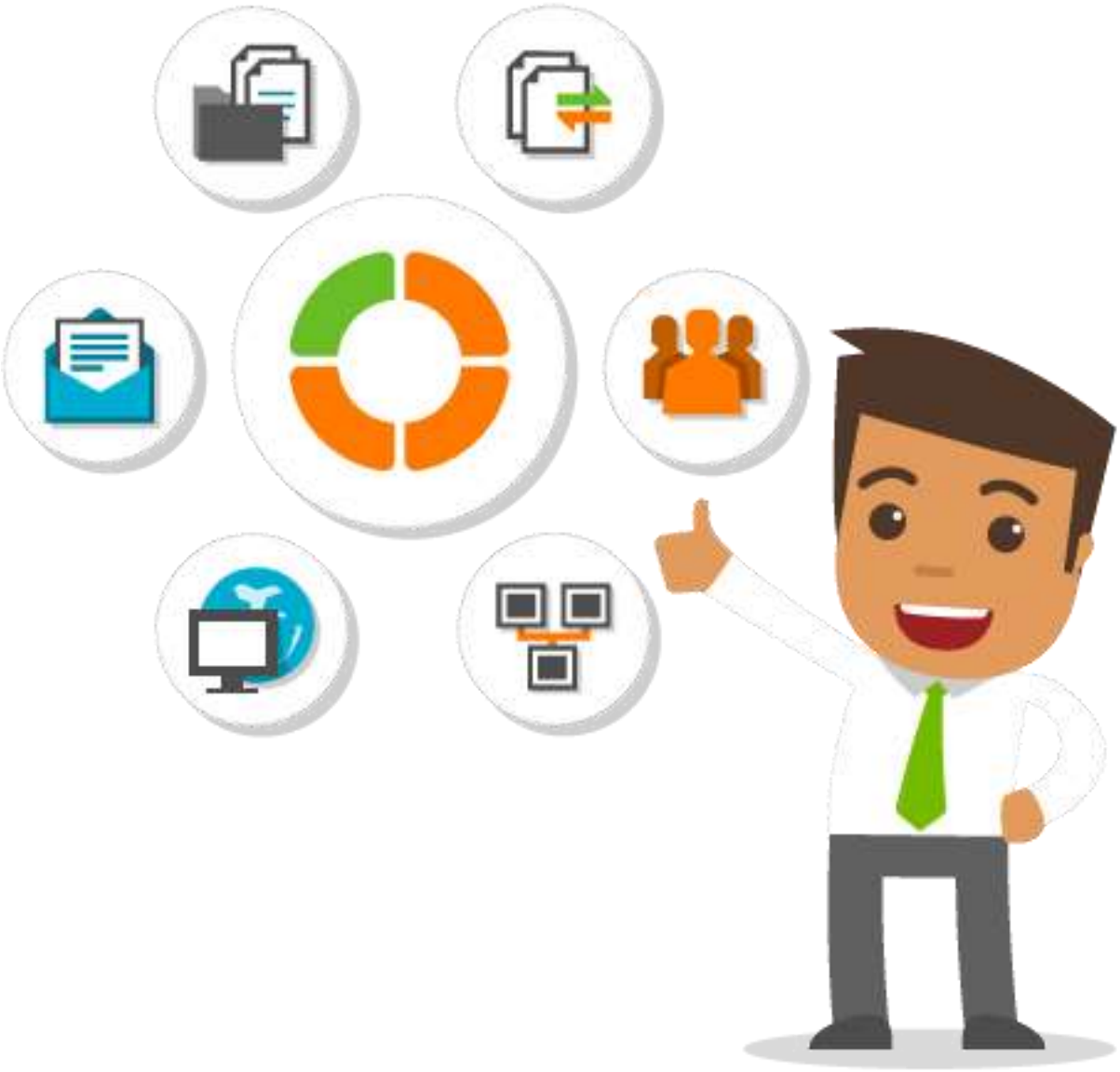


Aufbau eines zentralisierten Firmennetzwerkes mit einem Zentyal Server 4.0

DOKUMENTATION

Fabian Horst | IT-12 / Flensburg | 30. März 2015

Persönliche Erklärung:
Ich versichere, dass ich das Projekt und die dazugehörigen Dokumente selbstständig erstellt habe.

