Høgskolen i Sørøst-Norge

Prosjekt 2 - Bedriftsnettverk

Prosjektgruppe: Amund Bogetvedt, Martin Markussen, Christian Aashamar, Gard Rene Klemetsen og Eivind Børstad

Utgivelsesdato: 24.04.2017

Begrensning: Stengt

Sammendrag

Rapporten tar for seg oppsett og struktur for bedriftsnettverket til Bedrift3. Det består av to soner: DMZ og sikker sone. I DMZ har bedriften en web- og mailserver som er tilgjengelig også utenfor LANet, samt en DNS-server. I sikker sone kan klienter koble seg på og arbeide i et trygt nettverk. Her finnes det også en DHCP-service som deler ut IP-adresser til klientene.

Nettverket er satt opp med sikkerhet som en høy prioritet. Det befinner seg en relativt sikker brannmur mellom DMZ og nettet utenfor, en enda sikrere brannmur inn til sikker sone. I tillegg opererer nettverket med en Ossec-server som samler inn informasjon fra de forskjellige maskinene for mistenkelig aktivitet.

Innholdsfortegnelse

Innledning

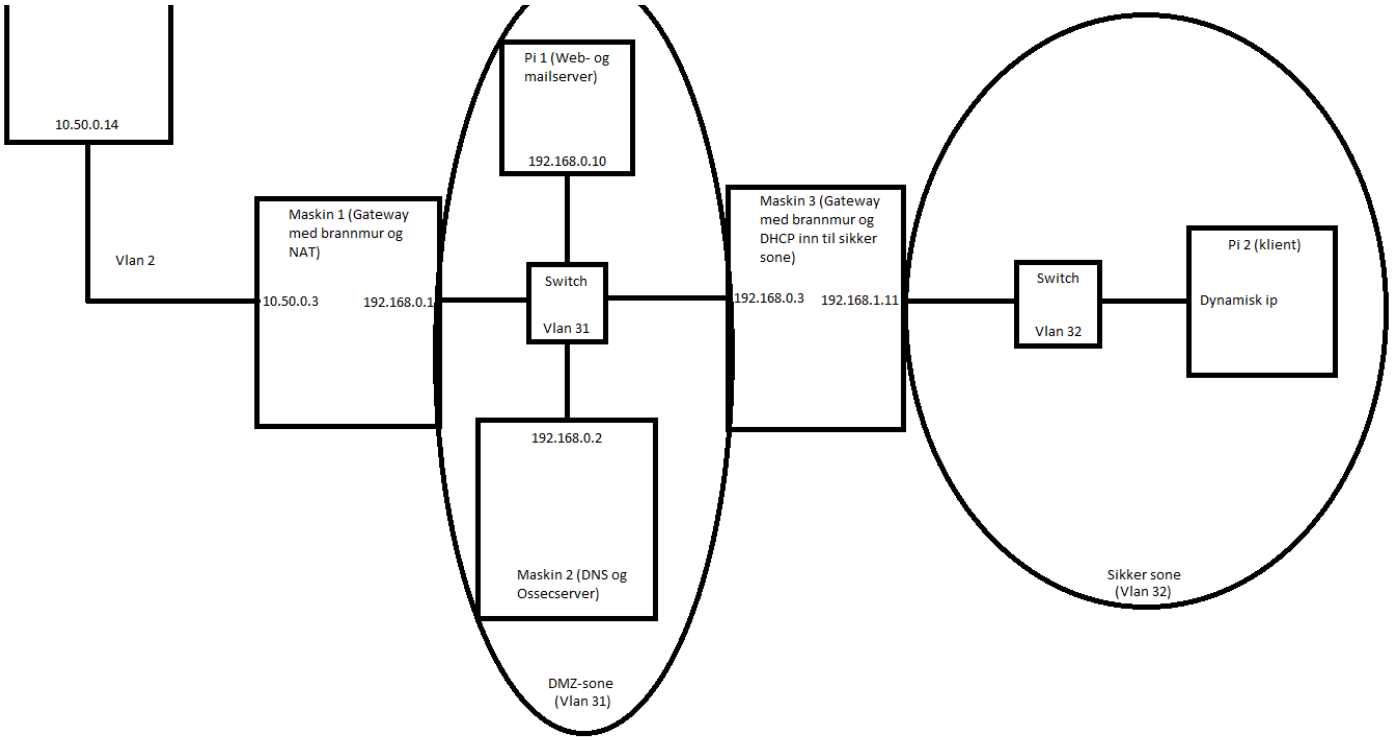
Denne rapporten tar for seg hvordan nettverket er blitt bygget opp i Bedrift3. Nettverket skal bestå av standard tjenester som webserver, mail, DHCP, NAT og DNS. Bedriften får tildelt en unik IP-adresse og det er derfor også nødvendig med en gateway med en NAT-funksjon for å kunne sette opp flere enheter i nettverket.

