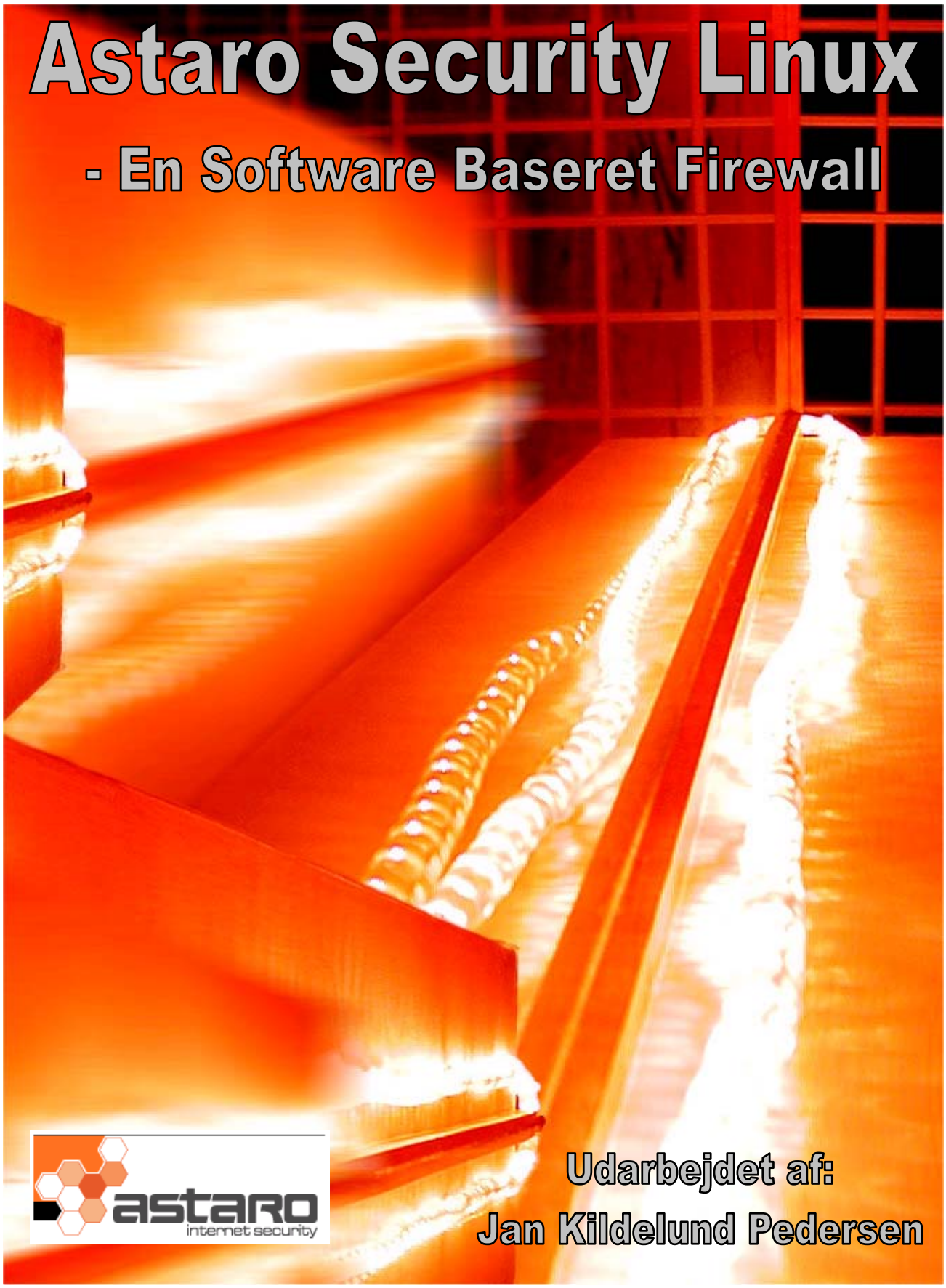
Astaro Security Linux

- En Software Baseret Firewall



Udarbejdet af:
Jan Kildelund Pedersen

Indholdsfortegnelse:

Indledning:

I Forbindelse med temaet firewall, har jeg valgt at undersøge software firewall'en Astaro Security Linux, fra ASTARO.