Flensburg 30.03.2015 _____
Ort, Datum Unterschrift des Prüfungsteilnehmers

Inhalt

1.0 Einleitung

Ich bin seit dem 01.05.2012 bei der absolutnet. UG Auszubildender zum IT-Systemelektroniker. Das Hauptgeschäftsfeld der absolutnet sind Webentwicklung, Marketing & Design für kleine Unternehmen und den Mittelstand. Ich bin hauptsächlich für die IT-Betreuung und die Webserver im Einsatz und unterstütze die Grafikerin und den Webdesigner bei allen Fragen rund um Ihre Projekte. Neben der Agenturtätigkeit bieten wir auch IT-Services und Support für Unternehmen sowie Privatkunden an.

Im gleichen Büro ist auch die Förde-Betriebs GmbH untergebracht, die im Gastronomie- und Handwerksbereich tätig ist. Beide Gesellschaften haben denselben Geschäftsführer, so dass ich auch diese Firma betreue.

Diese Dokumentation ist aus Datenschutzgründen mit Platzhaltern anstatt echten Daten versehen. Außerdem sind nicht unbedingt bekannte Begriffe **fett** markiert und im Glossar aufgeführt.

2.0 Projektbeschreibung

Hier wird das von mir bearbeitete Projekt beschrieben.

2.1 Projektanlass

In der absolutnet wurde seit Jahren ein Linux Server mit Dateifreigaben in einer Windows Arbeitsgruppenstruktur mit Windows 7 und 8 Clients genutzt. Der Server stellte gemeinsam genutzte Dateien im Netzwerk bereit. Eine Zugriffskontrolle bestand nur rudimentär. Die alte Hardware und die damit verbundenen Performanceengpässe, der hohe Pflegeaufwand und die aufwendige Rechtevergabe im Arbeitsgruppenmodus machten ein Überdenken der Lösung notwendig. Aufgrund der genannten Schwierigkeiten mit der bisherigen Lösung wurde entschieden, auf ein zentral verwaltetes Windows Domänen bzw. Active Directory Netzwerkmodell zu wechseln. Um Kosten zu sparen sollten dabei alternative, Linux-basierende Lösungen zum Einsatz kommen.

2.2 Projektziele

- Die Dateifreigaben der Firma und Benutzerkonten sollen auf einem Server zentral gespeichert und gewartet werden.

- Die Verwaltung der Freigaben und der Nutzer soll möglichst von technisch nicht versiertem Personal ausgeführt werden können.

- Die Möglichkeit der Bündelung von verschiedenen Internetzugängen um die Geschwindigkeit zu erhöhen und Ausfälle zu vermeiden.

- Einrichten einer Firewall und eines transparenten Proxys mit Sperrlisten und Cache um einen sicheren und schnellen Internet Zugang für die Mitarbeiter zu ermöglichen und unerwünschte Seiten filtern zu können.

- Der Netzwerkschrank ist durch seine Bauart nicht schalldämmend und der verbaute Switch ist sehr laut. Der Schrank soll durch einen kleineren Schrank ersetzt werden der auch geräuschärmere Komponenten enthält.

- Durch den Einsatz von einem Server der im Dauerbetrieb ist sollen auch kleinere Maschinen virtualisiert und auf dem Server mit betrieben werden.