Nettverket må også være utstyrt med sikkerhetsmekanismer som brannmur og HIDS. Videre med tanke på sikkerhet deles nettverket inn i 2 subnett: DMZ, der de mindre konfidensielle tjenestene skal kjøre, og sikker sone, der klienter kobler seg på. Det benyttes en switch for å danne VLAN som deler nettverket i disse to delene.

1 Overblikk

Dette kapittelet gir et overblikk over bedriftens nettverk. Det gies en beskrivelse av dets struktur, samt en forklaring på hvordan switchen er satt opp og de virtuelle LANene i nettverket.

1.1 Nettverksstruktur



Figur 1.1 - Bedriftens nettverksstruktur

Figur 1.1 viser oppbygningen av nettverket til bedriften. I dette underkapittelet vil det bli gitt en overfladisk beskrivelse av dette nettverket, og i de resterende kapitlene gåes det mer i dybden på de forskjellige delene. Dersom figuren over blir for liten finnes det en større versjon i vedlegg 1.1.

Nettverket består av to /24 subnett: DMZ-sone og sikker sone. I DMZ finnes de servicene som skal være tilgjengelig utenfor LANet, slik som web- og mailserver. Inne i sikker sone finner man det som skal være godt beskyttet fra verden utenfor, slik som nettverkets klienter. DMZ har ip-adressene 192.168.0.0/24 tilgjengelig, mens sikker sone har 192.168.1.0/24 tilgjengelig. De to subnettene danner tilsammen et /23 subnett som er hele bedriftens nettverk.

1.2 Switch

For å kunne koble alle enhetene sammen til ett nettverk og dele dette opp i subnettverk, tas det i bruk en switch. Switchen har 52 porter og har mulighet for å sette opp virtuelle LAN. Dette ble tatt i bruk slik at den demilitariserte sonen (DMZ) og sikker sone er på ulike LAN.

1.2.1 Trunk

For å simulere ulike LAN i samme switch kan en benytte trunk. Dette er noe som konfigureres i switchen og gjør det mulig å si hvilke virtuelle LAN som kan hentes på hvilke porter. Trunk kan benyttes for å overføre et LAN til en annen switch, eller sette opp en port i switchen som LANet kan hentes fra. På denne måten hentes WAN inn på den oppsatte gateway-maskinen og VLANet til den demilitariserte sonen. Maskinen inn til sikker sone henter ned VLANet til demilitarisert sone og VLANet til sikker sone.

1.2.2 Porter

Portene benyttet på switchen er fra og med 31 til og med 35. Over er det nevnt noen av VLANene som tas i bruk på ulike maskiner. Under, i figur 1.2, er det en fullstendig oversikt over hvilken fysisk port som er brukt, hvilken maskin den er tilkoblet, hvilke VLAN-tagger som er brukt og IP-adresser.

