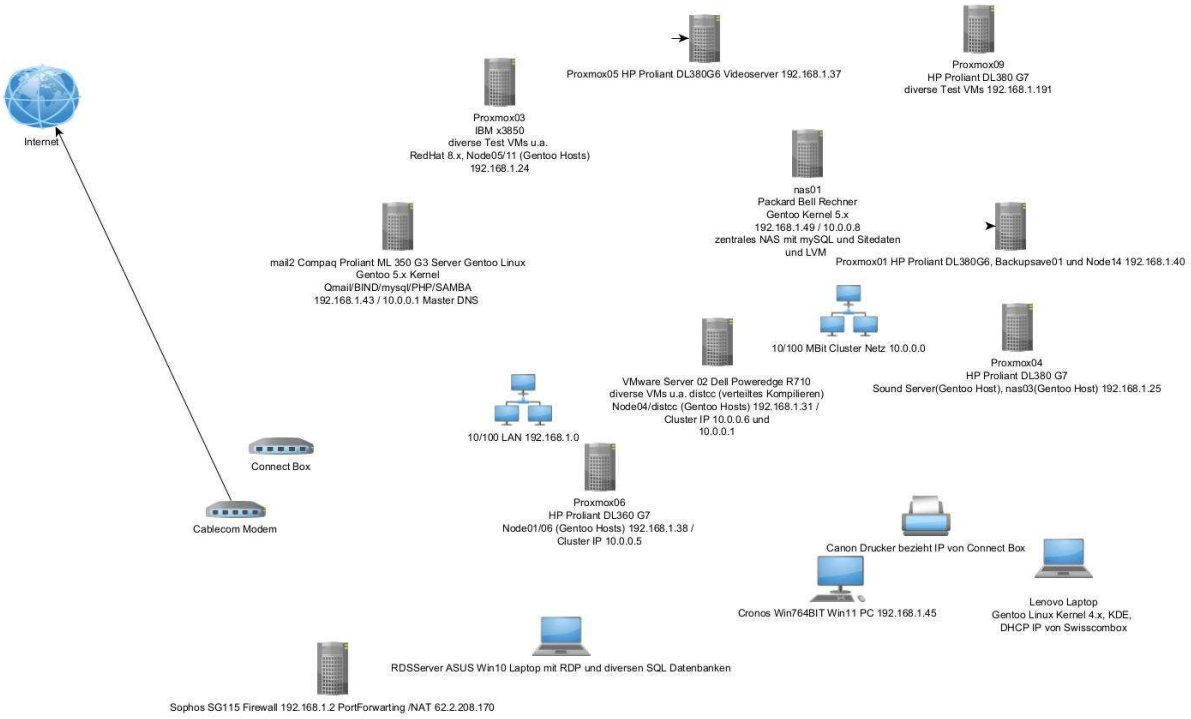
Aufbau privates Linux / Windows Netzwerk „Webtown“

Während meiner berufsbegleitenden Ausbildung zum Webmaster SIZ (die ich Ende 2001 erfolgreich abschloss) bin ich das erste Mal mit Linux in Berührung gekommen und war so begeistert davon, nicht zuletzt auch, weil es sehr stabil läuft und dank Open Source frei verfügbar ist, dass ich beschloss, mich damit näher auseinanderzusetzen.

Und so entstand das Netzwerk „Webtown“, welches wie folgt aufgebaut ist:

Grobschema:



Funktionsweise:

Erfolgt vom Internet über die öffentliche Cablecom IP Adresse 62.2.208.170 eine Anfrage beispielsweise auf den Web Port 80 dann wird diese durch die CISCO ISA 550 Firewall (neu Sophos) mit Hilfe von Port Forwarding an das interne Netzwerk bzw. an einen der Server weitergeleitet, wo der Apache Webserver 2.22 (installiert auf den Nodes 1,4,5,6,9,10 und Node14) dank Virtual Hosting können auf dem gleichen Server mehrere Webseiten betrieben werden, der Apache kümmert sich dann um die Datenlieferung) dann auf die Anfrage reagiert und den Inhalt bzw. die Webseite bereitstellt. Neu werden alle Anfragen direkt auf den Varnish Proxy Server weitergeleitet (der als Gentoo VM auf dem Videoserver installiert ist) der als Web Beschleuniger funktioniert und vorallem bei den Videos auf der DJ Site für eine Performanceverbesserung sorgt.

Um das Netzwerk effektiv vor Angriffen zu schützen, wurde auch Network Address Translation kurz NAT bzw. Masquerading aktiviert, sodass dieses von „aussen“ her nicht sichtbar ist, zumal private Adressen im Internet nicht routbar sind.

Weiter werden Angriffe zusätzlich durch ein integriertes Intrusion Prevention System direkt auf der Firewall abgewehrt.