2.3 Ist-Zustand

In den Geschäftsräumen der absolutnet lag folgender Ist-Zustand vor:
- 1 Ubuntu Server 12.04 **LTS** mit **SAMBA** Dienst
- 3 Arbeitsplätze mit Windows 7 Home Premium für Geschäftsführer, Assistenz und Vertrieb
- 1 Arbeitsplatz mit Windows 7 Professional für den Auszubildenden
- Telekom **DSL** Zugang mit fester IP-Adresse und FritzBox 7270
- 19 Zoll Netzwerkschrank mit Lochblech-Tür und Managed 10/100 Switch

2.4 Soll-Analyse

Aus den Anforderungen wurde der Soll-Zustand geplant:
- 1 Zentyal Server 4.0 mit **Silent** Hardware
- 5 Arbeitsplätze mit Windows 7 Professional
- 1 virtualisiertes Windows 7 Professional mit Lexware Financial Office Pro 2015
- 1 virtuelle Maschine mit Windows 7 Professional und Microsoft **RSAT** zur Domänenverwaltung
- Telekom **DSL** Zugang mit fester IP-Adresse und FritzBox 7270
- Kabel Deutschland Business Zugang mit Kabel Modem
- Kleiner Netzwerkschrank mit 2 passiven Gigabit Switchen

2.5 Zentyal Server 4.0

Als Server Betriebssystem hat bisher ein Ubuntu Server mit einem einfachen **SAMBA** Dienst die Aufgaben übernommen. Als Ersatz soll das ebenfalls auf Ubuntu Linux LTS basierende und als Open Source Software unter der **GPL-Lizenz** verfügbare Zentyal Small Business Server (Zentyal 4) eingesetzt werden. Für die Arbeit in unserem Unternehmen nutzen wir die Community Edition in der Version 4.0. Von den vielen Diensten, die mit Zentyal 4 realisiert werden können, wie z.B. **DNS**, **DHCP**, **IDS**, **NTP**, Webserver, **VLAN**, **VPN**, **AD**, **Firewall**, Gateway, **CUPS/Druckserver**, Mail-Server und **Proxy** sind nur wenige für das Projekt relevant. Trotzdem ist es wichtig, die Verfügbarkeit aller benötigten Dienste in der Lösung zu prüfen.

2.6 Entscheidungsfindung und Vergleich

Für die Software gibt es einige Lösungen die in Frage kommen würden. Die Entscheidungsfindung ließ die Wahl auf die Zentyal Lösung fallen.

Produkt	Preis[1]:	Benutzer anlegen	Sicherheit	Funktion	Anpassung	Lizenz	Erfahrung	Ergebnis[2]
Microsoft **Windows Server** 2012 R2 + 5 **CAL**	1938 €[3]	--	-	+	--	-- (Proprietär)	/	12
Zentyal 4.0 **CE**	0 €	++	+	++	++	++ (GPL v2)	++	29
ClearOS **CE**	0 €	/	/	++	+	++ (GPL v2)	--	21

[1] Nicht Bewertet
[2] Punkte: -- 1, - 2, / 3, + 4, ++ 5
[3] Siehe Angebot im Anhang

2.7 Hardwareauswahl

Die Hardware für den Server wurde aufgrund eines eingeschränkten Budgets direkt ausgewählt, da bereits eine Auswahl an Komponenten zur Verfügung stand, die die Auswahl stark einschränkten. Die **CPU** ist ein Intel i5 Quad-Core mit 6 MB Cache der 3ten Generation mit den beiden wichtigsten Funktionen für Virtualisierung. Insbesondere mit der VT-d Funktion wird es bei der Virtualisierung durch die verbesserten direkte I/O Leistung nicht sehr schnell eng. So sind Kapazitäten in Reserve wobei das Budget effektiv ausgenutzt wird.

Der Arbeitsspeicher ist mit 16 GB für einige virtuelle Maschinen ausreichend und kann noch auf 32 GB erweitert werden.

Die beiden Festplatten sind für den 24/7 Betrieb freigegeben und sind mit 2 TB für den Bedarf von 500 GB auch für die Zukunft noch einige Zeit ausreichend.

