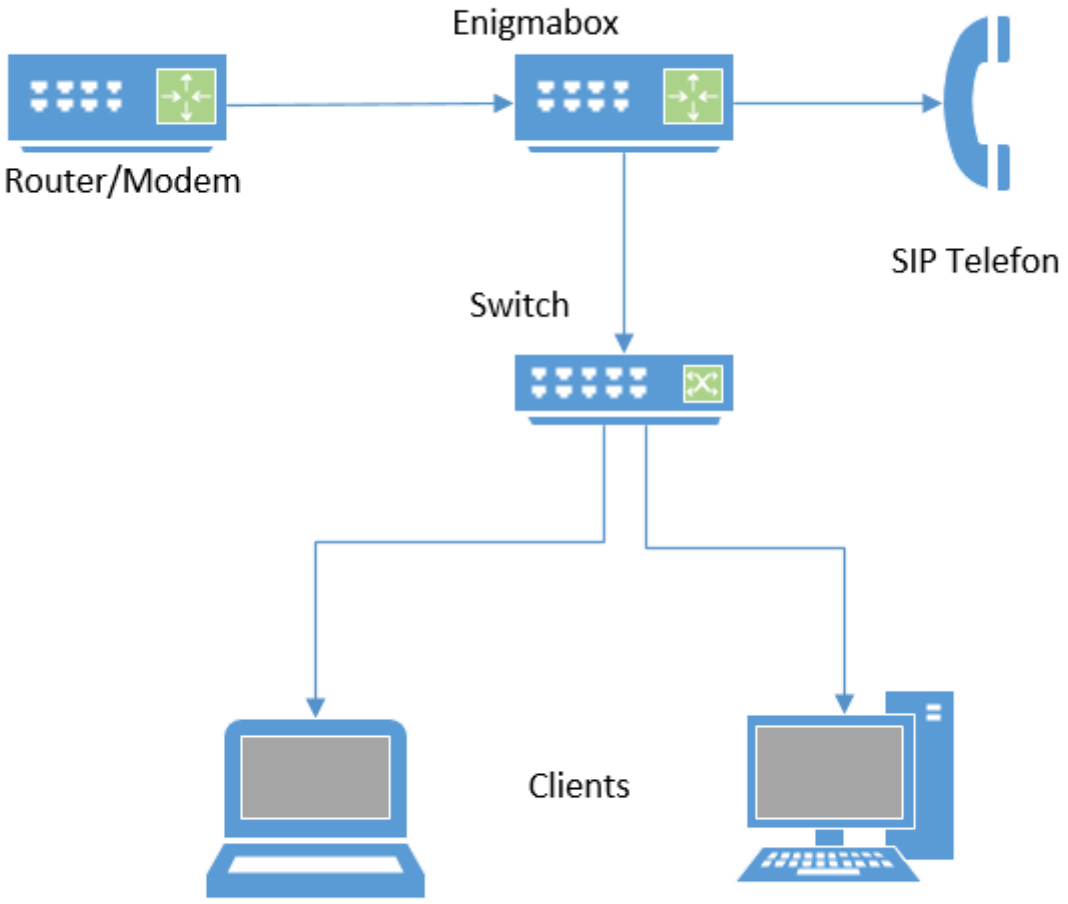
Lieferumfang der Box:

- Enigmabox mit bespielter SD Karte, Netzteil
- SIP Telefon mit Netzteil
- USB Stick mit Zertifikat
- Netzwerkkabel (ich glaube 2 Stück)

Es gibt eine Version mit 100 Mbit/s NIC's, und eine Neuere mit 1 Gbit/s Unterstützung. Die Preise findet man hier:

https://enigmabox.net/shop/

So wird das Netzwerk üblicherweise verkabelt (hier mit optionalem Switch):



Hier wird noch näher auf die Funktionsweise der Enigmabox eingegangen:

https://enigmabox.net/

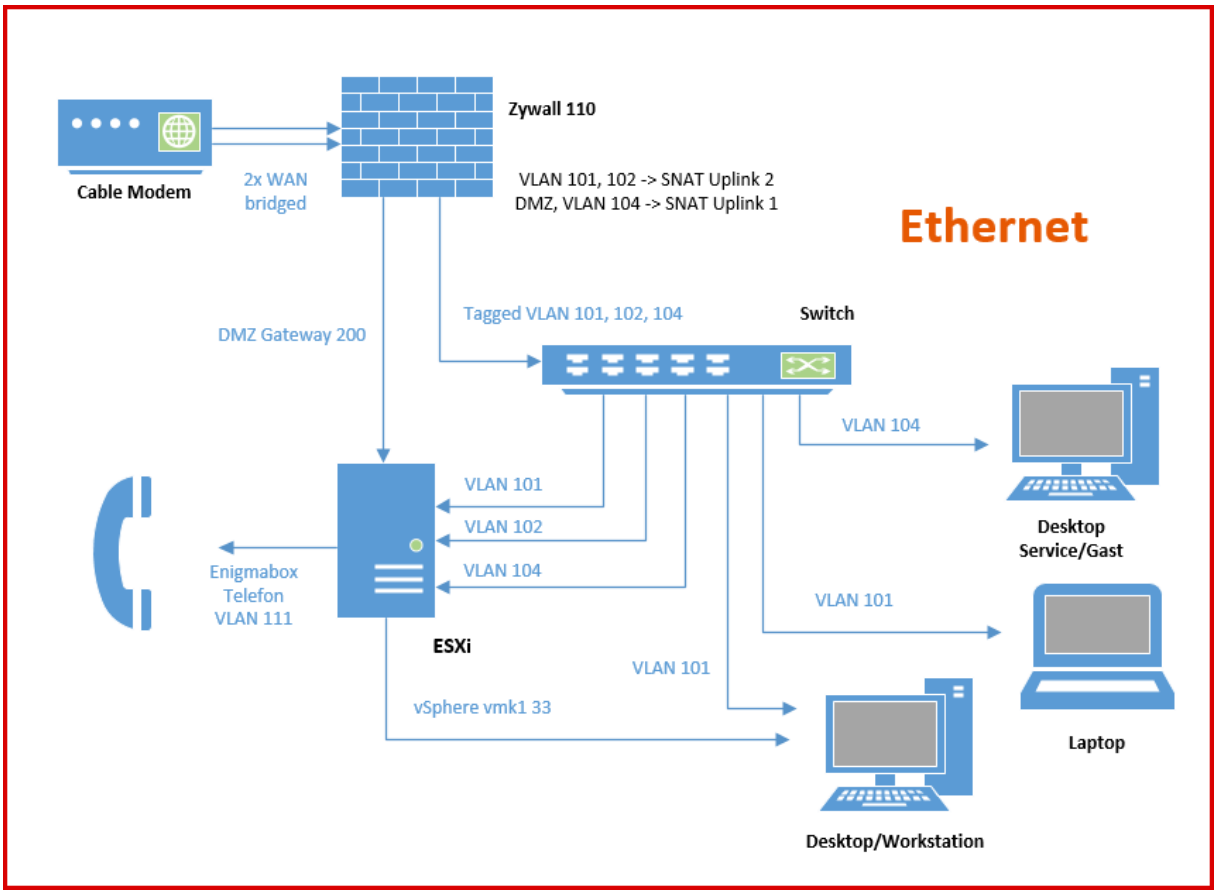
https://deutsche-wirtschafts-nachrichten.de/2013/11/09/enigmabox-telekommunikation-unter-dem-radar-der-nsa/

