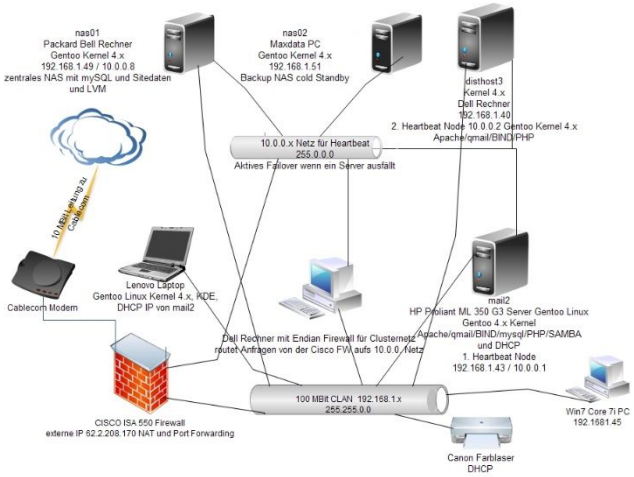
Aufbau privates Linux Netzwerk „Webtown“

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 Linux - 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 mit Hilfe von Port Forwarding auf das interne Netzwerk weitergeleitet.

Um das Netzwerk effektiv vor Angriffen zu schützen, wurde auch Network Adress Translation kurz NAT aktiviert, sodass dieses von „aussen“ her nicht sichtbar ist. Weiter werden Angriffe zusätzlich durch ein integriertes Intrusion Prevention System 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 Be-reiche 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 beiden Servern (mail2 und disthost3) ebenfalls mehrere private Webseiten gespeichert sind, ist auch der BIND Server Dienst aktiviert, der die korrekte Namenslauflösung zum Beispiel von www.elvisaltherr.ch oder www.paint-creations.ch übernimmt.

Alle Seiten basieren auf einem MySQL gestützten Open Source Content Management System, welches mir ermöglicht, die Seiten direkt im Webbrowser anzupassen.

Die Mailzustellung (die ebenfalls auf beiden Maschinen identisch konfiguriert ist) 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.

Neu wurden kürzlich 2 neue Gentoo Hosts ins Netzwerk integriert. Und zwar einerseits ein „NAS“ wo sämtliche Word/Excel Files gespeichert sind und ein 2. „NAS“ Server (ebenfalls Gentoo Linux) der ggf. die Services vom nas01 übernehmen kann. (kein aktives Failover)

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 Ver-fügung stellt, sodass via PC bequem und ohne Konvertierung direkt auf die Daten 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.

Damit eine hohe Verfügbarkeit und Ausfallsicherheit erreicht wird, wurde auch ein zweiter Rechner, namens disthost3 ins Netzwerk integriert, der ausser SAMBA, identische Dienste wie DNS/Mail und Web anbietet.

Mit Hilfe von Heartbeat (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.

Aus sicherheitstechnischen Gründen wurde dafür eigens ein separates Cluster Netzwerk 10.0.0.0 verwendet.

Das „Cluster“ Netzwerk ist durch eine separate Firewall abgesichert, die auf einem Dell Rechner läuft, auf welchem die „Endian“ Software Firewall Lösung installiert ist. So ist gewährleistet, dass nur jeweils ein aktiver Node im Clusterverbund auf die Requests aus dem Internet antwortet und gleichzeitig treten auch keine Kollisionen mit dem bestehenden C - Class Netzwerk 192.168.1.0 auf, da dieses separat abgeschottet ist.

Weiter befinden sich ein Windows 7 PC (auf dem, zur Remoteverwaltung der beiden Server, unter anderem das Freeware Tool „Putty“ installiert ist) sowie ein Canon Color Laser, der die IP-Adresse vom DHCP Dienst auf dem Mail2 bezieht, im Netzwerk. *Neu dazugekommen ist auch ein Lenovo Laptop, auf welchem Ubuntu Linux läuft mit KDE als Desktop und welches ebenfalls die IP vom DHCP auf dem mail2 bezieht. Mit diesem Laptop nehme ich als aktives*

Mitglied regelmässig an den „Linux Usergroup“ Treffen 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 gestaffelt durchgeführt.

Um Sicherheitsrisiken weiter zu minimieren, werden auf beiden 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.

Zu Testzwecken habe ich auf dem Mail2 noch qemu installiert, ein **Open Source Hypervisor, mit dem ich, wie z.B. mit VMware, mehrere virtuelle Server auf der gleichen physischen Maschine betreiben kann sowie auf dem disthost3 Tomcat ein Java Apache Webserver**

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

http://www.elvisaltherr.ch/nagios

Username+Passwort : Auf Anfrage

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.