Die restlichen Komponenten sind möglichst günstig, energiesparend und geräuscharm ausgewählt worden. Der Server ist im Betrieb sehr leise und auch bei Stille kaum wahrzunehmen.

3.0 Durchführen des Projekts

Die Durchführung ist in 3 Abschnitte unterteilt:

3.1 Installation

Die Integrität des ISO-Images muss mit den Prüfsummen nach dem Download und dem Brennen überprüft werden. Die Installation wird via **ISO**-Image, das auf einen Rohling gebrannt worden ist, vom DVD-Laufwerk gestartet. Am Anfang wird der Experten Modus und die deutsche Sprache gewählt. Dann wird der Hostname, Benutzername und doppelt das Passwort für den Benutzer angegeben. Danach folgt die Partitionierung: Durch das Software **RAID** 1 über zwei Festplatten wird es hier ein wenig detailliert. Zuerst erstellen wir am Anfang von Festplatte 1 eine 500 MB große primäre Partition und setzten das „boot“ flag. Die Partition als /boot angeben und das Dateisystem auf EXT2 einstellen. Dann eine neue Partition mit ca. 2 GB, primär erstellen. Diese mit swap kennzeichnen. Dann die letzte Partition primär auf dem Restspeicherplatz anlegen und mit / kennzeichnen und EXT4 formatieren. Diese Schritte wiederholen sich auf der kompletten Festplatte 2 genauso. Dann wird mit dem Software Raid Konfigurator jeweils sda1 und sdb1 zu md0, sda2 sdb2 zu md1 und sda3 sdb3 zu md2 mit dem RAID Modus 1 und beiden Festplatten zusammen gefasst. Der Installer hat nun nur noch die md* Laufwerke und Installiert darauf das System. Während der Installation wird für die aktuellsten Pakete nach einem http-proxy gefragt den wir nicht benutzen und daher ohne zu ändern schließen. Bei der Nachfrage ob eine Grafische Oberfläche gewünscht wird beantworten wir dies mit ja da wir diese später für die Pflege benötigen. Nach einem Neustart kommen wird der Zentyal Desktop angezeigt. Dort wird sich mit dem Benutzernamen und Passwort eingeloggt und die benötigten Features gewählt:

- Domain Controller and File Sharing / Benötigt für AD und Dateifreigaben
- DNS-Server / Benötigt für die einfache Verwaltung der DNS Einträge
- DHCP-Server / Zum Verteilen der IP-Adressen
- Firewall / Zum Schützen und Verwalten der Sicherheit
- Certification Authority / Wird für die Zertifikate von VPN benötigt

- HTTP-Proxy / Wird für den Cache und die Filter benötigt
- Printers / Installiert den CUPS-Druckserver
- VPN / Wird für die nachträgliche Konfiguration von Tunneln in die Firma genutzt

Nach der Installation der Pakete beginnt die Konfiguration.

3.2 Konfiguration

Nach der Installation der Zentyal Module wird mit der Konfiguration fortgefahren. Als erstes werden die Netzwerkinterfaces zugewiesen. eth0 wird statisch[4] belegt und als extern markiert, eth1 wird mit statisch 192.168.1.1 belegt und als intern markiert. Sobald die Konfiguration gespeichert ist erscheint die Weboberfläche mit der eigentlichen Verwaltung des Zentyal Servers. Anschließend wird dort unter Netzwerk das zweite Gateway[5] und die Muster[6] für die Erkennung, ob die Verbindung über das Gateway noch verfügbar ist, hinzugefügt. Danach werden unter „Computergruppen“ die MAC-Adressen der Maschinen eingetragen die über **DHCP** immer die gleiche IP-Adresse bekommen sollen.