https://www.datenschutzbeauftragter-info.de/enigmabox-sichere-internet-und-telefonverschluesselung-out-of-the-box/

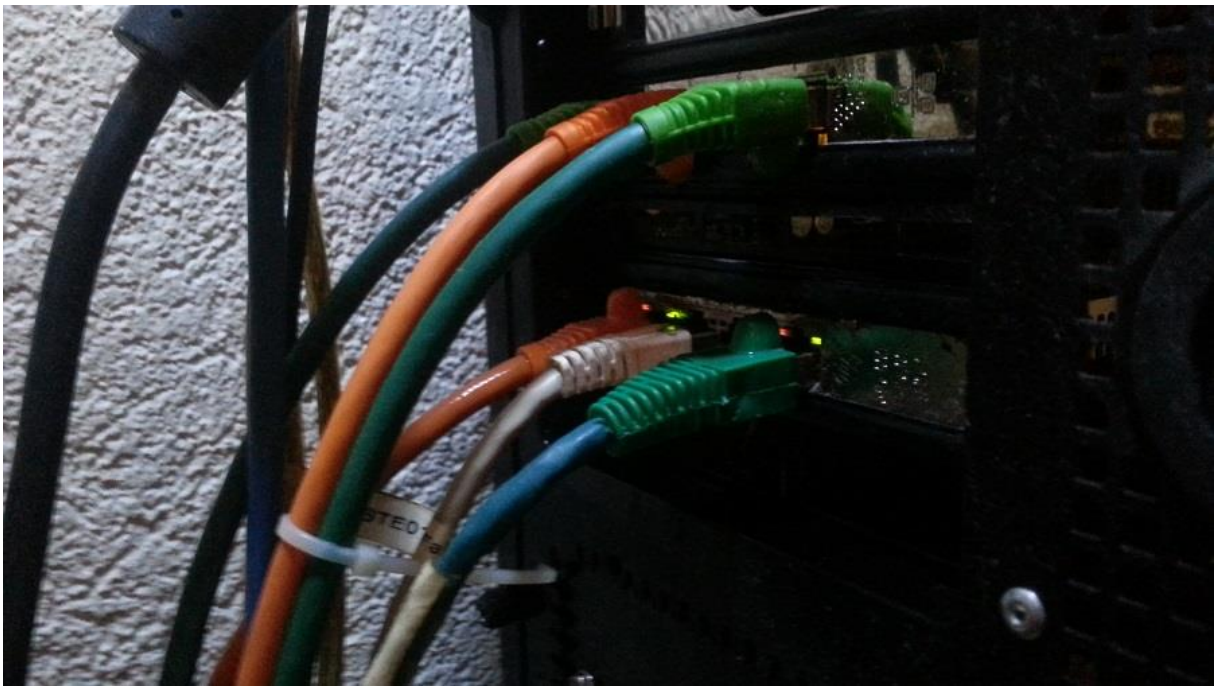
https://www.heise.de/ct/ausgabe/2014-1-kurz-vorgestellt-Verschluesselungsbox-2280320.html

Ich spare mir diese grundliegenden Infos daher in meinem Review, ich gehe hier mehr auf die Ergebnisse meiner Experimente und den Aspekt mit der Virtualisierung ein.

So sieht mein Testaufbau momentan aus:

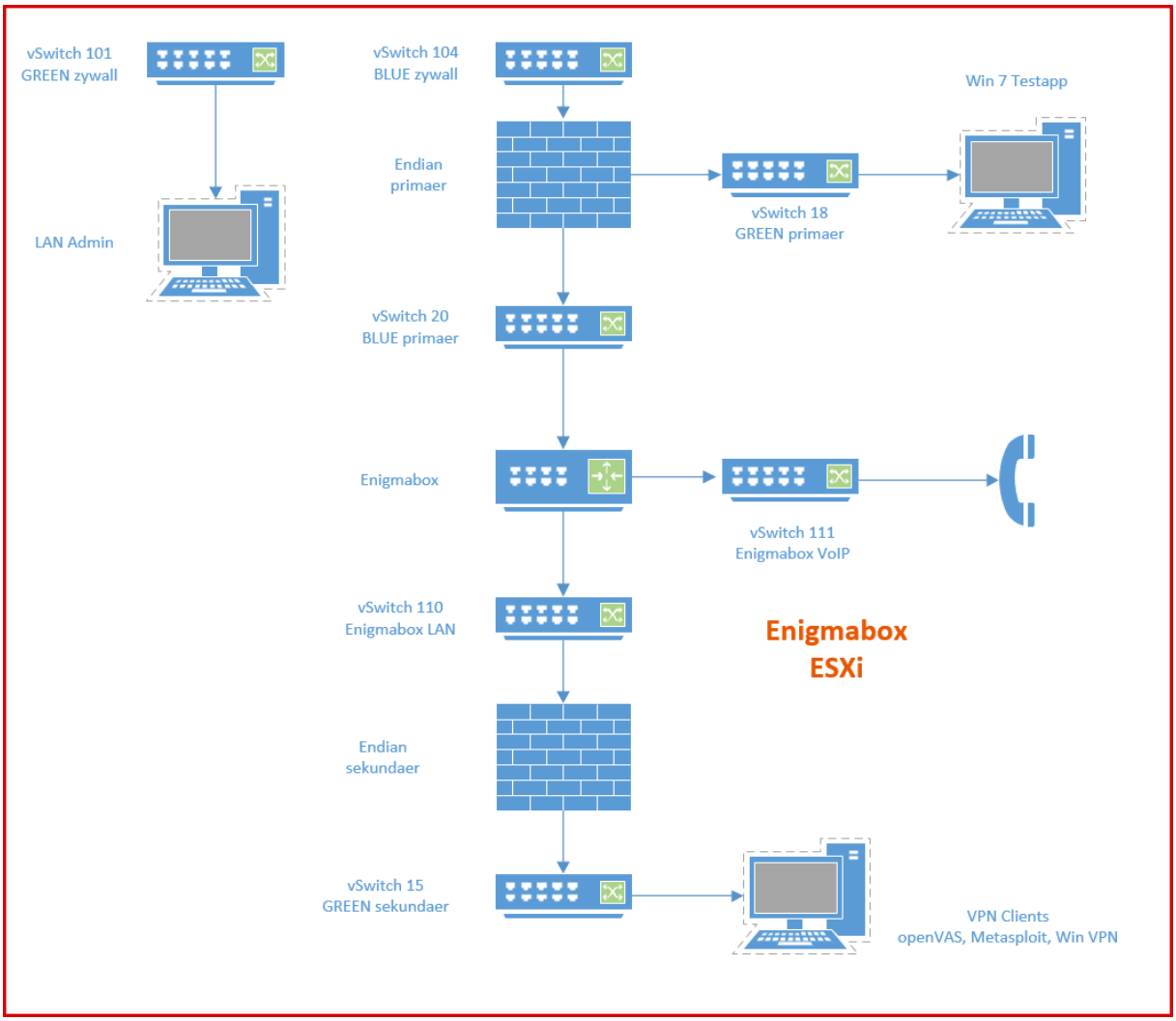


95% der IP Adressen in meinem Netzwerk werden von der Zywall, bzw. den Endians per DHCP und MAC-Bindung vergeben.



ESXi

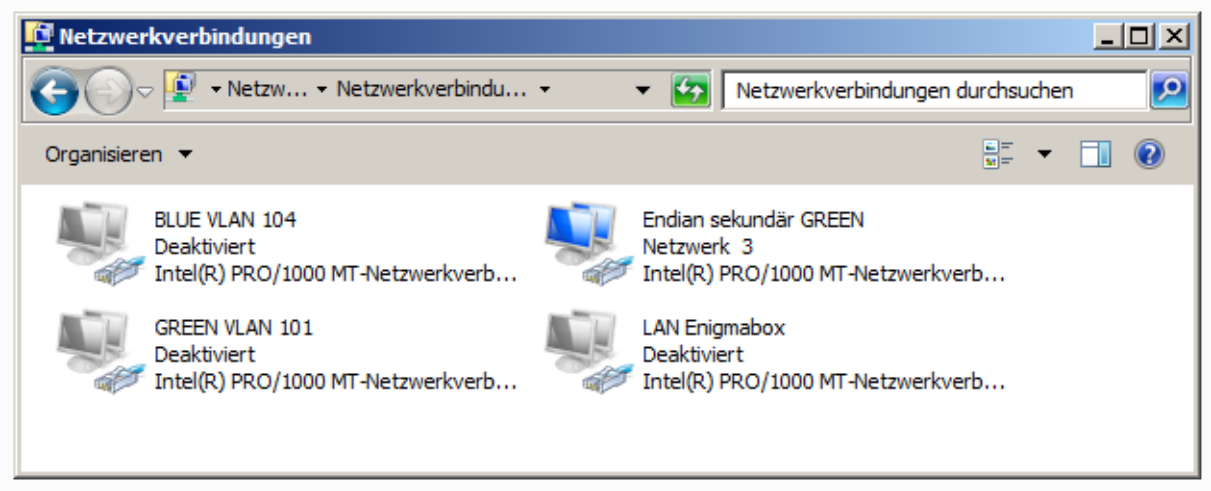
Auf vSphere (ESXi Server) habe ich es folgendermassen eingerichtet:



Die virtualisierte Enigmabox habe ich zwischen zwei Firewalls (Endian mit ntop für Traffic Monitoring) geklemmt, damit ich den Verkehr analysieren kann, den der Gateway so macht. Und der macht munter Traffic (siehe weiter unten), auch wenn die sekundäre Endian ausgeschaltet ist. Der Gateway kommuniziert aber nur verschlüsselt, so wie er soll. Allerdings gleichzeitig zu allen Servern. Der Entwickler meinte, das hängt mit dem Netzwerkprotokoll Cjdns zusammen.