Des Weiteren wurden nur die allerwichtigsten Ports aktiviert. Und auch die Firewall Regeln sind sehr restriktiv eingestellt und lassen zum Beispiel nur gewisse IP Bereiche zu, die in erster Linie zur Remote Verwaltung der Server via Smartphone dienen.

Denn je weniger auf einer Firewall „offen“ ist, je sicherer ist diese und sorgt so für einen effektiven Schutz.

Da auf den Apache 2.22 Servern (Node01, Node04, Node06, Node08, Node09, Node10, Node11, Node14) ebenfalls mehrere private Webseiten gespeichert sind, ist auch der BIND DNS aktiviert, der die korrekte Namenslauflösung zum Beispiel von http://www.elvisaltherr.ch/ oder z.B. www.djmcel.ch etc. übernimmt.

Alle Seiten basieren auf einem MySQL (neu Maria DB) /PHP gestützten Open Source Content Management System (Website Baker), welches mir ermöglicht, die Seiten direkt im Webbrowser anzupassen.

Die Gästebücher der jeweiligen Webseiten basieren auf Perl Skripten die ich als „Vorlage“ vom Internet heruntergeladen und für meine Zwecke (Name etc.) entsprechend angepasst habe. Des Weiteren läuft auf den Apache Webservern auch eine PHP 5.5.22 Engine, damit z.B. PHP in HTML direkt eingebettet werden kann und so Webseiten mit Datenbank-anbindungen realisiert werden können. Diese Skripte habe ich jeweils auch vom Internet runtergeladen und für meine Umgebung customized.

Die Mailzustellung übernimmt das sehr zuverlässige Software Paket Qmail.

Und dank Clamav und Spamassassin wird sowohl der eingehende als auch ausgehende Mailverkehr zuverlässig auf Spam und Viren geprüft und gegeben falls die SMTP-Verbindung unterbrochen, wenn ein Fund vorliegt.

Kürzlich wurden 2 neue Gentoo Hosts ins Netzwerk integriert. Und zwar einerseits ein „NAS“ wo sämtliche Word/Excel Files sowie die Datenbanken und die Webseiten gespeichert sind (und dank LVM bin ich sehr flexibel was die Diskgrösse betrifft, sprich ich kann die logischen Volumes im laufenden Betrieb ggf. anpassen, falls nötig) und ein 2. „NAS“ Server (ebenfalls Gentoo Linux) der ggf. die Services vom nas01 übernehmen kann. (kein aktives Failover, Cold Standby, d.h. die Umschaltung muss manuell erfolgen).

Um auf die Daten (Word und Excel) auf dem nas01 zugreifen zu können, wird dort der SAMBA Daemon betrieben, der windowsähnliche File und Druckdienste zur Verfügung stellt, sodass via PC bequem und ohne Konvertierung direkt auf die Daten (primär Word und Excel Dateien) zugegriffen werden kann.

Auch dieser Dienst ist natürlich so restriktiv wie möglich eingestellt und lässt zum Beispiel nur das interne Netzwerk 192.168.1.0 zum Zugriff zu.

Mit Hilfe von Corosync /Pacemaker (einer Open Source High Availability Lösung) wird ein Failover Szenario realisiert, das heisst, wenn einer der Server ausfällt, übernimmt automatisch der zweite Server dessen Aufgabe. Neu wird das Clustering von mehreren Gentoo Linux VMs (Node01, Node04, Node06, Node09, Node10, Node12,Node14) auf dem HP, dem Dell und dem IBM Server übernommen, d.h. auf den Servern sind mehrere Gentoo VMs installiert die untereinander das aktive (Failover) Clustering übernehmen.

Aus sicherheitstechnischen Gründen wurde dafür eigens ein separates «Cluster Netzwerk» 10.0.0.x/24 verwendet.

Weiter befinden sich ein Windows 11 PC (auf dem, zur Remoteverwaltung der Server, unter anderem das Freeware Tool „Putty“ sowie MS RDP Dienste installiert sind) sowie ein Canon Color Laser (der die IP via DHCP vom Swisscom Router bezieht).*Neu dazugekommen ist auch ein Lenovo Laptop, auf welchem Ubuntu Linux läuft mit KDE als Desktop der die IP vom DHCP auf dem Swisscom Router bezieht .Mit diesem Laptop nehme ich als Mitglied so oft es geht am Vereinstreffen im RUUM42 (Linux Verein) teil. Diese Treffen sind sehr interessant und ich kann ich mein Wissen speziell im Linux Umfeld à jour halten.*

Dank Linux läuft das Netzwerk sehr stabil und zuverlässig und praktisch rund um die Uhr, ausser wenn, zwecks Desaster Recovery, ein Backup der Maschinen erstellt wird, dann sind diese (aber immer nur einer der Server) offline. Damit aber die Webseiten jederzeit erreichbar sind wird das Backup wie gesagt gestaffelt durchgeführt und darauf geachtet, dass im Cluster immer mindestens ein Node online ist, bzw. dank Corosync/Pacemaker werden die Ressourcen (Cluster IP 10.0.0.3) sowie der Apache Webserver automatisch auf die anderen aktiven Nodes verschoben und so sind die Webseiten unterbruchsfrei erreichbar.