Domäne

Unter den Domänen Einstellungen werden noch die „Roaming Profiles“ / Servergespeicherten Profile aktiviert. Diese ermöglichen es den Rechnern in der Domäne die Benutzerdaten auf dem Server zu speichern. So können Mitarbeiter an verschiedenen Rechnern auf Ihre Daten und Einstellungen zugreifen.

Benutzer anlegen

Dann werden die Benutzer angelegt, zuerst ein Domänen Administrator der Rechner warten und hinzufügen kann. Mit diesem lassen sich dann die Rechner in die Domäne einbinden. Danach können die Benutzer und Gruppen angelegt werden. Die Gruppe „absolutnet“ wird angelegt und die 5 Nutzer der Gruppe zugewiesen.

Computer hinzufügen

Damit die Computer der Domäne angehören müssen sie mit dieser verbunden werden. Die Rechner mit Standard Windows 7 Professional werden in den Zentyal Netzwerkbereich gepatcht und mit **DHCP** mit Ihrer IP-Adresse versorgt. Über die Computer Einstellungen werden unter Zuhilfenahme des eingeloggten lokalen Administrator Accounts und dem Domänen Administrator Account werden die Computer der Domäne hinzugefügt. Nach einem Neustart können sich die Nutzer dann mit Ihrem Domänenaccount anmelden.

Dateifreigabe anlegen

Die Dateifreigaben werden über die Verwaltung erstellt und müssen die entsprechenden Rechte zugewiesen bekommen. Um dies möglichst einfach zu gestalten wurde bereits eine Gruppe für die Firma erstellt die Leserechte für die Freigabe erhält. Für Schreibrechte werden einzelne Nutzer direkt berechtigt.

Die Virtualisierungssoftware

Um den Server im 24/7 Betrieb noch effizienter zu gestalten sollen einzelne alte Maschinen virtualisiert werden. Der Lexware Server aus der Windows Arbeitsgruppe wird auf den freien Ressourcen des Servers als virtualisierte Maschine migriert und spart so Energie. Als

[4] IP: 192.168.178.254 Gateway: 192.168.178.1 Netzmaske: 255.255.255.0 DNS1: 8.8.8.8 DNS2: 8.8.4.4
[5] IP-Adresse: 192.168.178.2 Netzmaske: 255.255.255.0 DNS: 8.8.8.8, 8.8.4.4
[6] Ping: facebook.com, amazon.com, ebay.com, google.com & ping <100

Software wird dafür Virtual Box von Oracle verwendet. Dieses Software ist Open Source und unter **GPLv2** Lizensiert, das proprietäre Extension Pack was nur für die persönliche Verwendung freigegeben ist wird daher NICHT eingesetzt.

3.3 Testphase und Übergabe

In der Testphase wurden 3 virtuelle Maschinen auf der Maschine gestartet und in die Domäne hinzugefügt. Die Freigaben wurden getestet und auch die Benutzer Accounts zwischen den Maschinen oft gewechselt. Durch den Proxy funktionierte die Internetverbindung problemlos. Nach dem die gesamten Anforderungen erfolgreich getestet wurden ist die Anlage in den Betrieb übergegangen.

3.4 Probleme und Lösung

Nach der Installation war die Tastatureingabesprache auf Englisch eingestellt und nicht wie in der Installation auf Deutsch. Durch Sonderzeichen im Passwort war es so nicht möglich nach dem bedruckten Layout zu tippen. Beim Umschalten auf eine andere Konsole z.B. mit der Tastenkombination STRG+ALT+F1 kann mit dem Befehl setxkbmap die Sprache angepasst werden. Dieses wurde durch einen **Cronjob** beim Start endgültig behoben.

Beim Einspielen von Daten konnte der Datenträger nicht eingehängt werden. Um diesen Fehler zu beheben musste der NTFS Treiber für Linux nachträglich installiert werden. Dies wurde über die Konsole mit: „sudo apt-get install ntfs3g“ sehr schnell behoben.