An der VM „Win 7 Testapp“ (VLAN 18) monitore ich das WAN der Enigmabox (VLAN 20). Während der Performance Tests hängt natürlich sonst nichts am VLAN 20. Um an den einzelnen Netzwerken zu sniffen muss man beim betreffendem vSwitch den promiscuous mode zulassen.

Das Schaubild ist stark vereinfacht. Ich habe an den besagten virtuellen Maschinen mehrere virtuelle Netzwerk-Adapter mit eingehängt, die ich im Gast selber nach Bedarf de-/aktiviere. Hier wird nur die Testkonstellation aufgezeigt. So kann ich in den Gästen zwischen den VLAN‘s switchen, wie ich gerade will (hier am Beispiel des „Win VPN“ Gasts):



Virtualisierung:

Das Ganze auf die verschiedenen Plattformen zu virtualisieren war nicht ganz ohne. Ursprünglich wollte ich einen Guide erstellen, aber ich konnte keine einheitliche Methode, bzw. ein einheitliches Image für alle Plattformen finden. Ausserdem bin ich noch auf einem älterem Release des Box Images. Das Update will nicht so recht auf Anhieb, und ich bleibe bei meinem Stand bis auf weiteres. Automatische Aktualisierungen habe ich daher deaktiviert bei mir.

Falls das jemand nachbauen möchte, kann ich nur ein paar Tipp's dazu geben. Das Problem war folgendes:

Typ-1-Hypervisor:

Ich hatte mehrere Images zur Verfügung. Ursprünglich hatte ich ein Image der CF Karte des Boards (32bit) mit Clonezilla gezogen, welches ich nach langem hin und her dann am ESXi zum laufen gebracht hatte. Das Problem war der verwendete Festplattencontroller (Parallel bei der CF Version), da war ich echt am basteln, bis das lief. Ich habe es jetzt mit dem 32 bit Image auf dem ESXi am laufen, mit dem LSI Parallel Controller.

Wer sich das nachbauen möchte, findet weitere Infos in meinem folgendem Fred:

http://vmware-forum.de/viewtopic.php?f=40&t=31240

Folgende Ressourcen habe ich der Enigmabox auf dem ESXi zugewiesen:

- 1 CPU Kern
- 1.2 GB RAM
- 8 GB Speicher (flat) an LSI parallel -> ddb.adapterType = "lsilogic"
- 3x NIC *E1000* -> **WAN - LAN - VoIP**, bzw. **VoIP - LAN - WAN**, je nach Image
- USB Controller für Update und das Einspielen des Zertifikats
- Video Card 8 MB (empfohlen)
- COM Schnittstelle an .txt Datei für die Tests (optional)
- CD/DVD Laufwerk für Clonezilla oder Live Linux (optional)

Einstellungen der VM:

Gastbetriebssystem:	Anderes Linux-System (64 Bit)
Kompatibilität:	ESXi 5.5 und höher (VM-Version 10)
VMware Tools:	Nein

Typ-2-Hypervisor:

Auf den Desktop Systemen (VMware Workstation und VirtualBox) läuft die Enigmabox in einer separaten VM, welche dann den besagten Gateway weiteren Gästen zur Verfügung stellt. Am Host selber liegt dabei kein VPN an, hier geht der Internetverkehr normal über den Provider. Ideal auch auf einem Laptop. ☺

Ausserdem kann man im Gast mit der Linphone Software ohne SIP Telefon telefonieren. Das kann man übrigens auch mit der Hardwarebox. Das VPN Internet steht nur am LAN Port der Box zur Verfügung, VoIP hingegen an beiden Schnittstellen (bei mir VLAN 110 und 111, Enigmabox default ist 100 und 101).

Wenn die Box aus ist, und jemand eine Nachricht an das Mail System schreibt, landet diese allerdings im Nirwana. Es müssen da beide Seiten online sein, damit die Message durch kommt.

Für vmware Workstation und VirtualBox hatte ich ein 64 bit Image zur Verfügung, welches sich dann per SATA Controller einbinden liess. Dieses Image hatte mir der Entwickler direkt als virtual Disk kompiliert. Auf dem ESXi hatte ich das 64 bit Image leider nicht zum laufen gebracht. Das Ganze ist aber im Entwicklungsstadium. Offiziell supportet ist nur die Hardwarebox.