Um Sicherheitsrisiken weiter zu minimieren, werden auf allen Servern die Software Pakete regelmässig geupdatet und auch mehrmals ein Rootkit- und Virenscan durchgeführt, um allfällige Infektionen vor dem Ausbrechen zu erkennen und zu eliminieren.

Und auch der Linux Kernel wird aus Sicherheitsgründen à jour gehalten, sprich, wenn Sicherheitsupdates veröffentlicht werden, werden diese dann jeweils zeitnah eingespielt.

Nebst dem Firewall eigene Intrusion Prevention System wird auf allen Servern auch OSSEC Software IDS eingesetzt, welches Attacken, die die Firewall nicht erkennt, zuverlässig abwehrt, bzw. eine Meldung an den Serveradmin zur weiteren Bearbeitung sendet. Das Tool habe ich aus den Sourcen kompiliert, damit ich es optimal auf die jeweilige Hardware anpassen konnte und die Serverperformance nicht leidet. Dasselbe gilt für den Apache Webserver (2.22) und PHP(5.5.22) sowie Perl.

Neu ist auch ein IBM x3850 M2 Server (mit einer Dual Xeon CPU, 500 GB Diskspace und 32 GB RAM) im Netzwerk eingebunden, auf welchem ein IBM branded Win2008R2 Server mit Hyper-V (neu ist ebenfalls Proxmox installiert, da die Lizenz vom Windows abgelaufen ist) und mehreren virtuellen Maschinen läuft (2 Win2012R2/2016 VMs mit Citrix Virtual Apps/Delivery Controller eine *Kubernetes (Cent OS 7.0) VM* (Cent OS 7.0), und eine OpenShift (Cent OS 7) sowie eine Puppet (Debian 10.4.0) und eine Docker (Cent OS 7) sowie eine Ansible (Cent OS7) und eine **RedHat** sowie eine Windows 2016 Server VM (ein kleiner

AD Domain Controller inkl. Druck/Filediensten, DHCP und DNS) und eine **Ansible (Cent OS) VM.**

Ebenso wurde kürzlich ein HP Proliant DL360 G7 Server (ebenfalls mit einer Dual Xeon CPU, 500 GB Diskspace und 64 GB RAM (neu 72 GB da ich dort die Node01 VM betreibe und die grosse Mühe bei den Videos hat) , wo ich kürzlich auch die Diskkapazität von 300 GB auf 900 GB erhöht habe und dank Hot-Swap ging das im laufenden Betrieb ins Netzwerk eingebunden, auf dem Vmware/ESXi 6.7 läuft und mehrere virtuelle Maschinen u.a. 1 Windows 2016 AD Controller (DC), eine Solaris 11.4 VM, 1 WINDOWS 10 Client sowie ein qmail Reserve Server (speichert die Mails zwischen und schickt diese wenn der Mail2 wieder online ist) und eine Distcc Umgebung, die über mehrere Rechner verteiltes (und so die Zeitspanne zur Erstellung von Linux Binarys drastisch verkürzt) Kompilieren ermöglicht. Pro Architektur (I386 oder x64) gibt es eine separate VM und zu Testzwecken wurde noch eine Apache (Ubuntu 20.04) Test VM sowie ein Windows 10 Client (der sich mit dem Active Directory auf der Win2016 VM auf dem IBM verbindet) leider ist die Vmware Umgebung auf dem HP komplett abgestürzt und ich habe daher ebenfalls auf Proxmox gewechselt welches viel einfacher ist von der Bedienung. Auf diesem Server läuft auch **eine OpenShift VM (CentOS7)**

Neu ist auch ein HP Proliant ML350p G8 Server im Netzwerk eingebunden (bei dem ich kürzlich ebenfalls die Diskkapazität ausgebaut habe damit ich genug Platz für Test VMs habe), den ich von einem Vereinskollegen gratis bekam, worauf ebenfalls Vmware/ESXi 6.7.0 installiert ist und eine Oracle 12c Datenbank, eine PostgreSQL DB (Cent OS 7 VM), eine RH 8.0 und Ubuntu 18.0.4 und ebenfalls eine FreeBSD sowie eine **Python (Ubuntu)** und JSON (Cent OS 7) und SAP (open SUSE) sowie eine Kubernetes Node (Cent OS 7) und ngix (Ubuntu 20.04) und Ansible (Debian 10.04) und eine Apache Tomcat (Gentoo) Java Instanz und eine Elasticsearch (CentOS 7) und eine JBoss (CentOS 7) sowie eine Varnish VM (Cent OS 7) und eine **Rocky 9 und Ruby on Rails VM laufen.**

Leider ist der Server definitiv kaputt was ich sehr schade finde der war auch sehr schnell sprich ich werde den gelegentlich austauschen.