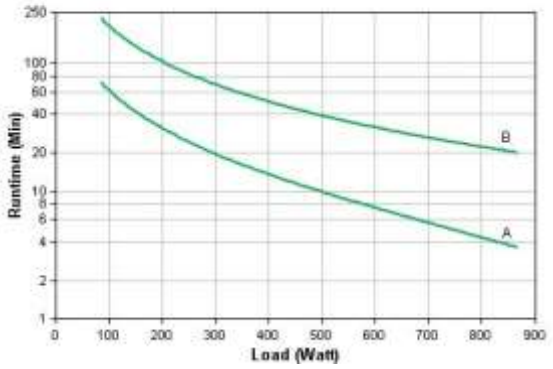
Die 3 Kernel Module für VirtualBox wurden nicht korrekt installiert und die Maschinen lassen sich nicht erstellen. Um dieses Problem zu beheben werden die Erweiterungen einfach mit „sudo apt-get install virtualbox-dkms“ nachinstalliert.

In einer vorherigen Zentyal Version war noch ein Modul für USV und Backup vorhanden. In diesem Projekt waren Backup und USV jedoch eingeplant und müssen nun anders umgesetzt werden. Das dateibasierte Backup wird nun mit einem Script auf einen **SFTP** Server in ein Rechenzentrum kopiert und dort in einem Wechselplan in 7 Tage versioniert gespeichert. Die USV ist aus Kostengründen nicht umsetzbar und ist daher nur technisch geplant. Mit 1500 VA und einem 500 Watt Netzteil im Server ist bei Vollauslastung eine Laufzeit von 10 Minuten erreichbar. Bei einem Test brauchte der Server im Durchschnitt ca. 3 Minuten um die virtuellen Maschinen und sich selbst herunterzufahren. Um Verschleiß auszugleichen und eine Reserve zu haben ist an der USV noch eine optionale Akkuerweiterung eingeplant die bei 500 Watt Last bis zu 60 Minuten überbrücken kann und auch Router, Switch, Kabelmodem und Monitor mit versorgen kann.

Extended Run Options — APC Power-Saving Back-UPS Pro 1500, 230V

Runtime Graph

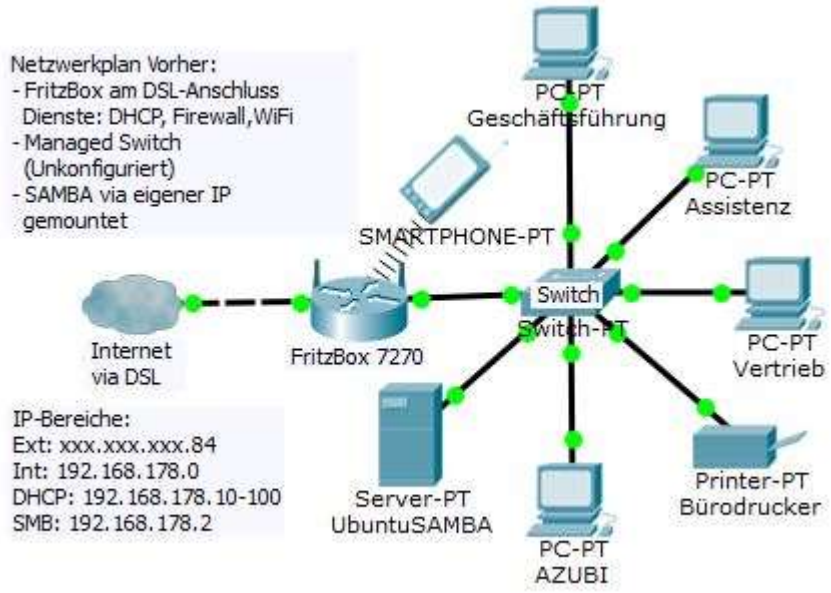
Curve	Part Number(s)
A	BR1500GI
B	BR1500GI + (1)BR24BPG



