

Aufgabe 1.2

Sicheres Mailsystem mit WAN Anbindung

Zu realisieren ist die Infrastruktur für sicheres e-mail. Mail soll sowohl im internen Netz, als auch über das Internet zu den Kunden realisiert werden können. Es wird angenommen, das e-mail unternehmenskritisch ist, und daher möglichst ausfallsicher realisiert werden muss. Das Unternehmen verfügt über verschiedene Niederlassungen, die mittels VPN Lösungen miteinander verbunden sind. Die Niederlassungen befinden sich in Mainz (Zentrale mit 120 Mitarbeitern), Hamburg (15 Mitarbeiter), Stuttgart (7 Mitarbeiter) und Dortmund (5 Mitarbeiter).

Auf Grund der Priorisierung wurde Mainz als zentraler IT Standort ausgewählt. Dort sind die meisten Mitarbeiter beschäftigt (120 MA).

Standort Mainz :

Die IT Zentrale des Unternehmens befindet sich an dem Standort, an dem sich die meisten Mitarbeiter konzentrieren. Dort befindet sich die gesamte e-mail Technologie. Im Grundprinzip sind dort Mailserver Cluster aufgestellt, getrennt in Empfang von externen Mails und Senden/Empfangen interner e-mails. Das Mailserver Cluster, das die Mails von extern empfängt, befindet sich in einer Demilitarisierten Zone (DMZ), da von extern möglicherweise schädlicher Code in das Unternehmen „geschickt“ werden kann. Das empfangene Mailcluster prüft erst jede eingegangene e-mail auf Viren, Trojaner etc. und spürt Spam etc auf. Eine DMZ ist notwendig, um mögliche Gefährdungen vom LAN des Unternehmens fernzuhalten.

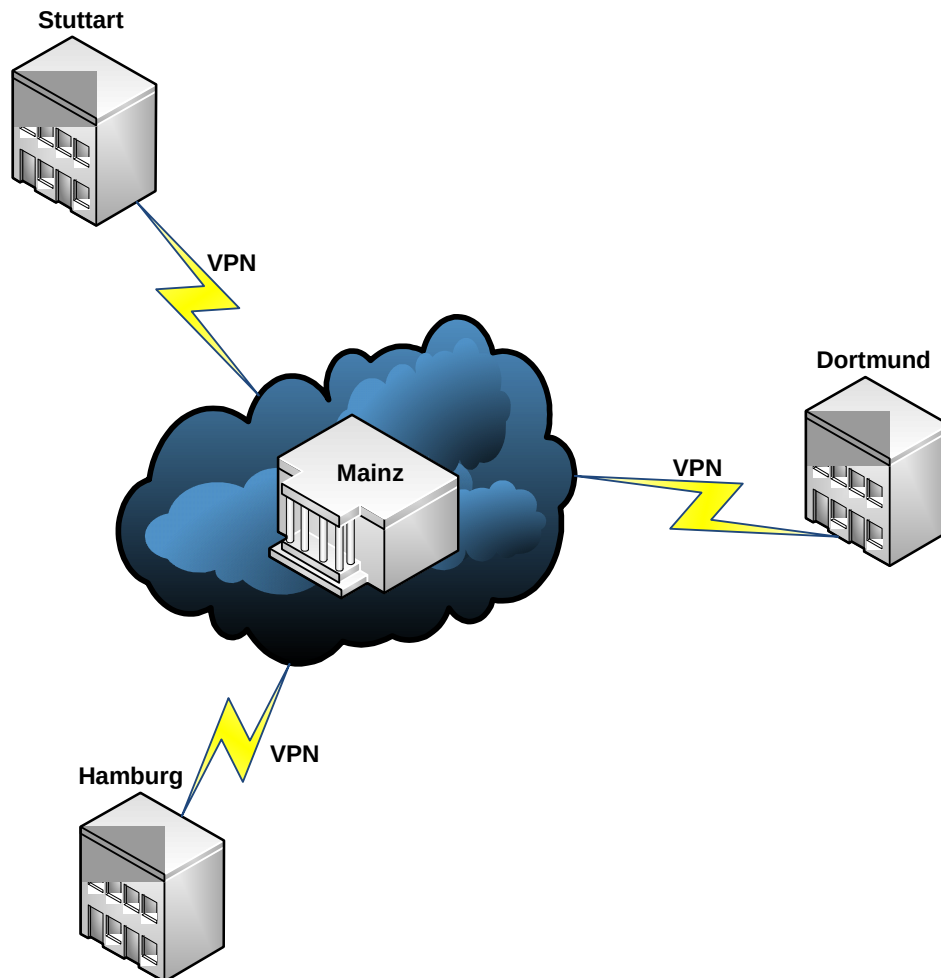
In Mainz werden alle e-mails erst nach Prüfung auf schädlichen Code (aus dem externen Netz) in der DMZ (SMTP Server) entgegengenommen und von dem Mailserver im LAN des Unternehmens abgerufen.

Im internen Netz ist sämtlicher Traffic ohne Restriktionen möglich, da der interne Netzabschnitt als trusted (trusted zone) gilt, und somit barrierefrei auch zwischen den einzelnen Standorten gemailt werden kann. Sollte eine externe e-mail intern zwischen verschiedenen Mitarbeitern weitergeleitet werden, so wurde diese vorerst durch den Spam/Viren Scanner in der DMZ auf schädlichen Code untersucht, und ist somit bereinigt oder frei von böartigen Daten.

Alle Filialen sind mittels eigener VPN Server, die in der jeweiligen DMZ aufgestellt sind, miteinander verbunden.

Somit wurde ein sicherer, verschlüsselter Tunnel über das Internet geschaffen (Ende zu Ende).

Der VPN Konzentrador befindet sich in der DMZ in Mainz, dort schlagen alle Verbindungen der weiteren 3 Standorte auf. Somit ergibt sich ein sternförmig angeordnetes Netzwerk. Die VPN Server sind vom Unternehmen frei wählbar, eine Cisco Infrastruktur mit Radius Servern als Authentifizierungsmaschinen ist denkbar, abhängig vom Budget. Eine Any-To-Any VPN Lösung ist ebenfalls denkbar, jedoch teurer und somit hier nicht implementiert.



Zur Sicherheit gegen Ausfälle, und somit zur Verbesserung der Verfügbarkeit, befindet sich in Mainz eine HSRP* Infrastruktur, welches eine doppelte Internetanbindung ermöglicht. Sollte eine Internetanbindung ausfallen, kann direkt über die Backupanbindung nahtlos weiteragiert werden. HSRP* erzeugt ein virtuelles Gateway aus zwei identischen physikalischen Gateways, die jeweils eine eigene Internetanbindung besitzen und per Trunk den eigenen Status untereinander in einer HSRP* Gruppe abfragen. HSRP* ist ein proprietäres Protokoll und bedarf keine Anbindung an SNMP Konzepte. Fällt ein Router aus, übernimmt der Passive Backup Router den Aktiven, Defekten Router, und die Arbeit ist nahtlos möglich. Bezüglich der externen (Internet) Anbindung wurde eine 2 Leitungen, 1 Provider Strategie gewählt. Somit stehen von einem Provider 2 getrennte Leitungen zur Verfügung, seitens des Providers wird auch das Routing realisiert. Sollte die primäre Leitung (PROD Line) ausfallen, wird schnell das Problem durch Port Triggering erkannt. Ports werden sowohl intern, als auch beim Provider getriggert, und bei einem Ausfall wird somit das Routing schnell auf die Backup Line umgeschaltet. Dies wird dadurch realisiert, dass die Hauptleitung eine niedrigere Metric besitzt, als die Backup Leitung. Bricht die PROD Line weg, wird automatisiert nach der nächstbesten Leitung mit der nächstbesten Metric gesucht. Automatisch wird durch den Provider auch DNS geupdated, damit das Routing weiterhin funktioniert, und Netzwerk Verkehr von extern auch sicher ankommt. Somit ist sichergestellt, dass das Routing bei einem Ausfall kurzfristig umgeleitet wird, und nicht mit

eigenen technischen Realisationen in Verbindung steht. Das richtige Routing ist über ein Agreement mit dem Provider geregelt. Routing wird somit „extern“ erledigt.