Port på switchen	Maskin	Servicer	Vlan-tag(er)	IP-adresse(r)
31	Maskin 1	Gateway Brannmur NAT	2, 31 (trunk)	10.50.0.3 192.168.0.1
32	Maskin 2	DNS HIDS	31	192.168.0.2
33	Maskin 3	Gateway Brannmur NAT DHCP	31, 32 (trunk)	192.168.0.3 192.168.1.11
34	Pi 1	Webserver Mailserver	31	192.168.0.10
35	Pi 2	-	32	Dynamisk

Figur 1.2 - Oversikt over maskiner

2 Gateway

I et bedriftsnettverk er det absolutt nødvendig med en gateway som tar hånd om alle inn- og utgående forespørsler. En gateway er en funksjon i de aller fleste rutere, men det er også mulig at en datamaskin fungerer som en gateway.[1] I denne bedriften er gatewayen satt opp på en maskin. Gatewayen har som oppgave å videresende pakker til riktig destinasjon og kaste pakker som ikke har lov til å videresendes.[2:360] En ruter forkaster pakker som er sendt fra private IP adresser, pakker som har “time to live” lik 0 og pakker den ikke vet hvor den skal sende [3].

En gateway må ha minst 2 interfacer: ett som alle innkommende pakker kan sendes til og et interface som alle utgående pakker kan sendes til. Gatewayen har som oppgave å pakke opp linklag-headeren og lese av IPv4-headeren. Utifra hva som står i IPv4-headeren, så kan den sjekke destinasjonsadressen opp mot sin rutingtabell. Når ruteren vet hvor pakken skal sendes så forwardes pakken til riktig output link / interface. I tillegg gjør den små endringer på IPv4-headeren, som å dekrementere “time to live” og utføre en error check på header-checksum [3]. Før pakken sendes videre så kapsuleres den, det betyr at det legges på en ny link header. Da legger gatewayen inn sin egen mac-adresse som source-adresse, og neste ruter sin mac-adresse som destinasjon adresse [4]. Så sendes pakken ned på linklaget igjen, hvor den finner frem vha. mac-adressen til neste ruter [2].

2.1 Brannmur

En brannmur er nødvendig i et bedriftsnettverk. Den har ansvar for å overvåke og kontrollere innkommende og utgående trafikk basert på reglene i brannmuren [5]. Brannmuren befinner seg mellom OS’et og hardware [2]. Reglene kan settes i brannmuren vha. “firewalld” i Centos 7 [6]. Det har bare blitt åpnet noen brukte porter og de viktigste servicene.[7] Se vedlegg 2.1 for reglene som er satt.

2.2 NAT

Bedriften har fått tildelt en unik IP-adresse (10.50.0.3), det er derfor nødvendig med NAT på enheten som benytter seg av denne. Hele nettverket gjemmer seg bak denne IP-adressen. Alle trafikk som sendes ut fra nettverket har derfor denne IP-adressen som source-adresse. Gatewayen har to interfacer, en med IP 10.50.0.3 som kan nåes fra utsiden av nettverket og en med 192.168.0.1 som er gateway for maskinene på innsiden av nettverket. Når en pakke sendes fra innsiden av nettverket, så blir de sendt til 192.168.0.1 på gateway maskinen, her blir den private IP-adressen og port lagret og pakken blir så sendt videre ut i nettverket med 10.50.0.3 som source-adresse [2:375-378]. For oppsett av NAT i gateway se vedlegg 2.5 [8].

2.3 Port-forwarding

Bedriften har de viktigste tjenestene sine i DMZ. Noen av disse tjenestene må være tilgjengelig utenfra, f.eks webserver. Det er derfor nødvendig å benytte seg av port-forwarding. Port-forwarding er en metode for å gjøre tjenester inne på det private nettverket bak en ruter tilgjengelig fra utsiden.[9] Det har blitt satt opp en port forward til webserver, se vedlegg 2.4. Figur 2.1 gir en oversikt over de forskjellige port-forwardingene som har blitt satt opp.