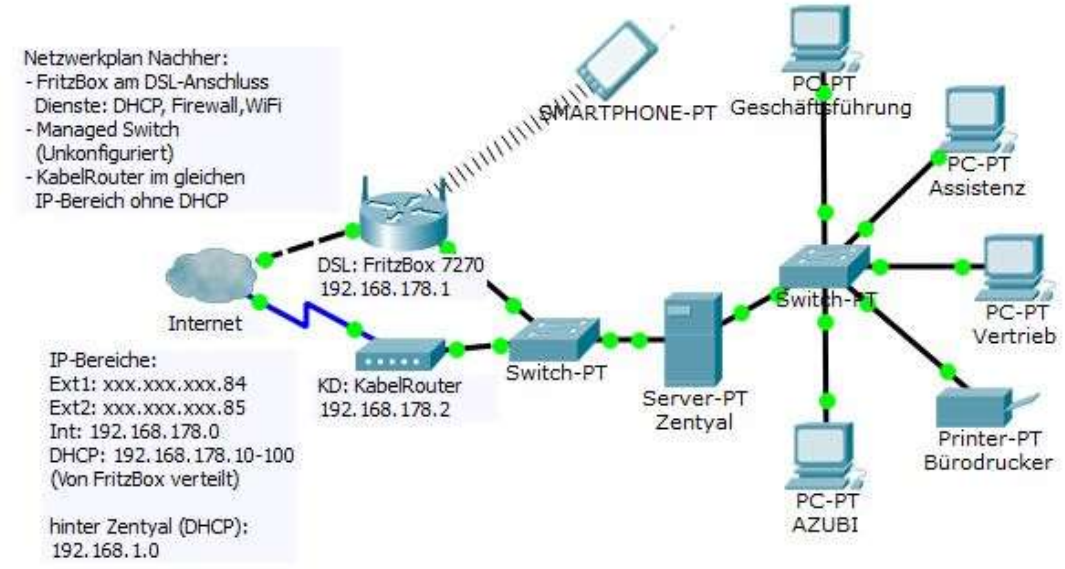
4.0 Anhang

4.1 Netzwerkpläne

Netzwerkplan Vorher:

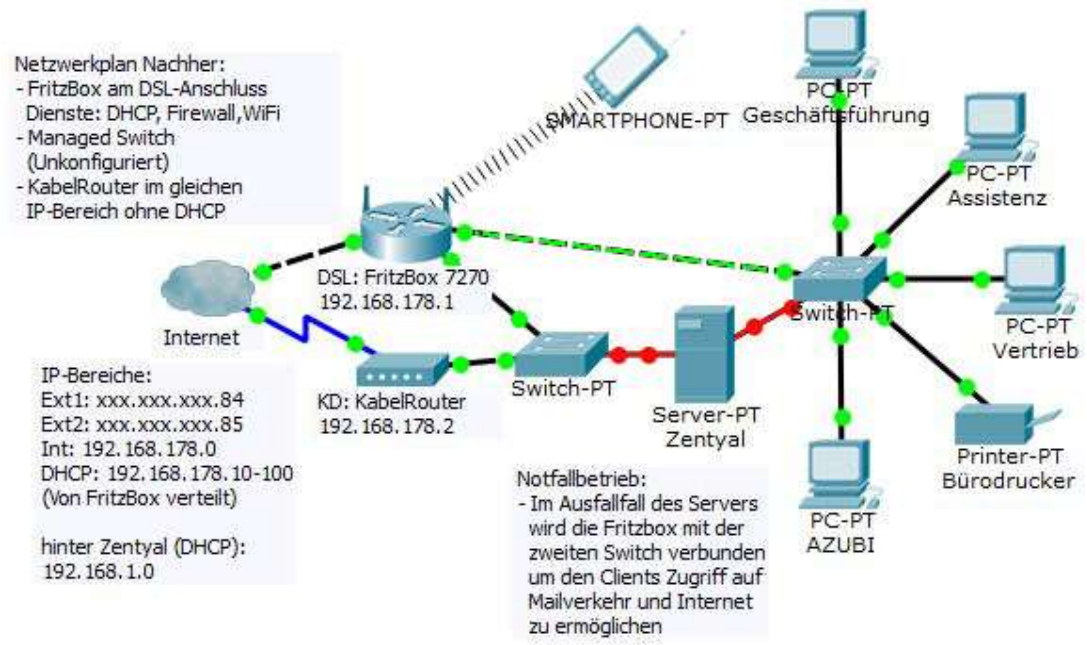


Netzwerkplan Nachher:



4.2 Notfallplan

Für den Fall eines Serverausfalls im Gateway Betrieb wäre eine Kommunikation mit dem Internet für die Clients nicht möglich. Um möglichst schnell an z.B. E-Mails und Informationen zu kommen ist durch einen manuellen Eingriff am Patchfeld ein Notfallbetrieb möglich, dieser bietet sich natürlich auch zur Wartung an. Hierbei wird ein Kabel zwischen dem kleinen Switch von der FritzBox und dem Kabel Modem zu dem Switch für die Clients gesteckt. Dadurch verteilt die FritzBox ihren eigenen **DHCP** Bereich an die Clients und ermöglicht zumindest rudimentäre Zugriffe auf Onlinedienste. Für diesen Fall ist bereits ein beschriftetes Kabel vorbereitet, dieses muss nach dem Überbrücken natürlich wieder entfernt werden da sonst zwei **DHCP** Server gleichzeitig im Netzwerk Adressen verschiedener Bereiche verteilen würden.



4.3 Abbildungen und Quellen

Deckblatt: http://www.zentyal.com/wp-content/themes/zentyalcom-2012/images/sbs/sbs.png

4.1 Vorher/Nachher: Cisco Paket Tracer Scenario

4.2 Notfallplan: Cisco Paket Tracer Scenario, GIMP editiert

3.4 APC USV:
http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=BR1500GI&total_watts=200

Angebot Microsoft Server: IT-Kontor GmbH & Co. KG, Flensburg

4.6 Glossar

AD – Active Directory ist der Verzeichnisdienst von Microsoft Windows Servern

CPU – Ist ein Prozessort oder eine elektronische Schaltung

Cronjob – Automatisierte zeitbasierte Ausführung von Prozessen

CUPS – Common Unix Printing System ist ein Druckerserver für unixioden Systeme

DHCP – Dynamic Host Configuration Protocol / Automatische IP-Adressverteilung

DNS – Domain Name System / Namensauflösung

DSL – Digital Subscriber Line / Übertragungsstandard für Daten / Internetanschluss

Firewall – Brandschutzmauer / Sicherungssystem für Computernetze

Gateway – Vermittlungsgerät zwischen Netzwerken

GPL-Lizenz – Weit verbreitete Software Lizenz für kostenfreie und änderbare Software

IDS – Intrusion Detektion System / Erkennungen von Angriffen

ISO – Abbild eines Datenträgers im ISO9660 Format

LTS – Long Term Support / Lange gepflegte Version

NTP – Network Time Protocol / Zeitsynchronisation über das Netzwerk

PROXY – Vermittlung zwischen Netzbereichen, Filtermöglichkeiten

RAID - Redundant Array of Independent Disks / Zusammenfassen von Datenträgern

RSAT - Remote Server Administration Tools / Tool für AD/Domänenverwaltung

SAMBA – Freie Verwendung von AD und Dateifreigaben und nicht Microsoft Systemen

SFTP - Secure File Transfer Protocol / Übertragen von Dateien über SSH Verbindung

Silent – Still / möglichst leise

USV – Unterbrechungsfreie Stromversorgung

VLAN - Virtual Local Area Network / Aufteilung von physikalischen Leitungen

VPN – Virtual Private Network / Verschlüsselte Tunnel