Formålet med denne rapport, er at jeg personligt gerne vil stifte bekendtskab med dette firewall produktet, dets egenskaber og muligheder. Samt beskrive de erfaringer jeg gør mig under installation og opsætning.

Endvidere ønsker jeg også at fremstille en rapport, som skal forklare hvad og hvordan man bruger Astaro Security Linux, og dermed skabe et overblik over det primær indhold i denne firewall-løsning, hvilket der skal gøre interesserede i stand at se, om dette produkt ville dække deres sikkerhedskrav og behov.

Kort om Astaro Security Linux:

Astaro Security Linux er et stykke software, som er udviklet af et tysk firma ved navn Astaro. Astaro blev grundlagt i Januar 2000, og Astaro Security Linux er i dag implementeret i over 10.000 organisationer.

Astaro Security Linux er en Software firewall, som kør på en Linux kerne. Selve firewall'en funktionen er baseret på Linux's egen IPTables, som er en kommando baseret applikation til opsætning af regler og parameter for TCP/IP-protokolen.

Astaro Security Linux kan erhverves for ca. 2500,00 kr. og op efter, alt afhængige af ønskede ekstra moduler.
Det er dog muligt at hente en gratis og funktions dygtig evaluerings version far Astaro's Website, dog uden nogen ekstra moduler med, og den kan kun benyttes i 30 dage. Denne udgave er benyttet til udarbejdelsen af denne rapport.

Hvad er en firewall?

En firewall er en enhed, der har som funktion at overvåge alt trafik, til og fra computer/netværk efter bestemte regler.
Når firewall'en er installeret føres al kommunikation gennem denne og bliver dermed computeren/netværkets "dørmand".
For at kunne tillade eller afvise trafik fra Internet eller interne programmer, arbejder firewall'en efter nogle foruddefinerede regler. En sådan regel kan for eksempel være, at et ikke-godkendt program ikke kan få lov til at kommunikere til eller fra Internet.

Rent fysisk kan en firewall være konstrueret på 2 måder!

- Software
  - En Software applikation som er installeret på den enkelt PC, kaldet en ”Personlig Firewall”.
  - En Software service, som er installeret på en PC/Server, der er placeret på samme måde som en hardware firewall.

- Hardware
  - En hardware enhed, som rent fysisk kobler 2 eller flere netværk sammen. I nogle tilfælde vil sådan en firewall, bestå af en ”lille PC”, med f.eks. et Linux operativ system med en firewall applikation installeret!

Hvorfor skal man bruge en firewall?

Behovet for at beskytte virksomhedens netværk mod angreb ude fra, stiger i takt med udbredelsen af højhastigheds Internetforbindelser.

Er Deres virksomheden koblet på nettet 24 timer i døgnet, vil firmaets data netværk være i fare
for hacking og datatyveri, hvis ikke det beskyttes.

I dag anvendes ofte en firewall som beskyttende led mellem det lokale netværk og Internettet.
Firewall´ens opgave er at sørge for, at kun godkendt trafik passerer mellem det lokale netværk
og Internettet.

Hidtil har en firewall været en dyr investering, da dette har krævet høj teknisk ekspertise samtidig med et stort budget til vedligehold og opdatering af både viden og software.

Men da efterspørgslen er steget efter firewalls, er der kommet flere produkter på markedet, deriblandt Linux produkter som f.eks. Astaro Security Linux fra det tyske firma ASTARO.

Installation af “Astaro Security Linux”.

Firewall Maskine:
Pentium 166MMX
128 Ram
3,2 GB Harddisk
3 x 10/100 Netkort

Installation forgår meget nemt og hurtigt!
Man henter programmet fra Astaro’s Website i form af et CD-billede som så skal brændes ud på en cd, og der genereres så en ”boot-bar” installations cd.