Port på gateway	Intern IP	Port på maskin
2222	192.168.0.2	22
3333	192.168.0.3	22
4444	192.168.0.10	22
8080	192.168.0.10	80

Figur 2.1 - Port-forwarding

3 DMZ-sone

I DMZ (Demilitarisert sone) finnes det som skal være tilgjengelig utenfor bedriftens nettverk. Kostnaden ved dette er noe redusert sikkerhet, da det er en begrenset mengde pakker som kan stenges ute for at tjenestene skal kunne fungere riktig. Dette medfører at sensitiv informasjon og klienter heller vil plasseres i sikker sone enn her.

Det er hovedsakelig fire tjenester bedriften opererer med i DMZ-sonen: DNS, webserver, mailserver og Ossec-server. Disse er i bedriften fordelt på en servermaskin og en Raspberry Pi. Maskinen har statisk IP-adresse 192.168.0.2 og pi'en har adresse 192.168.0.10. Detaljer om de forskjellige tjenestene dekkes i de neste underkapitlene.

3.1 DNS

DNS er en tjeneste som knytter domenenavn sammen med IP-adressen til en tjener på internett.[10] DNS er organisert i et hierarkisk system som ligner på en trestruktur. Øverst i dette hierarkiet er det 13 rotservere. Det er en av disse klienter først kontakter når de spør om IP eller domenenavn. Rotserveren sender så en IP adresse tilbake til klienten som tilhører en TLD (Top Level Down) DNS server. Disse serverne har ansvar for enkelte domener som com, org og net. Klienten spør en av disse TLD serverene og får tilbake en ny IP adresse som tilhører en autoritær DNS server. Disse autoritære serverene inneholder den informasjonen som klienten spør etter. [2:160-161] Dette er slik det er i stor skala. Tjenesten gjør det mulig for klientene å komme seg inn på webserveren ved å skrive inn bedrift3.usn istedenfor å skrive inn IP-adressen 192.168.0.10:80. Tjenesten er ikke nødvendig i seg selv, men gjør at klientene slipper å huske på IP-adressen til webserveren. Vedlegg 3.1 til 3.3 viser filene som setter opp vår DNS-server. [11]

3.2 Webserver

I bedriften var det behov for å ha en webserver tilgjengelig på lan og wan. Denne er derfor plassert i DMZ. Der står serveren innenfor gatewayens brannmur. Oppsettet setter ikke sikker sone i fare da denne har en egen gateway og brannmur. Dette beskrives nærmere senere.

Webserveren er satt opp ved hjelp av apache. Dette er et enkelt og mye brukt verktøy for å opprette websider. Valget falt på apache da dette er et velkjent og mye brukt verktøy, samt at gruppen har erfaring med det fra før. Med tanke på sikkerhet er det heller ikke noe problem å bruke apache.

For selve websiden ble Wordpress satt opp. Dette er et gratis og enkelt webside-verktøy hvor administrasjon av websiden gjøres i nettleseren. På siden er det lagt opp til en hovedside med info om bedriften, en link til eventuell blogg og en link videre til webmailen.

3.3 Mailserver

Ettersom bedriften også ønsket egen mail er det satt opp egen mailserver. Mailserveren er bestående av mail-tjenester som tar seg av sending og mottak av epost. Disse er dovecot og postfix. Dette er erfaringsmessig gode tjenester for å ivareta SMTP-, IMAP- og POP3 protokollene.

Over dovecot og postfix er det lagt et webmail-grensesnitt for å holde god oversikt over sendte og mottatte mailer, samt sende mail. Valget falt på squirrelmail, en enkel og lite ressurskrevende webmail-løsning. Grunnlaget for valg av en lite ressurskrevende webmail er at webserveren er satt opp på en Raspberry Pi. Det ble derfor prioritert å sette opp en stabil løsning fremfor noe mer avansert.

3.4 Ossec-server

Ossec HIDS (Host Intrusion Detection System) brukes for å detektere uvanlige og mistenkelige handlinger på maskinene. Ettersom sikkerhet i bedriftens nettverk er av stor betydning er det naturlig å installere dette i nettverket. Ossec er en mye brukt open source plattformuavhengig HIDS. Dette innebærer at den er lett tilgjengelig og går over ens med stort sett alle servere/enheter en ønsker å tilkoble nettverket.