Das SNMP wird in Mainz (und allen weiteren Standorten) zur Überwachung der Server verwendet. Fällt ein Mailserver oder VPN Konzentrator aus, kann dies mittels SNMP ermittelt werden, ein Clusterserver übernimmt als Backup die Aufgaben des ausgefallenen Servers. Mittels Alarming werden die technischen Wartungsmitarbeiter über den Ausfall benachrichtigt, und können die Server wieder instandsetzen. Die Mailserver werden ständig repliziert, damit sich immer aktuelle Datensätze auf allen Maschinen befinden. Die Replizierung kann permanent erfolgen, da im eigenen LAN schnelle Leitungen vorhanden sind und nicht als Flaschenhals wie z.B. bei Backup Strategien an externen Standorten zu Problemen und Lastspitzen führen können.

Eine Datensicherung erfolgt täglich inkrementell sowie wöchentlich Vollständig auf die Stagesysteme in Mainz, um stets einen gleichen Datenhaushalt zu gewährleisten. Die Stagesysteme betreffen jedoch nicht direkt das Mailsystem, und sind somit im e-mail Diagramm nicht verzeichnet. Der SMTP Server der DMZ in Mainz wird nicht gesichert, um schadhafte Code nicht in das Stagesystem einzubinden. Lediglich der LAN Mailserver wird gesichert, hier befinden sich ja die e-mails von extern direkt nach der Spam und Virenprüfung. Wenn e-mails vom SMTP Mailcluster aus der DMZ abgeholt werden, sind diese auch vom SMTP Cluster gelöscht, da Sie dort nichtmehr benötigt werden. Als SMTP Mailcluster sind somit keine großen Speicher notwendig, da Speicher kostenintensiv ist.

Die Internetanbindung ist mittels der redundanten HSRP Gateways hochverfügbar und ausfallsicher. Als Zusatz wurde in der DMZ von Mainz ein Proxy Server implementiert, der alle Internetzugriffe reguliert und gleichzeitig schützt. Es werden Managed Switches eingesetzt, sollte z.B. der I-Net Proxy durch externe Angriffe kompromittiert werden, kann diese durch Shutdown des LAN-Ports direkt vom Netz getrennt werden und gefährdet somit keine weiteren Einheiten des Netzes.

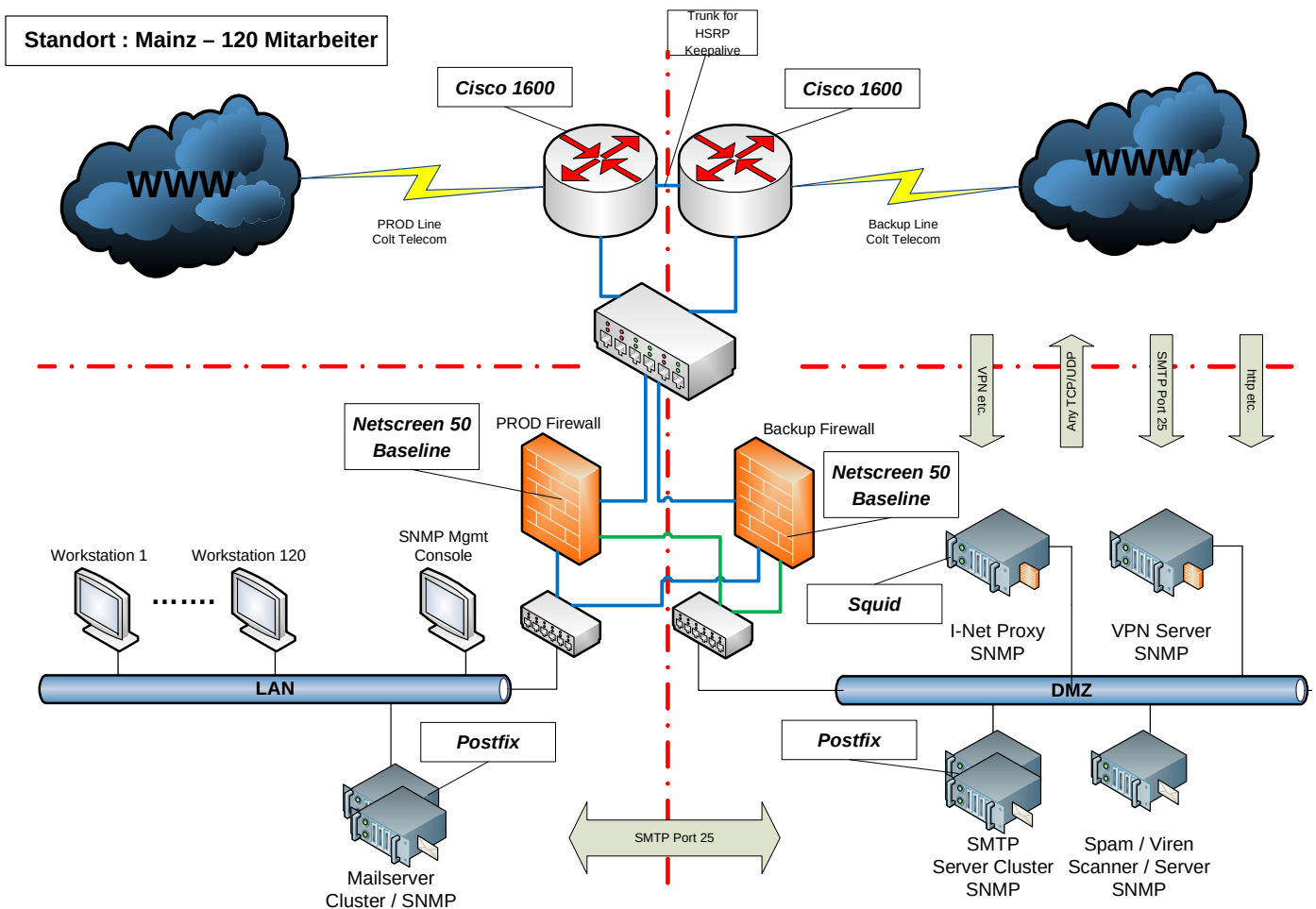
Die Firewallstufen basieren auf Netscreen und beherrschen VPN Tunnel mit bis zu 100 Parallelverbindungen schon in der kleinsten Basisversion. Die Firewall ist ebenfalls redundant ausgelegt, und sollte die Aktive Firewall ausfallen, schaltet sich automatisch die Backup Firewall aktiv und übernimmt das Filtering. Die Erkennung einer defekten Firewall wird durch Netscreen mitgeliefert und bedarf daher keiner Softwarelösung, die implementiert werden muss.

Die Mailserver basieren auf Postfix, was kostenfrei und effizient eingesetzt werden kann. Der Proxyserver basiert auf Squid, ebenfalls kostenfrei und frei verfügbar.

Aus der Erfahrung heraus sind Software Lösungen wie „Squid“ und „Postfix“ auch in Unternehmen erfolgreich in Betrieb.

!!!! Diese Beschreibung soll grob das Konzept darstellen, und ist nicht vollständig und nur in Grundzügen beschrieben !!!!!