Derefter sættes installations cd’en i den maskine man ønsker som firewall, og boot’er maskinen hvorefter installationen startes automatisk!(Husk at Boot fra CD-ROM)
(Hertil skal dog nævnes, af installationen af Astaro Security Linux, beslaglægger hele maskinen, og alt i forvejen installeret data , bliver dermed slettet!)

Installation er forholdsvis kort, og kræver ikke det stor kendskab til hverken Linux eller maskinens opbygning!
Dog er det en fordel hvis man har alle hardware komponenter installeret, da der bliver fortaget en scanning af maskinen, hvorefter der så bliver installeret de tilhørende software driver/komponenter.

Det eneste man skal konfigurere er placering, klokken, og ip-konfigurationen af et enkelt netkort til den kommende opsætning.

Når installationen er færdig fjernes cd’en fra cd-rom drevet, maskinen genstartes, og er nu klar til endelig opsætning via en Web-browser placeret på hvilken som helst klient, som er tilkoblet og konfigureret på det samme net, som det netkort der blev defineret under installationen af firewall’en.

Opsætning af Astaro Security Linux

Web Administration:

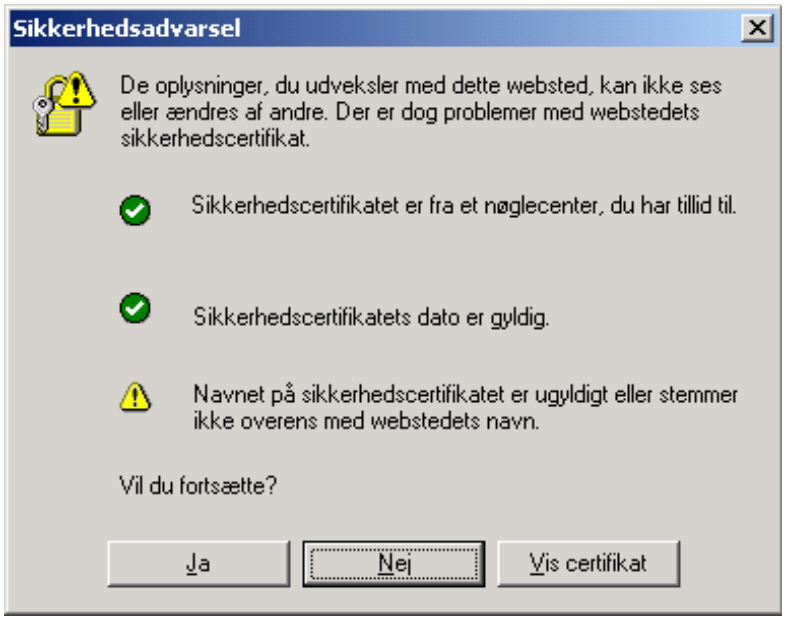
Når firewall'en er startet op, vil den prompte med Login, og der vil lyde 3 beep fra firewall'en.
Her efter er det ikke nødvendigt at fortage sig mere lokalt ved maskinen.
Den videre opsætning og administration af Astaro, forgår gennem en web-browser på en klient tilkoblet firewall'en.

Forbindelsen fra Web-browseren, skabes ved hjælp af en sikret http forbindelse således:

Syntaks:
https://<ip-adressen>

Eks.
HTTPS://192.168.1.100

Herefter skal sikkerheds certifikatet accepteres, og der skal logges ind for første gang, hvor der samtidig oprettes bruger og defineres passwords.



Efter der er logget ind, bliver man præsenteret for hovedmenuen, hvor man har de forskellige valgmuligheder ude i venstre side!
Ønsker man at have flere menubjælker åbne på samme tid, er der en lille tegnestift i hver bjælke, som ved et klik, vil tvinge den åben hele tiden!

Opsætning af Net/Netkort:

Det første man bør gøre, er at oprette de ønskede net-segmenter, som firewall'en skal beskæftige sig med.
Dette gøres under "Network", også "Interfaces".
Nederst på denne side, er der en liste over de netkort som er installeret på firewall'en.
Her opretter man så de enkelte net, og konfigurere dem med adresser m.m. efter ønske.
Her opretter man normalt efter en struktur med 3 net: (se også Bilag 1)

Current Interface Status — New ...