Oppgaven til Ossec er å se gjennom filsystemet og logger som enhetene produserer [12]. Disse analyseres slik at dersom det forekommer mistenkelig aktivitet vil det klassifiseres i ulike trusselnivåer og det kan sendes en alarm i form av en mail.

I et større nettverk kan det være nyttig å ha dette systemet på alle enheter med data som ønskes å være sikret. Dette kan bli uoversiktlig å holde styr på med flere klienter. Dermed er det mulig å sette opp en Ossec-server for å samle informasjon fra alle klientene på nettverket med HIDS. Derfor er maskin 2 i demilitarisert sone installert med Ossec-server, mens resten av serverene i DMZ og sikker sone utstyrt med Ossec-agent. Agentene samler informasjon om sine filsystemer og logger for så å sende informasjonen videre til serveren [13].

4 Sikker sone

I sikker sone finnes klientene som er koblet til nettverket. Dette kan være de ansattes datamaskiner og andre servicer det er viktig at holder høy sikkerhet. For å opprettholde høy sikkerhet vil det kun være mulig å sende pakker til sikker sone om disse pakkene er relatert til pakker som opprinnelig stammer fra en klient inne i sikker sone. Dette vil bli forklart nøyere i kap. 4.1.

På nåværende tidspunkt finnes det kun en Raspberry Pi som fungerer som en klient inne i sikker sone, men det vil være enkelt å koble til flere klienter senere.

4.1 Gateway og brannmur

Gateway'en kobler sammen DMZ og sikker sone. Den har statisk IP-adresse 192.168.0.3 på interfacet ut til DMZ-sonen og 192.168.1.11 på interfacet inn til sikker sone. Brannmuren er satt opp slik at ingen trafikk slipper inn til sikker sone med mindre trafikken startet fra den sikre sonen.

For at klientene innenfor den sikre sonen skal kunne kommunisere med andre klienter innenfor samme sone eller utenfor må gatewayen være konfigurert for å kunne rute pakker. Hvordan dette er konfigurert vises i vedlegg 4.1. Når en klient sender en pakke blir den sendt til "default gateway", dersom destinasjonen er på samme LAN blir pakken sendt til klienten. Derimot hvis gatewayen ikke finner IP adressen på LAN-et blir pakken sendt videre til en annen router.

Routere inneholder tabeller med data, disse tabellene inneholder blant annet alle mulige ruter som routeren vet om og hvilke koblinger som leder til spesifikke IP adresser.[14] Denne informasjonen om nettverk og routere skaffes ved hjelp av routing protokoller og plasseres i tabellene i routerens minne. Routing-algoritmer blir så utført ut fra denne informasjonen for å finne beste vei mellom forskjellige nettverkene. [15]

4.2 DHCP

Siden klientene som skal kobles til bedriftsnettet befinner seg inne i sikker sone, ligger DHCP-servicen også i denne sonen. Nærmere bestemt ligger den på gateway-maskinen mellom DMZ og sikker sone, men deler bare ut IP-adresser til klienter i den sikre sonen. Det er ikke nødvendig å ha en DHCP-service i DMZ, da det her kun vil være noen få servicer som det er hensiktsmessig at har statiske adresser, slik at det enkelt kan finnes frem til disse.

Konklusjon

I rapporten er det beskrevet hvordan Bedritf3s nettverk er satt opp, hvilke tjenester det består av og hvorfor spesifikke tjenester er valgt. Det oppsatte nettverket med alle tjenester anses å dekke behovet Bedrift3 hadde til deres nettverk.

Bedrift3 er en liten bedrift og det er derfor forståelig og unødvendig at det ikke er for mange servere i nettverket. Dette både med tanke på økonomi og oversiktlighet. Under oppsettet er det derfor blitt vektlagt å legge de ulike tjenestene på fornuftige plasser i nettverket. Tjenester som brannmur, NAT og gateway er definert av bedriften selv, resten har gruppen tatt en avgjørelse på med tanke på hvor tjenestene er lagt.