* HSRP => Weitere Erläuterungen finden Sie im Anhang



Standort Hamburg :

In Hamburg ist wie in den übrigen Filialen keine weitere technische Umsetzung für mail und Internet vorhanden. Alle Filialen arbeiten über VPN mit den Servern, die sich im Rechenzentrum in Mainz befinden. Lediglich ein VPN Server befindet sich in der DMZ in Hamburg, der die Verbindung mit dem VPN Konzentrador in Mainz aufrechterhält.

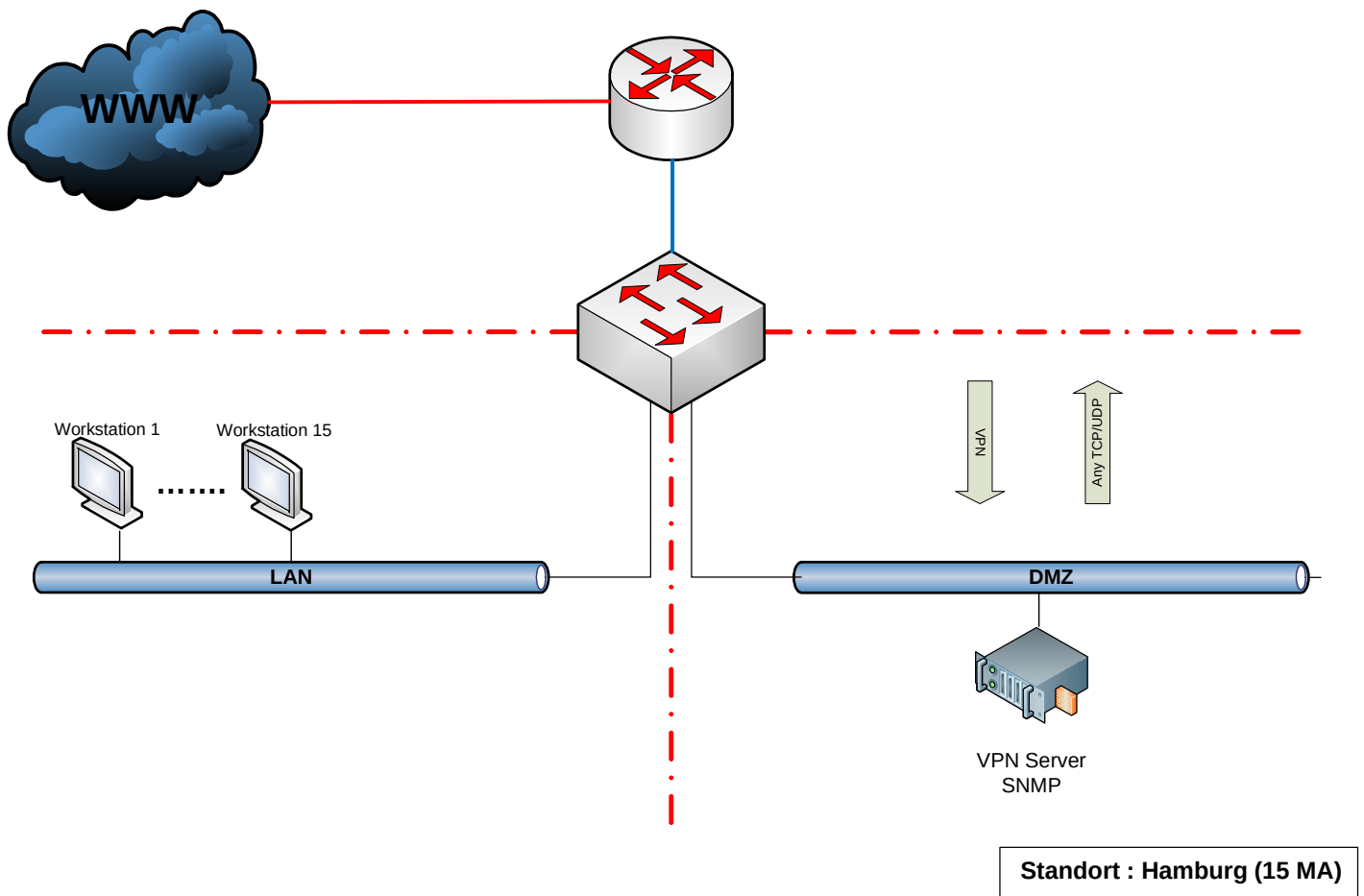
Somit werden e-mails über Mainz versendet und empfangen, ebenso wird über den Proxy in Mainz im Internet gesurft, man ist also mit den Sicherheitsstufen aus Mainz abgesichert. Ein Backupserver in Hamburg aufzustellen macht keinen Sinn. Hier ist zwar die Niederlassung mit den zweitmeisten Angestellten vor Ort, jedoch sind die VPN Leitungen schmalbandig, so dass eine permanente Replizierung des Mailservers nicht durchführbar ist (außer nachts, mit dem Problem, das im Worst Case 1 Tag e-mails fehlen, sofern Mainz ausfällt. Daher wurde bewusst die Strategie gewählt, Mainz möglichst zu härten und ausfallsicher zu gestalten).

Jede Niederlassung besitzt eigene Router, die notwendig sind, um per WAN Anbindung zum Rechenzentrum nach Mainz verbunden zu werden. Jede Niederlassung besitzt somit eine eigene Broadcast und Kollisionsdomäne, und hat intern ein schnelles LAN und eine sichere Anbindung an die Zentrale.

Eine eigene Firewall besitzt Hamburg nicht, da durch VPN die Niederlassung an Mainz angebunden ist, und externe Netzwerkzugriffe (Internet Surfen etc.) durch die Mainzer

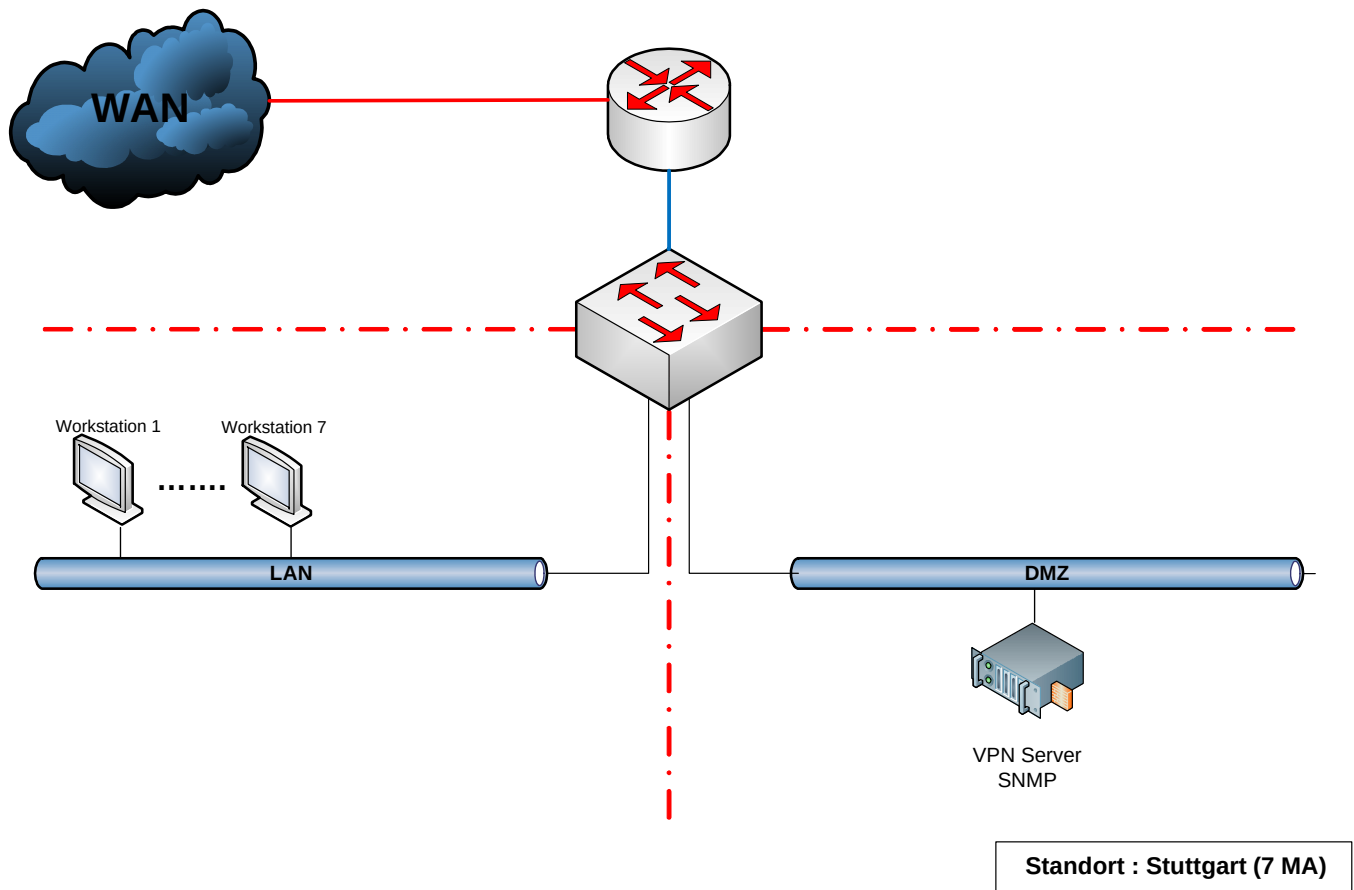
Firewallstufen abgesichert sind. Internetzugriffe werden für alle Niederlassungen von Mainz aus realisiert. Im LAN sind alle Filialen in der „Trusted Zone“, so dass keine Sicherheitsstufen notwendig sind.