Admin	Oper	Name/Type	Parameters	Actions
	Up	**DMZ** (Standard ethernet interface) on **eth2** (Intel Corp.82557/8/9 [Ethernet Pro 100])	192.168.20.1 / 255.255.255.0 Gateway: none	**edit** **delete**
	Up	**External** (Standard ethernet interface) on **eth1** (Intel Corp.82557/8/9 [Ethernet Pro 100])	192.168.1.100 / 255.255.255.0 Gateway: 192.168.1.1	**edit** **delete**
	Up	**Internal** (Standard ethernet interface) on **eth0** (Intel Corp.82557/8/9 [Ethernet Pro 100])	192.168.10.1 / 255.255.255.0 Gateway: none	**edit** **delete**

Sys ID

Sys ID	Name/Parameters	PCI Device ID
eth0	Intel Corp.82557/8/9 [Ethernet Pro 100] base=fe3ff008 irq=10 mac=00:A0:C9:3A:4D:46 type=eth io=0000	10.0
eth1	Intel Corp.82557/8/9 [Ethernet Pro 100] base=fe3fe008 irq=9 mac=00:A0:C9:42:89:BA type=eth io=0000	12.0
eth2	Intel Corp.82557/8/9 [Ethernet Pro 100] base=fe3fd008 irq=11 mac=00:A0:C9:42:71:40 type=eth io=0000	14.0

Nederst ses de installerede netkort, og øverst ses de oprettede net, med tilhørende konfiguration

Intern:

Det interne net er her alle arbejdsstationer er placeret, og er derfor her man ønsker at sikkerheden skal være maksimal. Det vil sige at udefrakommende ikke på nogen måder må kunne få adgang her til!
Intern defineres derfor som værende "Grøn".

DMZ:

De-Militarized Zone(DMZ), er der hvor man normalt placere f.eks. WEB- Og FTP servere, som man ønsker tilgængelige for udefrakommende.
På denne side at netværket, skal sikkerheden selvfølgelig også være i top, men da der er delvis åben for trafik udefra, er der også risiko for at udefrakommende skaber sig adgang til hele nettet, gennem diverse software fejl, huller, trojanskeheste og viruser. Derfor tages der ingen chancer, og nettet adskilles fra det interne net.
DMZ defineres derfor som værende "Gul".

Ekstern:

Det eksterne net, er den usikre side, som for det meste vil være Internettet. Men kan også være et hvilket som helst andet netværk, som man ønsker at sikre sig fra!
Ekstern defineres derfor som værende ”Rød”.

Definitioner:

Astaro er opbygget på den måde, at man definere alle værdier og parameter så som netkort, netværk, adresser og porte under ”Definitioner”, så det er nemmere at overskue. Og derefter benyttes disse definitioner når der skal oprettes regler m.m.

Når man vælger Menu’en definitioner, får man yderlige nogle menupunkter frem:

Networks:

Under ”Networks”, defineres enkeltstående ip-adresser som man ønsker at benytte når der f.eks. skal konstrueres regler for enkelte ip-adresser, da det ikke er muligt at angive ip-adresser når selve reglen eller parameteren konstrueres. Dette er gælder ligeledes for ip-net og ip-subnet.

Add Network

Name: IP address: Subnet mask: Add

Hint: to create a host entry, use the subnet mask 255.255.255.255 (or 32)