Maskin 2 som er tilkoblet DMZ er på sett og vis hjertet av DMZ-sonen. Derfor er det sannsynlig at alle får kontaktet den. Den har kontakt med gateway-maskinen sin LAN-del og har en kobling inn til sikker sone. Denne blir et naturlig tilknytningspunkt som kan holde styr på de ulike IP-adresser i nettverket, porter og domener.

Videre er webserver og webmail lagt inn på en Raspberry Pi. Dette gjør at andre funksjoner som er vitale for selve nettverket holdes adskilt fra en nettside som typisk er åpen og muligens også brukes kommersielt. Denne kan være spesielt utsatt for hacking og en kan raskt stenge serveren uten at brukere mister internett, for eksempel.

Med tanke på sikkerhet sørger den installerte HIDSen for å monitorere alle agentene i nettverket. Ossec-serveren som innhenter alle dataene fra enhetene er lagt i hjertet av DMZ-sonen. Gruppen mener det er oversiktlig at DNS og Ossec-server er på samme maskin da dette er to store og/eller overordnede oppgaver. Ossec-serveren har også et webgrensesnitt installert som gjør det oversiktlig å holde orden på agentene. Oversikten er ikke tilgjengelig via nettsidene da det er viktig å skille på bruker-view og administrator-view. Mekanismer for dette er ikke implementert per nå, men kan enkelt gjøres ved en senere anledning.

Alt i alt er Bedrift3s nettverk per nå et velfungerende nettverk med de tjenester bedriften har behov for. Sikkerheten er ivaretatt slik at brukere i sikker sone kan føle seg trygge. Websiden er også enkel å administrere slik at nytt innhold enkelt kan tillegges og oppdateres.

Litteraturliste

[1] WhatIsMyIPAddress (u. dato). What is a Gateway? Tilgjengelig: http://whatismyipaddress.com/gateway Hentet: 21.04.2017

[2] J. F. Kurose og K. W. Ross. *Computer Networking, A Top-Down Approach, sixth edition*. Harlow: Pearson Education Limited, 2013

[3] Linfo. (2005) Time-to-live Definition. Tilgjengelig: http://www.linfo.org/time-to-live.html Hentet: 21.04.2017

[4] Cisco. (2016). *What happens when router recieves a packet*. Tilgjengelig: https://supportforums.cisco.com/blog/153276/what-happens-when-router-receives-packet

[5] Cisco. (u. dato). *What Is a Firewall?*. TIlgjengelig: http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. Hentet 19.04.2017

[6] Fedora Project. (2017). *FirewallD*. Tilgjengelig: https://fedoraproject.org/wiki/Firewalld?rd=FirewallD. Hentet 19.04.2017

[7] Digital Ocean. (2015). *How to set up a firewall using firewalld on Centos 7*. Tilgjengelig: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7. Hentet 19.04.2017

[8] Redbranch. (2015). *Centos 7 as nat gateway for private network*. Tilgjengelig: http://blog.redbranch.net/2015/07/30/centos-7-as-nat-gateway-for-private-network/. Hentet 20.04.2017

[9] Port Forward. (u. dato). *How To forward a Port*. Tilgjengelig: https://portforward.com/. Hentet 20.04.2017

[10] J. Halliday. (2010). *Explainer: what is 'DNS', why does it matter and how does it work?*. Tilgjengelig: https://www.theguardian.com/technology/2010/dec/03/dns-ip-ddos-explained. Hentet 21.04.2017

[11] LinuxPitStop. (2016). *How to Setup DNS Server Setup with Bind 9 on CentOS 7.* Tilgjengelig: http://linuxpitstop.com/dns-server-setup-using-bind-9-on-centos-7-linux/ Hentet: 21.04.2017

[12] OSSEC. (u. dato). *Getting started with OSSEC*. Tilgjengelig: https://ossec.github.io/docs/manual/non-technical-overview.html. Hentet 20.04.17