Auch Datensicherungen werden durch die Storage Systeme in Mainz durchgeführt. Bei einem Wegfall der Anbindung werden die Daten spätestens am Folgetag durch die inkrementelle Datensicherungsroutine wieder nach Mainz gesichert. Die Datenmenge wird vorzugsweise durch das sichern der Deltas niedrig gehalten, volle Datensicherungen werden nur nachts mittels Scheduler durchgeführt.



Standort Stuttgart :

In Stuttgart sind wenig Mitarbeiter beschäftigt, die Filiale ist äquivalent zur Niederlassung in Hamburg. Dort befindet sich ein VPN Gateway in der DMZ, durch den die Filiale mit der Zentrale in Mainz verbunden ist. Somit wird der gesamte e-mail Traffic, wie auch Internet usw. über Mainz geregelt. Alle Filialanbindungen sind Kupferleitungen, die mit 98,5% Durchschnittsverfügbarkeit ausreichend sind, um die Filiale sicher anzubinden.

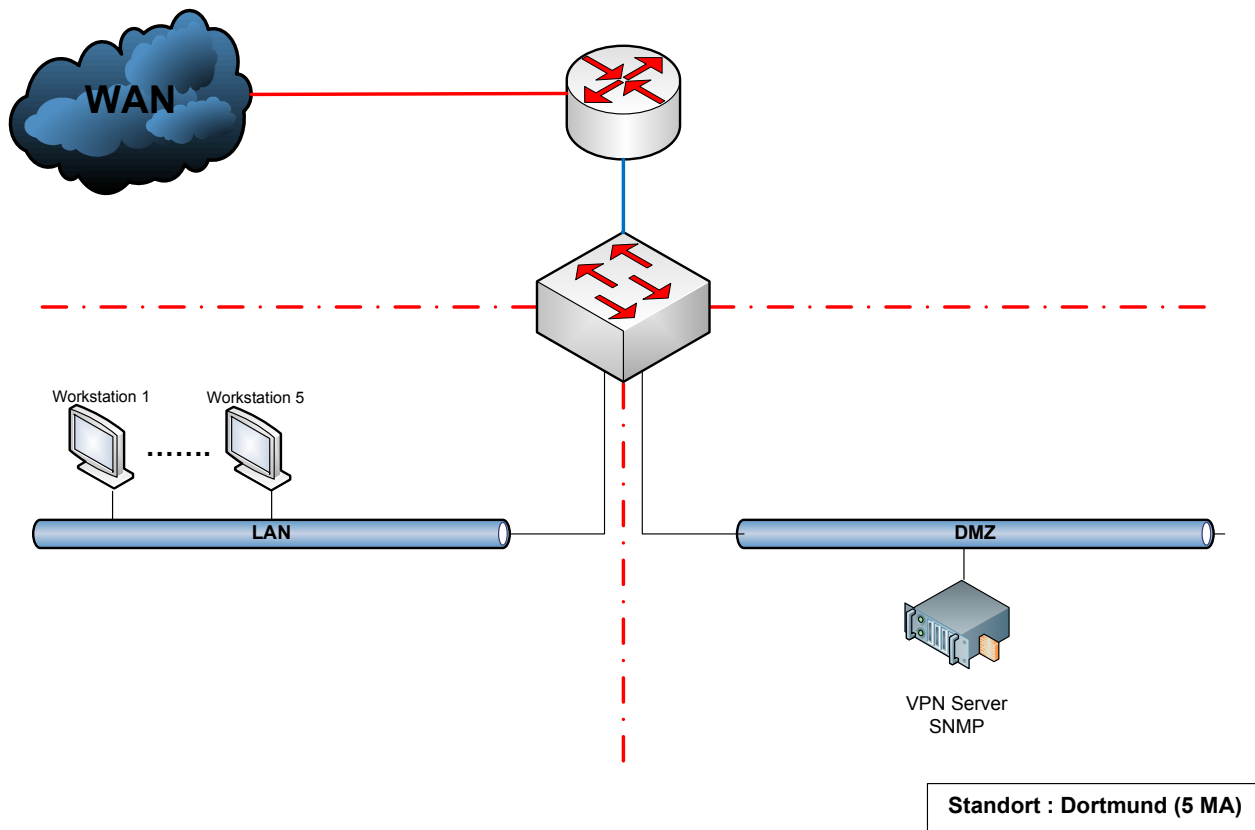


Standort Dortmund :