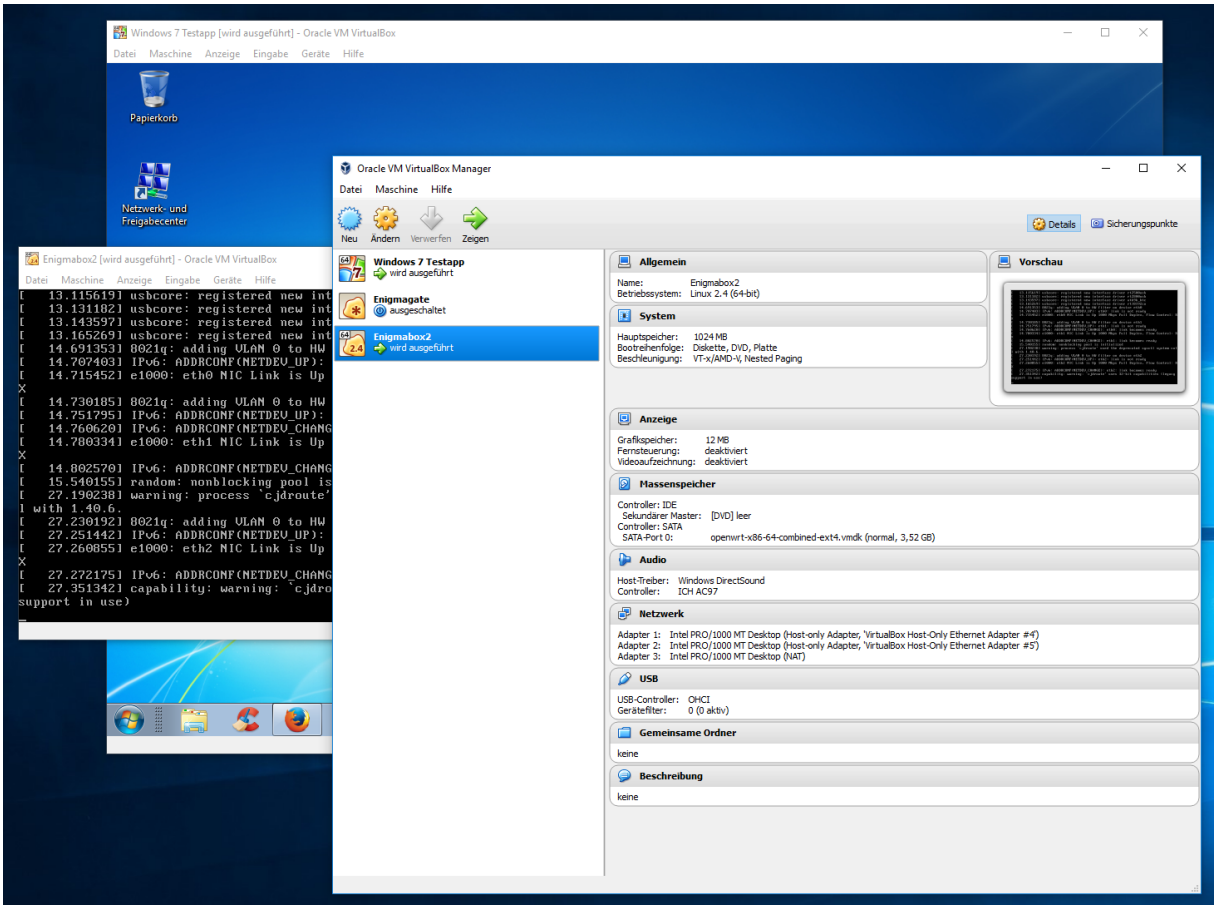
Den Source Code findet man bei github:

https://github.com/enigmagroup/enigmabox-openwrt

Auf den zwei Host-only vmnet's „Enigmabox LAN" und „VoIP" (z.B. vmnet 4 und vmnet 5) ist das DHCP zu deaktivieren. DHCP übernimmt die Enigmabox VM. Das WAN der Box habe ich am NAT Adapter (vmnet 8), hier wäre aber auch bridged (vmnet 0) eine Option.

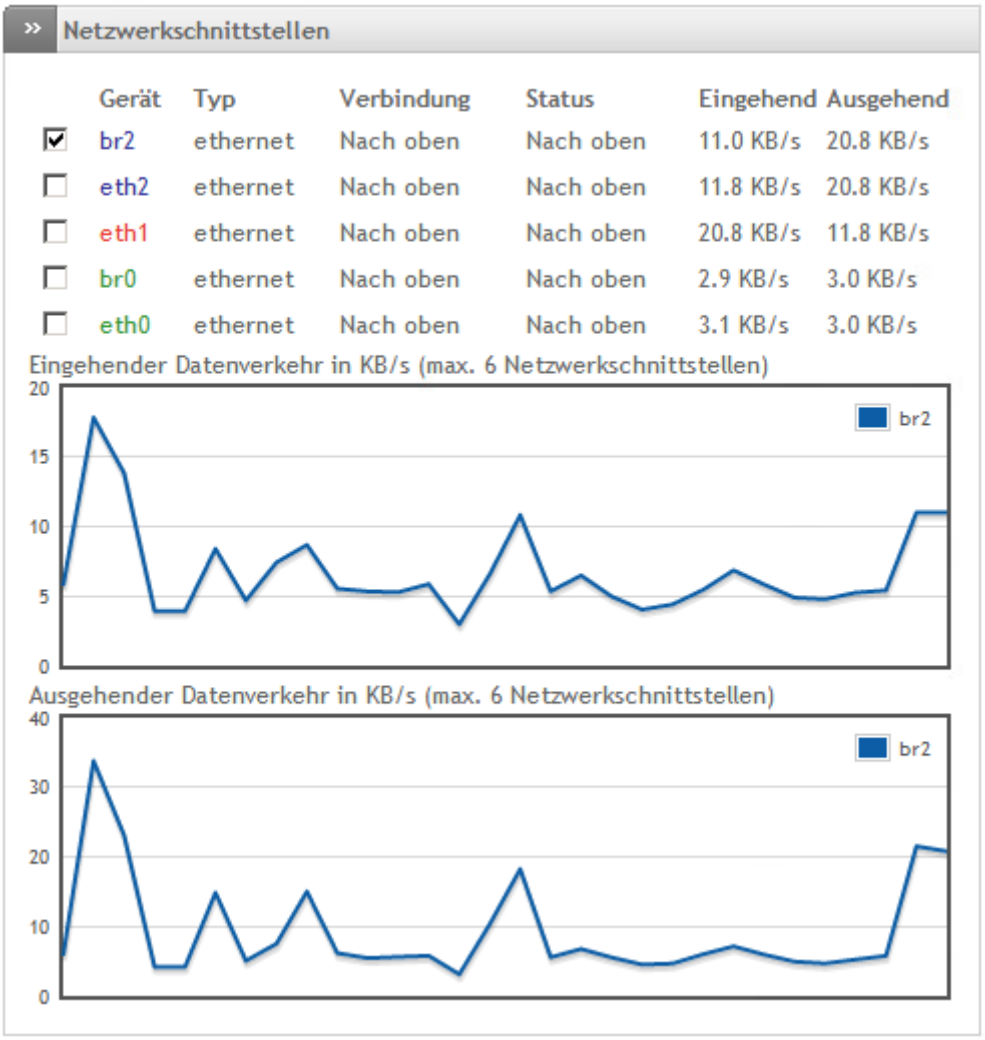
VoIP - LAN – WAN ist die Reihenfolge bei den Adaptern beim 64 bit Image.