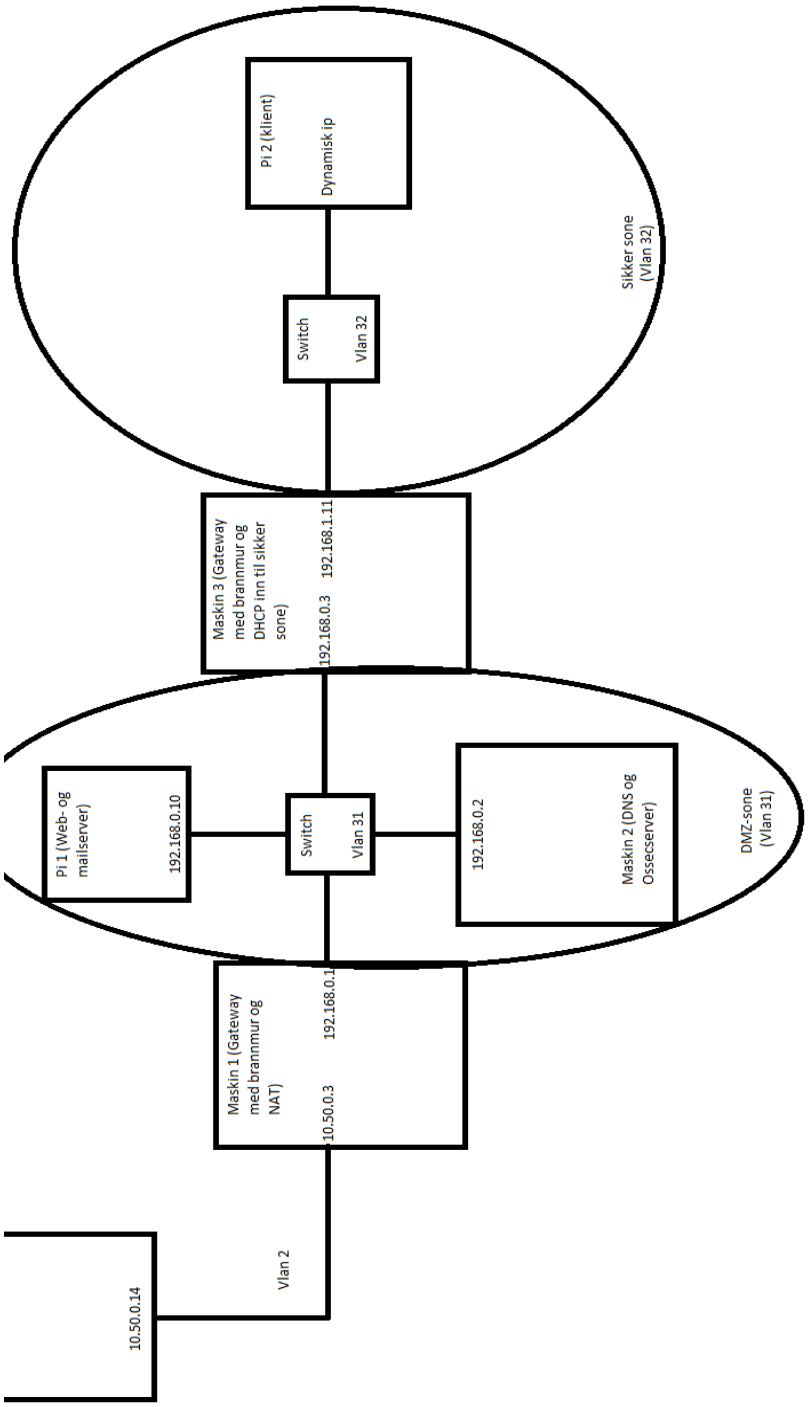
[13] OSSEC. (u. dato). *Agents*. Tilgjengelig: https://ossec.github.io/docs/manual/agent/index.html. Hentet 20.04.17