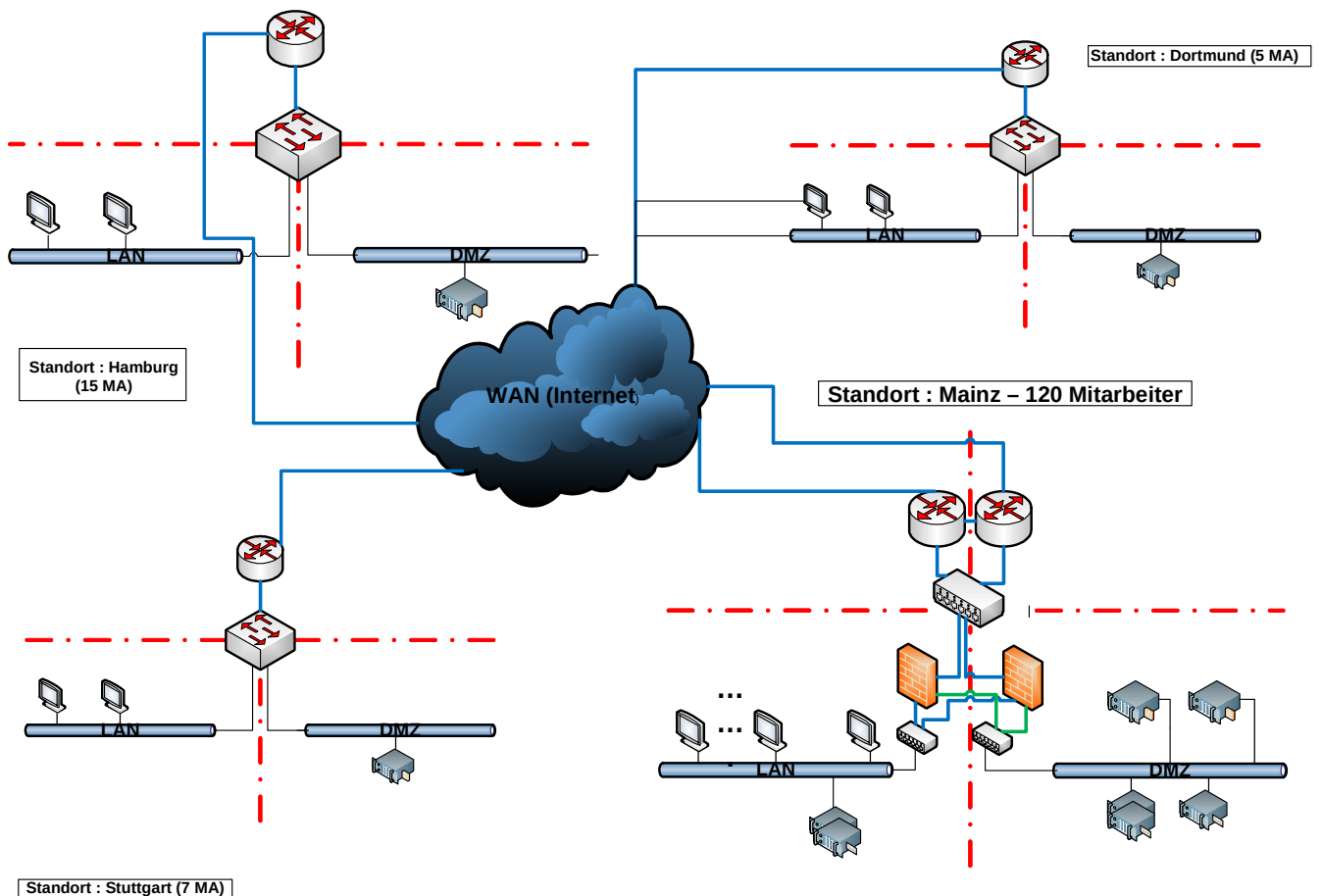
In Dortmund sind die wenigsten Mitarbeiter beschäftigt, wodurch kein großes Konzept zur Verfügbarkeit der Systeme benötigt wird. Alle wichtigen Systeme stehen am Standort Mainz. Daher ist diese Filiale infrastrukturell identisch der Stuttgarter Filiale. Entsprechend der bereits erwähnten Infrastruktur ist Dortmund mittels VPN an das Netzwerk angebunden, und befindet sich somit in der trusted Zone. Genutzt werden die Mailserver aus Mainz, angebunden mittels Kupferleitung.

Da alle Filialen gleich aufgebaut sind, und über die gleichen technischen Einrichtungen angebunden sind, ist das Netz in höchstem Maße transparent und wartbar.

Auf Grund der Größe der Filiale ist keine redundante Leitung von Nöten, da bei einem Ausfall einer Leitung lediglich 4% der Gesamtmitarbeiteranzahl arbeitsunfähig sind. Den Kosten für eine Backupleitung gegenübergestellt ist diese Infrastruktur mit einfacher Anbindung wesentlich kostengünstiger.



Im Gesamten findet man im Unternehmen somit folgende Infrastruktur vor :



Die Software Realisation ist individuell auf das Unternehmen abgestimmt, und kann daher frei gewählt werden. Neben kostenfreien Freeware Mailservern (z.B. Hamster Mailserver etc.) sind auch professionelle Serverlösungen denkbar. Je nach Budget kann auch auf einen Microsoft Exchange Server ausgewichen werden, zu empfehlen wäre eine Lotus Notes e-mail Umgebung mit Lotus Domino Server.

Der Lotus Domino Server vereint e-mail mit weiteren Funktionalitäten, die für Unternehmen zu Kosteneinsparung führen, da keine weiteren Server für Datenbanken etc. notwendig sind. Mit Lotus Domino lassen sich nebst Mail z.B. auch Warenwirtschaft, Bestellwesen, Kalender, Telefonbuch, Resource Access Control Facility (RACF) zur Verwaltung von Permissions, UserIDs, Ressourcen, Gruppen etc. und Instant Messaging betreiben.

Für welche Software Lösung sich das Unternehmen entscheidet, hängt vom Budget, den Kosten und den gewünschten Standards ab, die das Unternehmen abbilden möchte.

Im oben aufgeführten Fall wurde für Mail der kostenfreie Postfix Mailserver eingesetzt, als Firewalls kommen Netscreen Systeme zum Einsatz, als Router verwendet man Cisco 1600 Devices. Der Proxy wird mittels Server (Unix bzw. Linux) sowie SQUID realisiert.

Bitte beachten Sie, das dieses Dokument nur die Grundzüge beschreibt, und eine Ausweitung in die Tiefe möglich ist, aber aus Gründen, den Umfang möglichst gering zu halten, nicht umgesetzt wurde.

Anhang (zu Aufgabe 1) :

Aus: Wikipedia, der Freien Enzyklopädie :

Das **Hot Standby Router Protocol (HSRP)** ist ein Verfahren zur Steigerung der Verfügbarkeit von wichtigen Gateways in lokalen Netzen durch **redundante Router**.

Das proprietäre HSRP ist von **Cisco** entwickelt worden. Heute ist es aber auch in vielen Routern anderer Hersteller verfügbar. Das HSRP wurde entwickelt, um eines der großen Probleme in der Ausfallsicherheit von Datenwegen zu adressieren, die Verfügbarkeit des so genannten *Standardgateways* in lokalen Netzen.

Beim Routen von Datenpaketen durch Netzwerke wird dem Ausfall von Teilstrecken auf dem Weg zum Ziel durch das dynamische **Routing** entgegengewirkt. Fällt jedoch der erste Router auf einer Strecke aus, so ist dieser Fehler nicht durch dynamisches Routing zu beheben, da ein Host im Normalfall nur ein statisches Standardgateway kennt und meist auch nur eines unterstützt. Durch einen Ausfall des ersten Routers, des Standardgateways, sind die betroffenen Hosts von der Kommunikation mit der Außenwelt abgeschnitten, selbst dann, wenn noch aktive Router im gleichen Teilnetz verfügbar sind.

An dieser Stelle setzt das HSRP an. Mehrere physikalische Router werden zu einer logischen Gruppe zusammengefasst. Diese Gruppe von Routern präsentiert sich im Netzwerk nun als **ein** logischer Router.

Hierzu wird dem logischen Router eine virtuelle IP-Adresse und eine virtuelle MAC-Adresse zugeordnet. Einer der Router innerhalb der Gruppe wird als der Primary-Router definiert, dieser bindet darauf die virtuelle MAC und die virtuelle IP an sein Netzwerkschnittstelle und informiert in regelmäßigen Abständen (Default: 3 Sekunden) die anderen Router der Gruppe,

die als Secondary-Router agieren, mittels einer **Multicast**-Nachricht an die Zieladresse 224.0.0.2, Port UDP 1985.

Fällt der Primary-Router aus und bleiben die Multicast-Pakete für länger als die Zeit des "Holddown timers" (Default: 10 Sekunden) aus, so werden die virtuelle IP-Adresse und die virtuelle MAC-Adresse sofort auf einen der Secondary-Router übertragen, der damit zum neuen Primary-Router wird. Die MAC- und die IP-Adresse werden transferiert, damit die betroffenen Hosts nicht ihren **ARP**-Cache aktualisieren müssen. Die Gefahr des Ausfalls des ersten Routers auf der Route kann somit reduziert werden.