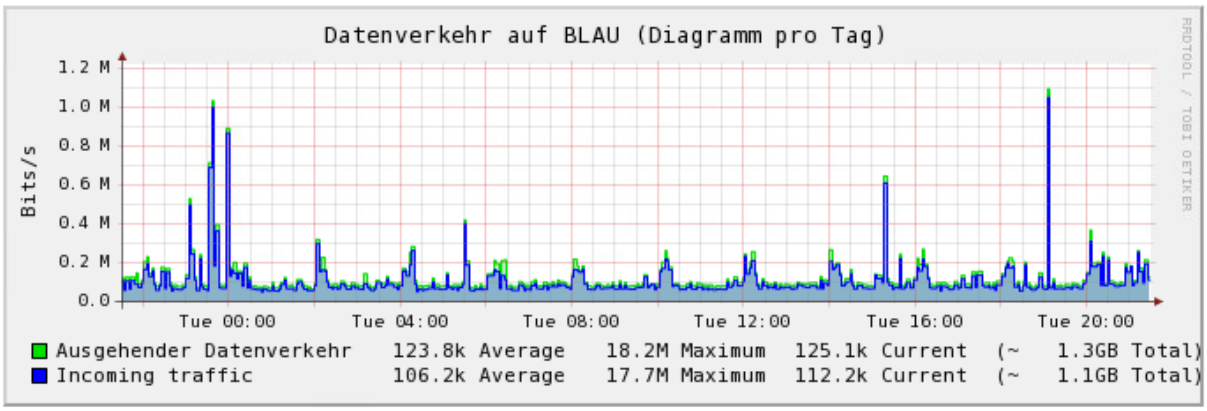
Ich empfehle den Host, den Hypervisor und die Gäste auf SSD zu installieren. So arbeitet es sich einfach smoother.



Enigmabox virtuell auf Oracle VirtualBox

So idelt die Box auf dem VLAN 20 (Endian Primaer):



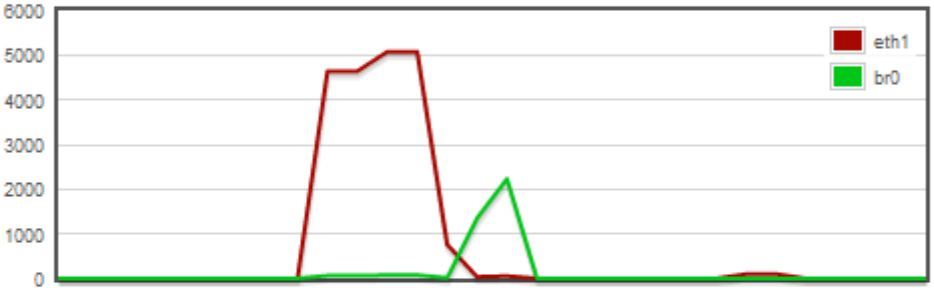


Speedtest an VLAN 15 (Endian sekundaer):

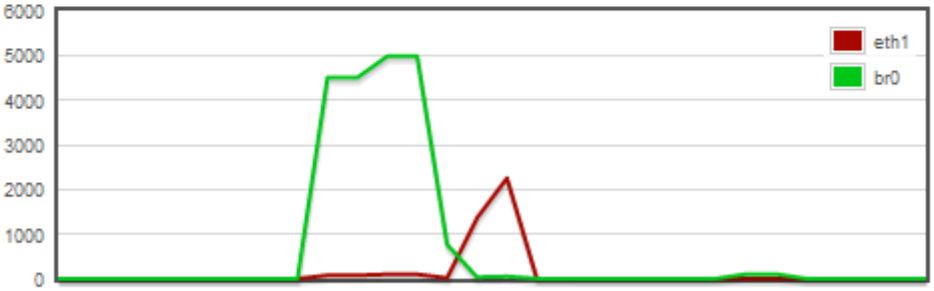
Netzwerkschnittstellen

	Gerät	Typ	Verbindung	Status	Eingehend	Ausgehend
☐	br1	ethernet	Nach oben	Nach oben	0.0 KB/s	0.0 KB/s
☐	eth2	ethernet	Nach oben	Nach oben	0.0 KB/s	0.0 KB/s
☐	br2	ethernet	Nach oben	Nach oben	0.0 KB/s	0.0 KB/s
☐	eth3	ethernet	Nach oben	Nach oben	0.0 KB/s	0.0 KB/s
☑	eth1	ethernet	Nach oben	Nach oben	0.1 KB/s	0.1 KB/s
☑	br0	ethernet	Nach oben	Nach oben	2.0 KB/s	2.2 KB/s
☐	eth0	ethernet	Nach oben	Nach oben	2.1 KB/s	2.2 KB/s

Eingehender Datenverkehr in KB/s (max. 6 Netzwerkschnittstellen)



Ausgehender Datenverkehr in KB/s (max. 6 Netzwerkschnittstellen)