[14] Cisco. (u. dato). *Routing 101: The Basics*. Tilgjengelig: http://www.cisco.com/en/US/netsol/ns339/ns392/ns399/ns400/networking_solutions_white_paper0900aecd802d5489.shtml. Hentet 21.04.2017

[15] J. DiMarzio. (2002). *Routing 101: Routing Algorithms*. Tilgjengelig: http://www.informit.com/articles/article.aspx?p=27267. Hentet 21.04.2017

Vedlegg

1.1 Bedriftens nettverksstruktur, forstørret



2.1 Brannmurinnstillinger på gateway-maskin

firewall-cmd -- zone=dmz -- permanent -- add-service=http

firewall-cmd -- zone=dmz -- permanent -- add-service=https

firewall-cmd -- zone=dmz -- permanent -- add-service=smtp

firewall-cmd -- zone=dmz -- permanent -- add-service=pop3s

firewall-cmd -- zone=dmz -- permanent -- add-service=tftp

firewall-cmd -- zone=dmz -- permanent -- add-service=dns

firewall-cmd --zone=dmz --permanent --add-port=465/tcp

firewall-cmd --zone=dmz --permanent --add-port=25/tcp

firewall-cmd --zone=dmz --permanent --add-port=993/tcp

firewall-cmd -- zone=external -- permanent -- add-service=http

firewall-cmd -- zone=external -- permanent -- add-service=https

firewall-cmd -- zone=external -- permanent -- add-service=smtp

firewall-cmd -- zone=external -- permanent -- add-service=pop3s

firewall-cmd -- zone=external -- permanent -- add-service=dns

firewall-cmd --zone=external --permanent --add-port=1514/tcp

firewall-cmd --zone=external --permanent --add-port=143/tcp

2.2 Forwarding fra gateway til DMZ

firewall-cmd --permanent --zone=external
--add-forward-port=port=2222:proto=tcp:toport=22:toaddr=192.168.0.2

Gjør det mulig å koble seg til DMZ maskinen via SSH på port 2222.
ssh 10.50.0.3 –l root –p 2222

2.3 Forwarding fra gateway til sikker sone

firewall-cmd -- permanent -- zone=external -- add-forward-port=port=3333:proto=tcp:toport=22:toaddr=192.168.1.10

Gjør det mulig å koble seg til sikker sone maskinen via SSH på port 3333.
ssh 10.50.0.3 –l root –p 3333

2.4 Forwarding til dmz PI fra WAN

firewall-cmd --permanent --zone=external --add-forward-port=port=3333:proto=tcp:toport=22:toaddr=192.168.0.10

2.5 NAT i gateway

net.ipv4.ip_forward = 1
firewall-cmd --zone=external --add-masquerade --permanent
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o enp0s25.2 -j MASQUERADE -s 192.168.0.1/24

3.1 DNS - /etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        #listen-on port 53 { 127.0.0.1; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
```

```
        reduce such attack surface
    */
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "usn" IN {
    type master;
    file "fwd.usn.db";
    allow-update { none; };
};

zone "0.168.192.in-addr.arpa" IN {
    type master;
    file "0.168.192.db";
    allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

3.2 DNS - /var/named/fwd.usn.db

```
$TTL 86400
@ IN SOA primary.usn. 140434.hbv.no. (
2016042112 ;Serial
3600 ;Refresh
1800 ;Retry
604800 ;Expire
43200 ;Minimum TTL
)
 IN NS primary.usn.
primary IN A 192.168.0.2
www IN A 192.168.0.10
bedrift3 CNAME www
```

3.3 DNS - /var/named/0.168.192.db

```
$TTL 86400
@ IN SOA primary.usn. 140434.hbv.no. (
2014112511 ;
3600 ;
1800 ;
604800 ;
86400 ;
)
 NS primary.usn. ;jævla mellomrom ødela alt igjen
2 IN PTR primary.usn.
10 IN PTR www.usn.
```

4.1 Skru på ruting i gateway mellom DMZ og sikker sone

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```