Aus: Salinas IT Service :

Hot Standby Routing Protocol (HSRP)

- eine Gruppe von Routern repräsentiert ein Gateway mit einer virtuellen IP und einer virtuellen MAC-Adresse
- MAC-Adresse 0000.0c07.acXX (XX steht für die Gruppe)
- verwendet Port 1985 UDP
- Multicast an 224.0.0.2 (TTL ist 1)
- max. 255 Gruppen

Wer ist Active Router ?

- höchste Priorität --> Active Router

- zweit höchste Priorität --> Standby Router
- bei gleicher Priorität entscheidet die höchste IP-Adresse
- Standardpriorität ist 100
- Active Router wie auch Standby Router senden alle 3 Sekunden ein „Hello“
- hold-down time ist 10 Sekunden

HSRP Zustände

- Initial
- Learning (Welche Router gibt es ?)
- Listening (Wer ist Active oder Standby ? Router, die nicht active oder standby sind, verbleiben in diesem Zustand)
- Speaking (sendet Hello-Paket aus)
- Standby
- Active

Aufgabe 1.1

Infrastruktur ohne externen Mailversand

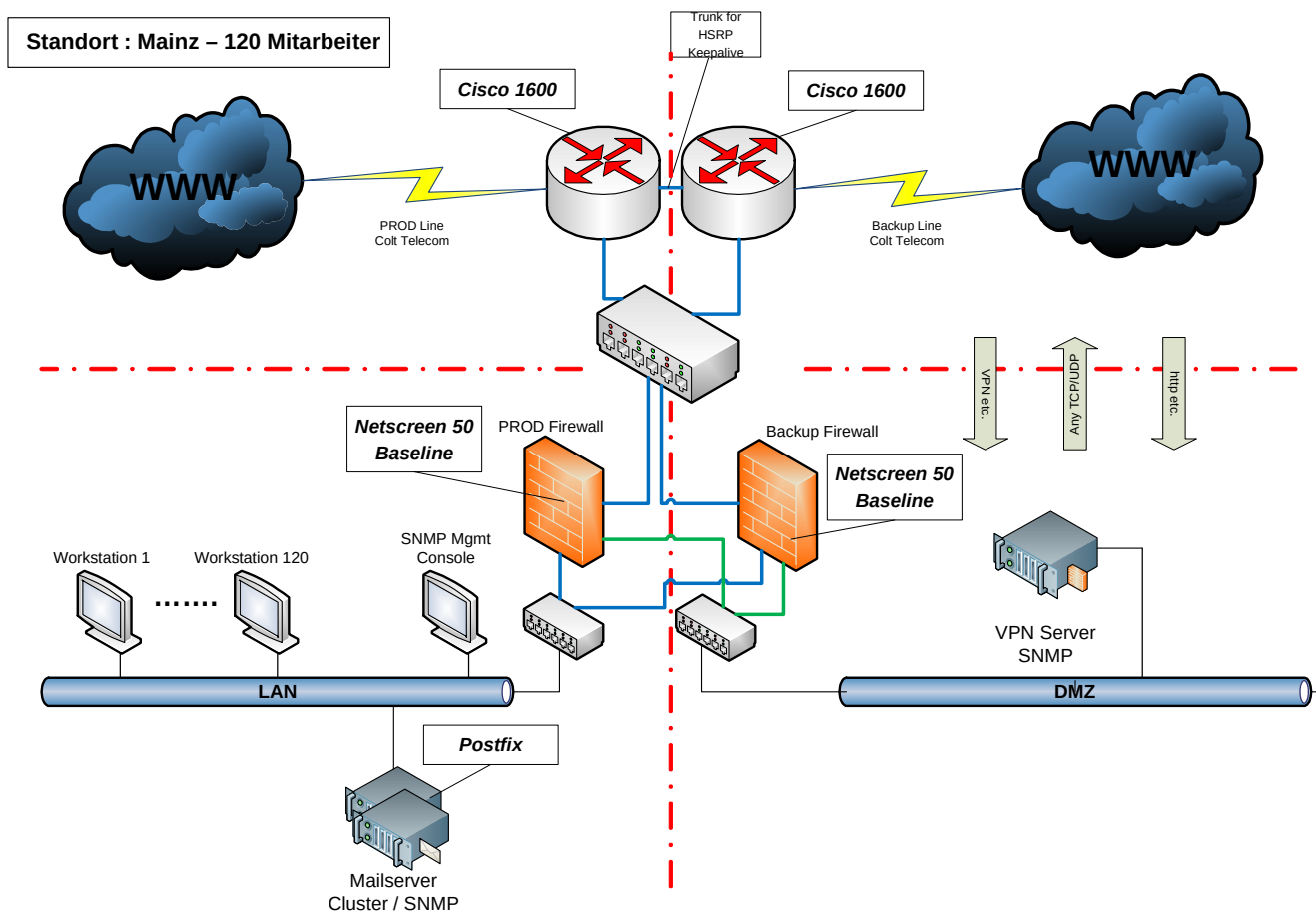
Standort Mainz :

Angelehnt an die Infrastruktur aus Aufgabe 1.2 ist das Netz ohne externe e-mail Möglichkeit nicht stark abweichend von der Infrastruktur mit externem Mailversand.

Grundlegend ist ein Unterschied in der DMZ des Hauptrechenzentrums in Mainz (120 MA) zu finden. Dort befindet sich der SMTP Server mit Spam und Virensan in der DMZ. Dieser empfängt externe e-mails, durchsucht Diese auf schädlichen Code, und lässt die internen Mailserver die gescannten e-mails bei sich abholen, zwecks Übermittlung in das interne Netz. Wird der externe Mailversand nicht gewünscht, müssen lediglich die MX Einträge auf dem LAN Mailserver in Mainz entfernt werden, und durch eine lokale DNS Adresse ersetzt werden. Damit wird kein e-mail Name mehr aufgelöst und ein Empfang / Versand von Mails nach extern ist nichtmehr möglich.

Wird kein externer Empfang mehr gewünscht, können die beiden Server SMTP & Spam/Virensan in der DMZ in Mainz abgebaut werden, da diese lediglich externe e-mails bearbeiten. Dadurch reduziert sich die Infrastruktur um diese beiden Devices, alles Weitere bleibt bestehen.