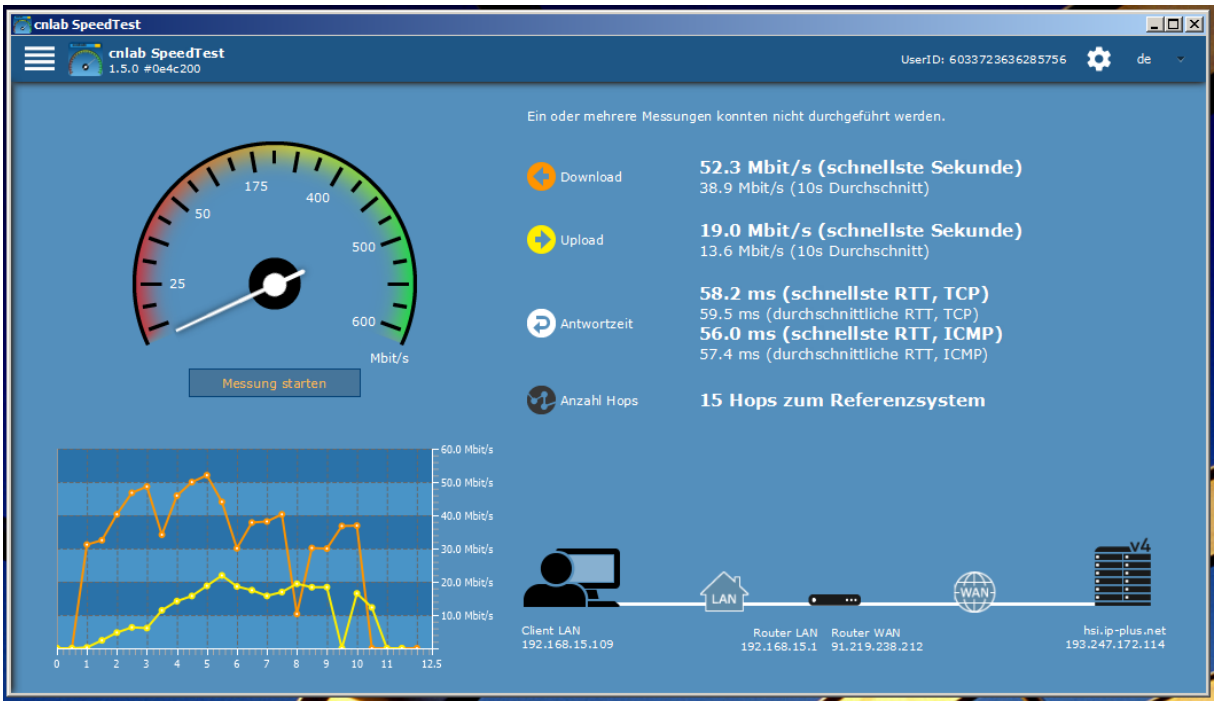


Uplinks

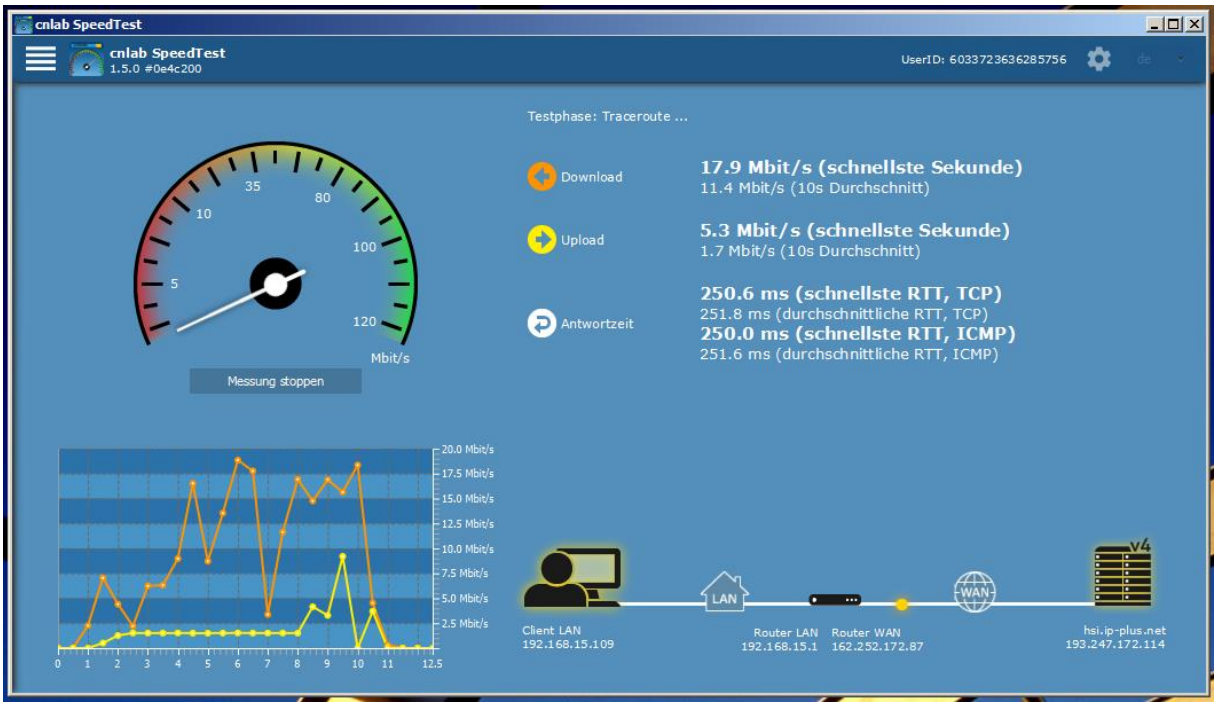
Name	IP Adresse	Status	Betriebszeit	Aktiv	Verwaltet	
Haupt-Uplink	192.168.110.50	UP	0d 0h 19m 43s	☑	☑	

→ = *Backup Uplink*

Hier die Ungarn Node:



In die USA sieht es erwartungsgemäss etwas anders aus:



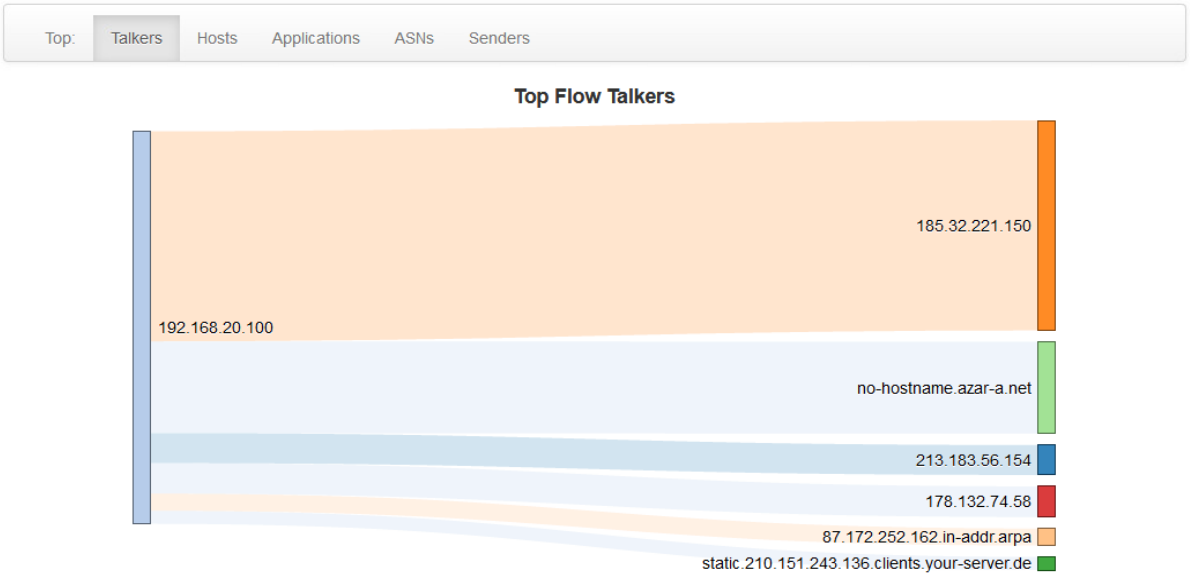
Folgende Exitnodes stehen zur Verfügung:

Land	IP	Up (Mbit/s) **	Down (Mbit/s)	Ping (ms)
Ungarn	91.219.238.212	> 20.0	Ø 40.0	Ø 60
Schweiz	185.32.221.150	> 20.0	Ø 54.0	Ø 15
Deutschland	136.243.151.210	> 20.0	Ø 40.0	Ø 33
Schweden	178.132.74.58	> 20.0	Ø 34.0	Ø 80
USA	162.252.172.87	Ø 2.0	Ø 9.0	Ø 250
Russland * **	213.183.56.154	-	-	-

** Ich habe nur 20 Mbit/s Upstream zur Verfügung, daher sind die Werte hier nicht repräsentativ.

*** Da ich auf einem älteren Release bin, läuft bei mir der Russland Server nicht auf dem ESXi.

Mit folgenden Host's redet die Box:



66.88 Kbps [32 pps]
Uptime: 10 days, 21 hours, 15 min, 32 sec
23 hosts 6 flows

ntop

Home Flows Hosts Interfaces Admin Search Host

Hosts List

10

IP Address	Location	Symbolic Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.168.20.100	Local	192.168.20.100	9 days, 16 hours, 58 min, 52 sec		Sent Rcvd	40.82 Kbit	6.14 GB
91.219.238.212	Remote	no-hostname.azar-a.net	9 days, 16 hours, 58 min, 44 sec		Sent Rc	13.05 Kbit	3.92 GB
185.32.221.150	Remote	185.32.221.150	9 days, 16 hours, 58 min, 44 sec		Sent Rcvd	10.11 Kbit	1.65 GB
136.243.151.210	Remote	static.210.151.243.136.clients.your-server.de	9 days, 16 hours, 58 min, 44 sec		Sent Rcvd	13.57 Kbit	309.03 MB
162.252.172.87	Remote	87.172.252.162.in-addr.arpa	9 days, 16 hours, 58 min, 44 sec		Sent Rcvd	816 bps	121.63 MB
178.132.74.58	Remote	178.132.74.58	9 days, 16 hours, 58 min, 44 sec		Sent Rcvd	2.08 Kbit	84.25 MB
213.183.56.154	Remote	154.56.183.213.in-addr.arpa	9 days, 16 hours, 58 min, 44 sec		Sent Rcvd	1.22 Kbit	59.17 MB
00:0C:29[redacted]	Local	00:0C:29[redacted]	57 sec		Sent	0 bps	87.45 KB

Showing 1 to 8 of 8 rows

586.03 Kbps [204 pps]
Uptime: 10 days, 21 hours, 13 min, 29 sec
27 hosts 6 flows

Fazit:

Im Gegensatz zum reinen VPN aus dem Client heraus finde ich positiv, dass es ein Gateway ist. Ausserdem sind die Mail/VoIP Module ganz nett. Für mich ist es mehr Spielerei, ich traue da für 99.99% meines Traffics eher meinem Provider als einem VPN Anbieter (ist wohl Geschmackssache). Aber auf jeden Fall nice to have!

Geschwindigkeit hat man anscheinend erhöht in letzter Zeit, ich finde sie recht gut so.

Wär nice, wenn man dazu ein universelles Box Image kompilieren könnte, welches an allen virtuellen Festplattencontrollern funktioniert. Oder zumindest, welches auf allen Systemen mit den gleichen Controller Einstellungen läuft. Ausserdem klappt es noch nicht so ganz mit den online Box Updates und durchgereichtem USB. Falls jemand mit Linux Kenntnissen Lust hat: bitte PM an mich!

Wenn das mein System wäre, würde ich wohl noch folgende Features einbauen:

- ISO Installer für individuelle Installation auf x86 Systemen
- MAC Bindung für die Clients, Netzwerk Editor
- Daten und Zertifikate sichern/wiederherstellen über Browser, bzw. am Client