Anstelle des defekten HPs ist nun ein Dell PowerEdge R710 Server mit einer Dual Xeon CPU sowie 2 TB Diskspace und 32 GB RAM im Einsatz, d.h. die VMs laufen nun auf dem neuen Server.

Kürzlich ist ein HP Proliant DL380G7 Server mit einer Single Xeon CPU, 12 GB RAM und 300 GB Diskspace online gegangen. Dieser Server dient in erster Linie als Soundserver, d.h. dort drauf sind die Remixes von der DJ Webseite (ein Hobby von mir) gespeichert, gleichzeitig sorgt ein Varnish Proxy der dem Apache Server vorgeschaltet ist für eine hohe Performance.

Auf dem Server läuft auch das nas03 (Gentoo VM) das wie das nas02 cold standby ist und nur zum Einsatz kommt wenn sowohl das nas01 als auch das nas02 nicht online sind.

Leider ist der alte Dell Rechner (Nas02) kürzlich ausgestiegen und als Ersatz ist nun ein HP Proliant ML350G8 Server im Einsatz mit einer Single Xeon CPU, 16 GB RAM und 300 GB HD Kapazität. Dort ist ebenfalls Proxmox installiert und das «Nas02» läuft als VM drauf.

Da die Videoperformance der Videos auf der DJ Webseite schlecht war wurde dafür eigens ein HP Proliant DL380G6 Server angeschafft ebenfalls mit einer Single Xeon CPU, 16 GB RAM und rund 4 TB Diskkapazität. Dasselbe gilt für die Remixe. (neu hat der Server doppelt soviel RAM also 32 GB da eben die Videoperformance vorallem auf dem Handy der DJ Webseite, (etwas was ich hobbymässig betreibe) nicht so gut war.

Als Windows10 RDS und SQL 2019 Server fungiert ein ASUS Laptop, auf dem diverse SQL-Datenbanken und .NET Applikationen (Eigenentwicklungen in C#) installiert sind und die RDP Dienste freigeschaltet sind.

Nebst VMware ist auch Proxmox 7.0 im Einsatz, eine Linux basierte Virtualisierungslösung, die ähnlich wie Vmware oder Hyper-V funktioniert. Aus technischen Gründen wurde diese auf dem EX – Nas02 Rechner (Maxdata PC) installiert, da der alte Dell Rechner (Pentium4) keine Hardware Virtualisierung ermöglicht. Auf dem Rechner laufen mehrere FreeBSD VMs und eine varnish (Ubuntu 20.04) Test VM.

Leider ist der Maxdata PC kürzlich komplett ausgestiegen und daher läuft das Ganze nun auf einem HP Proliant DL380G6 Server mit einer Single Xeon CPU, 16 GB RAM und rund 1 TB Diskkapazität worauf der Node08 (Gentoo Host) sowie der Backupsave (Gentoo Host) und eine Squid Cache (Gentoo Host) VM läuft.

Für weitere Test VMs (RedHat und andere) und für die Uebungen des RHCSA Kurses habe ich kürzlich erneut einen DL380 G7 angeschafft mit einer Single Xeon CPU, 12 GB RAM und 446 GB Diskspace. Dort laufen wie gesagt diverse Test VMs ohne speziellen Funktionen aber um die Uebungen im Kurs direkt «live» durchspielen zu können

Und die VMs auf den HP Servern und dem Dell Server werden mit VEEAM Backup & Replication Version 9.5 gesichert (Snapshot Verfahren). Leider lässt aber die Free Version nur die Sicherung von maximal 3 VMs zu, daher werden die Server noch separat mit Acronis gesichert für alle Fälle.

Das Ganze wird von Zabbix überwacht, welches bei Ausfall eines Services jeweils eine Fehlermeldung per Mail oder per SMS verschickt.

Dieses Wissen kam mir beispielsweise beim labor team w ag sehr zugute, wo ich unter anderem mitverantwortlich für die Betreuung der Linux Server und der Oracle Datenbanken war.

Statt der CISCO ISA 550 Firewall wird neu eine Sophos SG115 Firewall (ebenfalls eine Hardwarebox) verwendet, da das IDS auf der CISCO nicht mehr weiterentwickelt wurde, die in etwa die gleichen Funktionen wie die CISCO bereitstellt, jedoch auch über Advanced Protection usw. verfügt, welches noch einen Schritt weitergeht in Sachen Bekämpfung von aktuellen Bedrohungen wie Zero Day Attacken etc.