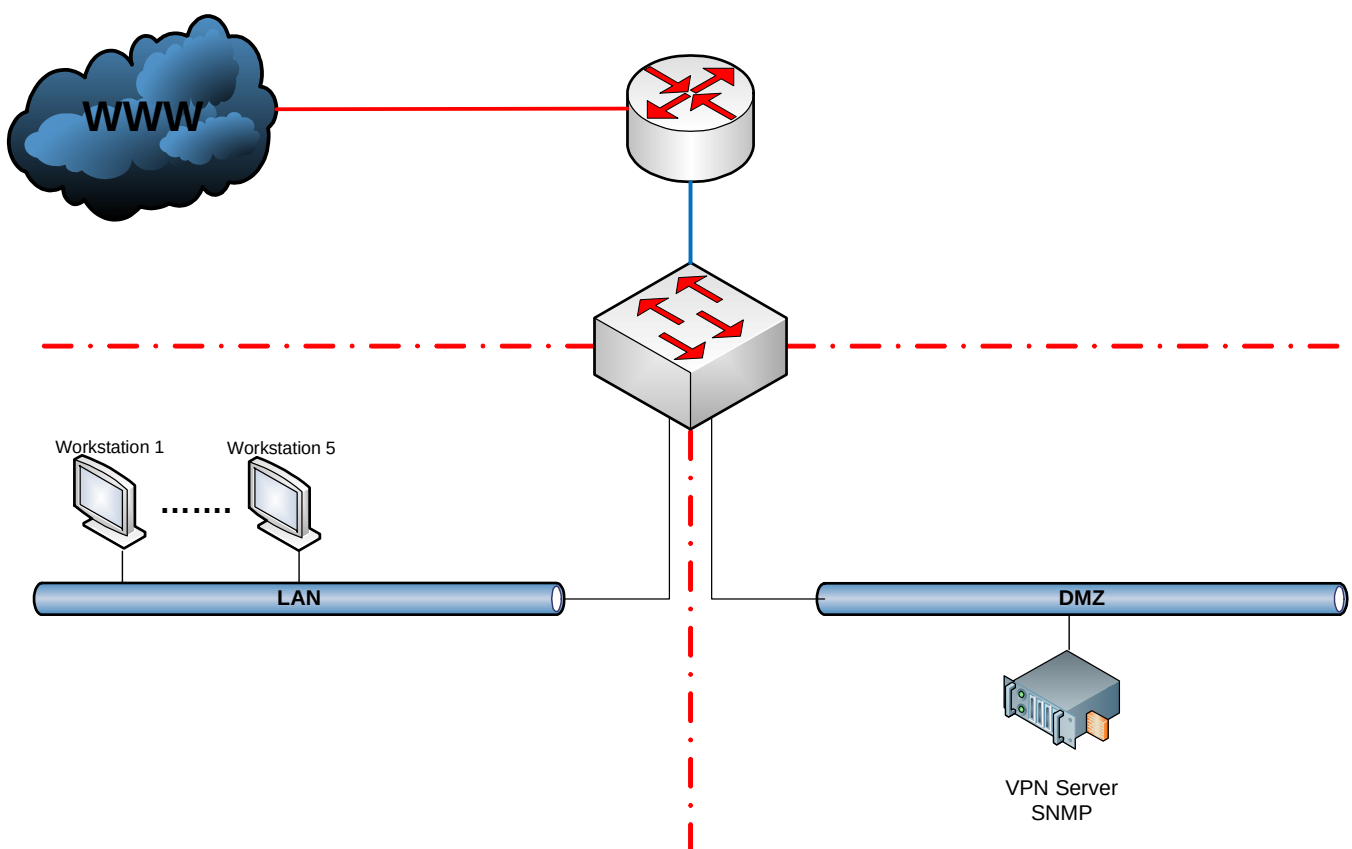
Somit würde der Standort Mainz infrastrukturell wie folgt aussehen :



Deutlich zu erkennen ist, dass die Infrastruktur in Mainz sich nur durch die weitestgehende Räumung der DMZ Infrastruktur unterscheidet. Mailserver, Spam und Viren Scanner, Proxy Server etc. wurden abgebaut und sind nichtmehr notwendig. Somit bleibt nur der Mailserver im LAN übrig, da innerhalb der trusted Zone ohne Restriktionen gemailt werden kann.

Die drei Niederlassungen sind identisch mit dem Aufbau aus Aufgabe 1.2 und unterscheiden sich nicht, da diese so konzipiert wurden, das alles über das Rechenzentrum in Mainz realisiert wird, und diese lediglich dorthin angebunden sind, um dort möglichst wenig IT Infrastruktur vorzuhalten.

Niederlassung Stuttgart / Dortmund / Hamburg :



Aufgabe 1.3

Verfügbarkeiten

Die Verfügbarkeit stellt die Mean time between failures (MTBF) der Mean time to repair (MTTR) gegenüber. Die Verfügbarkeit eines technischen Systems ist die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt, und ist somit eine Eigenschaft des Systems. Sie ist ein Qualitätskriterium/Kennzahl eines Systems.

Die Verfügbarkeit eines einzelnen, isolierten Server beträgt 98,5 %.

Betrachtet man in Aufgabe 1.2 das hinzurechnen eines Backup Servers, erhöht man die Verfügbarkeit des Systems theoretisch auf durchschnittlich 99,5 % (maximal 15,6 Stunden Ausfallzeit pro Jahr). Diese Verfügbarkeit wird in der wichtigsten Niederlassung Mainz (120 Mitarbeiter) prinzipiell erreicht (für den Inhouse Mailversand). Die Verfügbarkeit sinkt für alle weiteren Niederlassungen, und ist abhängig von weiteren Faktoren (Leitung etc.)

Die Leitungsverfügbarkeit ist pro Leitung Kupfer mit 98,5% angegeben. Diese muss in allen Konzepten beachtet werden, und senkt somit die Gesamtverfügbarkeit je Standort.

So beträgt die Verfügbarkeit von Mail in der Filiale Mainz :

98,0 % bei Mail im internen Netz. Intern wird lediglich 1 Server für den Mailversand benötigt, der im LAN (vor Ort) verfügbar ist. Das Backup Konzept (Clusterserver) ermöglicht eine 99,5%ige Verfügbarkeit des Mailsystems in Mainz selbst, d.h. 120 Mitarbeiter haben ein hochverfügbares Mailsystem,

Für den internen Mailversand zu anderen Niederlassungen muss die Leitungsverfügbarkeit mitberechnet werden. In Mainz ist das Mailcluster mit 99,5% Verfügbarkeit die Berechnungsgrundlage, verrechnet mit 98,5% Leitungsverfügbarkeit (Kupferleitung) in andere Filialen, da die Niederlassungen jeweils nur eine Leitung besitzen.. Zwar erhöht sich die Verfügbarkeit des Mailserver durch Hinzukalkulation der Backupleitung in Mainz, jedoch ist die Leitungsverfügbarkeit der „schwächsten“ Filiale entscheidend, und gibt den Berechnungswert vor (98,5% pro Leitung der Niederlassungen).

98,5 % bei Mail in das externe Netz. Das Mailkonzept mit Betrachtung auf die Leitungen ist mit einer Verfügbarkeit für Mainz bei lediglich 96,54 %, da hier 2 getrennte MailCluster (jeweils 99,5% Verfügbarkeit) notwendig sind, um Mail für externen Versand zu gewährleisten. Die Leitungen sind durch die Backup Strategie bei einer Verfügbarkeit von 99,5% mit einzuberechnen.

Filiale : Hamburg :

97,51 % bei Mail im internen Netz. Intern wird lediglich 1 Server benötigt. Zwar ist der primäre Mailserver nicht vor Ort, wodurch die Verfügbarkeit sinkt, Bei einem Wegfall ist aber ein Backup Mailserver (Servercluster) in Mainz vorhanden, der den Mailversand übernehmen kann. Somit erhält man bei diesem Konzept eine Verfügbarkeit von 99,5% für das Servercluster, verrechnet mit der Verfügbarkeit der Kupferleitung, um Niederlassungsübergreifend e-mails zu versenden.

97,02 % bei Mail in das externe Netz. Das Mailkonzept mit der Betrachtung auf Leitungen ist mit einer Verfügbarkeit für HH bei lediglich 95,56 %, da hier 2 isolierte Server (- Cluster) notwendig sind, um Mail für externen Versand zu gewährleisten. Hinzu kommt, dass man von der Verfügbarkeit der Kupferleitung abhängig ist, welche isoliert bei 98,5% liegt (gemäß Regulierungsbehörde, Werte sind als Durchschnitt angegeben).

Filiale Stuttgart :

97,51 % bei Mail im internen Netz. Intern wird lediglich 1 Server benötigt. Zwar ist der primäre Mailserver nicht vor Ort, wodurch die Verfügbarkeit sinkt, Bei einem Wegfall ist aber ein Backup Mailserver (Servercluster) in Mainz vorhanden, der den Mailversand übernehmen kann. Somit erhält man bei diesem Konzept eine Verfügbarkeit von 99,5% für das Servercluster, verrechnet mit der Verfügbarkeit der Kupferleitung, um Niederlassungsübergreifend e-mails zu versenden (mit Beachtung der doppelten Anbindung der Zentrale Mainz)

97,02 % bei Mail in das externe Netz. Das Mailkonzept mit der Betrachtung auf Leitungen ist mit einer Verfügbarkeit für Stuttgart bei lediglich 95,56 %, da hier 2 isolierte Server (- Cluster) notwendig sind, um Mail für externen Versand zu gewährleisten. Hinzu kommt, dass man von der Verfügbarkeit der Kupferleitung abhängig ist, welche isoliert bei 98,5% liegt (gemäß Regulierungsbehörde, Werte sind als Durchschnitt angegeben).

Filiale Dortmund :

97,51 % bei Mail im internen Netz. Intern wird lediglich 1 Server benötigt. Zwar ist der primäre Mailserver nicht vor Ort, wodurch die Verfügbarkeit sinkt, Bei einem Wegfall ist aber ein Backup Mailserver (Servercluster) in Mainz vorhanden, der den Mailversand übernehmen kann. Somit erhält man bei diesem Konzept eine Verfügbarkeit von 99,5% für das Servercluster, verrechnet mit der Verfügbarkeit der Kupferleitung, um Niederlassungsübergreifend e-mails zu versenden (mit Beachtung der doppelten Anbindung der Zentrale Mainz)

97,02 % bei Mail in das externe Netz. Das Mailkonzept mit der Betrachtung auf Leitungen ist mit einer Verfügbarkeit für Dortmund bei lediglich 95,56 %, da hier 2 isolierte Server (- Cluster) notwendig sind, um Mail für externen Versand zu gewährleisten. Hinzu kommt, dass man von der Verfügbarkeit der Kupferleitung abhängig ist, welche isoliert bei 98,5% liegt (gemäß Regulierungsbehörde, Werte sind als Durchschnitt angegeben).

Fazit: Durch das vorliegende Mailkonzept erreicht man in allen Niederlassungen die gleiche Verfügbarkeit für den internen Mailversand, für die größte Niederlassung wird auch der Mailversand nach extern erhöht, im Vergleich zu den kleineren Niederlassungen, die das Unternehmen besitzt. Verfügbarkeit ist teuer, und daher wird nur der Hauptsitz möglichst verfügbar aufgebaut, die kleinen Niederlassungen besitzen eine angemessen hohe Verfügbarkeit, die rechnerisch unterhalb der der Hauptniederlassung liegt.

Aufgabe 2

Antwort: Um zu verdeutlichen, wo und wann etwas passiert, haben wir den vorgegebenen Header etwas zerpflückt und farblich die Wege markiert. So sind die Zeiten in **grün**, der Weg in **blau** und die Netzübergänge in **rot** dargestellt.

[mzmail1.intern.hzd.hessen -> marcel.boffo@ hzd.hessen.de]

Microsoft Mail Internet Headers Version 2.0

Received: from mailman.nic.hessen ([10.7.98.3]) [mailman.nic.hessen -> mzmail1.intern.hzd.hessen]

by mzmail1.intern.hzd.hessen with Microsoft

SMTPSVC(6.0.3790.1830);

Wed, 15 Oct 2008 14:19:05 +0200

[- 26 sek : zb. Fehlkonfiguration(kein NTP)]

Received: (gmail 9487 invoked from network); [network -> gmail]

15 Oct 2008 12:19:31 -0000

[+ 57min + 26 sek]

[Die Mail kommt hier verzögert beim gmail Server an => gmail Server Problem oder mailman.* verschickt nicht.]

Received: from unknown (83.243.48.68) [mail1.rlp.de -> mailman.nic.hessen]

by mailman.nic.hessen with QMTP; **15 Oct 2008 11:22:05 -0000**

[+ 0 sek]

[Netzwechsel]

Received: (gmail 22545 invoked from network); [mailto.hessen.de -> mail1.rlp.de]

15 Oct 2008 11:22:05 -0000

[+1 sek]

X-Spam-Checker-Version: SpamAssassin 3.2.0 (2007-05-01) on mail1

[hierbei handelt es sich wohl um einen externen Spamfilter scheinbar fehlt ein Teil des Namens mail1... da unknown (83.243.48.68) laut Nslookup mail1.rlp.de sein müsste.]

[Netzwechsel]

Received: from fmmailgate05.web.de (217.72.192.243) [fmmailgate05.web.de -> mailto.hessen.de]

by mailto.hessen.de with ESMTP; **15 Oct 2008 11:22:04 -0000**

[+10 sek]

[Netzwechsel]

Received: from web.de [web.de -> fmmailgate05.web.de]

by fmmailgate05.web.de (Postfix) with SMTP id 35CB130FFA2B

for <marcel.boffo@hzd.hessen.de>; Wed, **15 Oct 2008 13:21:54 +0200 (CEST)** **[+ 1 sek]**

Received: from [79.211.191.36] [vom computer zu freemailing0503.web.de]

by freemailing0503.web.de with HTTP; [t-ipconnect]

Wed, **15 Oct 2008 13:21:53 +0200**

[Netzwechsel]

[Die Mail]

Date: Wed, **15 Oct 2008 13:21:53 +0200** **[Startzeit]**

Message-Id: <1714960166@web.de>

MIME-Version: 1.0

To: marcel.boffo@ hzd.hessen.de

Subject: Teschtmail 13:21:45 Uhr

Precedence: fm-user

Organization: http://freemail.web.de/

X-Provags-Id: V01U2FsdGVkX1+rWwJ/FxO/FpGEgc1OwQeZNHzyMG+y8TQ/zP61uuV2ENIK4Y8Y4wXjARU+FOMogVVq1D6X3wBDHebqWIRnpJ2wKLpkPRKpAgE=

Content-Type: text/plain; charset=iso-8859-15

Content-Transfer-Encoding: quoted-printable

Return-Path: mboffo@web.de

X-OriginalArrivalTime: 15 Oct 2008 11:22:05.0684 (UTC) FILETIME=[DB839340:01C810D9]

Man kann den Weg so sehr gut von unten nach oben verfolgen.

In blau sieht man hier das bei jeder Received-Zeile auch eine Blaue Klammer steht, diese soll verdeutlichen, von wo das Paket gekommen ist.

So soll die Zeile:

Received: from web.de [web.de -> fmmailgate05.web.de]

Verdeutlichen, daß die Mail von **web.de** bei **fmmailgate05.web.de** angekommen ist.
fmmailgate05.web.de schreibt die Received-Zeile hier in den Header.

In grün kann man die Mail zeitlich verfolgen.

Hier fallen zwei Dinge auf :

Zum Einen wird die Mail im *.hessen Netz für 57min nicht weitergeschickt, zum Anderen wird laut Header die Zeit, in der letzten Instanz, für 26 Sekunden zurückgesetzt.

Eine mögliche Erklärung hierfür wäre, dass der letzte Server seine Zeit nicht per NTP bekommt, sondern beispielsweise manuell vom Administrator konfiguriert wurde.

Die Verzögerung der Mail könnte zustande kommen durch einen Fehler des qmail Servers oder noch wahrscheinlicher durch ein Problem von **mailman.nic.hessen**.

Des Weiteren ist noch auffällig, dass der Spamfilter für hessen.de scheinbar in Rheinland Pfalz ist.

Dieses Dokument wurde erstellt von :

- ⇒ **Klaus Schwartz**
- ⇒ **Matthias Bach**