Name	IP address	Subnet mask	Command
Administrator	192.168.1.101	255.255.255.255	edit del
PPTP-Pool	10.113.233.0	255.255.255.0	edit del
Server_IP_192_168_20_2_bag_DMZ	192.168.20.2	255.255.255.255	edit del
Any	0.0.0.0	0.0.0.0	static
DMZ_Broadcast__	192.168.20.255	255.255.255.255	static
DMZ_Interface__	192.168.20.1	255.255.255.255	static
DMZ_Network__	192.168.20.0	255.255.255.0	static
External_Broadcast__	192.168.1.255	255.255.255.255	static
External_Interface__	192.168.1.100	255.255.255.255	static
External_Network__	192.168.1.0	255.255.255.0	static
Internal_Broadcast__	192.168.10.255	255.255.255.255	static
Internal_Interface__	192.168.10.1	255.255.255.255	static
Internal_Network__	192.168.10.0	255.255.255.0	static
localhost	127.0.0.1	255.255.255.255	static
localnet	127.0.0.0	255.0.0.0	static
NTP_Server_Atlanta	130.207.244.240	255.255.255.255	static
NTP_Server_Berlin	130.149.17.21	255.255.255.255	static
NTP_Server_Bern	193.5.216.14	255.255.255.255	static
NTP_Server_Canberra	137.92.140.80	255.255.255.255	static
NTP_Server_Colorado	204.34.198.40	255.255.255.255	static
NTP_Server_Erlangen	131.188.3.220	255.255.255.255	static
NTP_Server_Fukuoka	133.100.9.2	255.255.255.255	static
NTP_Server_Hong Kong	137.189.6.18	255.255.255.255	static
NTP_Server_Palo_Alto	192.5.5.250	255.255.255.255	static
NTP_Server_Rocquencourt	192.93.2.20	255.255.255.255	static
NTP_Server_Saskatchewan	142.3.100.2	255.255.255.255	static
NTP_Server_Stockholm	192.36.143.151	255.255.255.255	static
NTP_Server_Washington_DC	192.5.41.209	255.255.255.255	static
Private_Network_10.0.0.0	10.0.0.0	255.0.0.0	static
Private_Network_172.16.0.0	172.16.0.0	255.240.0.0	static
Private_Network_192.168.0.0	192.168.0.0	255.255.0.0	static

Definerede Adresser og Net, som senere benyttes under videre konfiguration!

Services:

Princippet er det samme for Services, her opretter man profiler for net-applikationer, ved at definere Source og Destination nummer på de port der benyttes, og hvilken protokol de benytter.

Name	Protocol	S-Port/Client	D-Port/Server	Command
ftpjan	udp	1024:65535	1900	edit del
ICQ	tcp	1024:65535	5190	edit del
MSNM Text	tcp/udp	1024:65535	1863	edit del
netbios_ekstra	tcp/udp	1024:65535	137	edit del
skype	tcp/udp	1024:65535	33033	edit del
Any	any	0:65535	0:65535	static
AUS	tcp	1:65535	222	static
BGP	tcp	1024:65535	179	static
CITRIX	tcp	1024:65535	1494	static
DNS	tcp/udp	1:65535	53	static
EUDORA	tcp	1024:65535	106	static
FTP	tcp	1024:65535	20:21	static
FTP-CONTROL	tcp	1024:65535	21	static
HBCI	tcp	1024:65535	3000	static
HTTP	tcp	1024:65535	80	static
HTTPS	tcp	1024:65535	443	static
IDENT	tcp	1024:65535	113	static
IMAP	tcp	1024:65535	143	static
IRC	tcp	1024:65535	6667:6668	static
ISAKMP	udp	500	500	static
LDAP_TCP	tcp	1024:65535	389	static
LDAP_UDP	udp	1024:65535	389	static
LOCAL_ALL	tcp/udp	1:65535	1:65535	static
LOTUSNOTES	tcp	1024:65535	1352	static
Microsoft-SMB	tcp/udp	1:65535	445	static
Microsoft-SQL_Monitor	tcp/udp	1:65535	1434	static
Microsoft-SQL_Server	tcp/udp	1:65535	1433	static
netbios-dgm	tcp/udp	138	138	static
netbios-ns	tcp/udp	137	137	static
netbios-ssn	tcp/udp	1024:65535	139	static
NEWS	tcp	1024:65535	119	static
NNTP	tcp	1024:65535	119	static
NTP	udp	123	123	static
NTP-Async	udp	1024:65535	123	static
Oracle	tcp	1024:65535	1522	static
Oracle_SQL_NET	tcp	1024:65535	1529	static
Oracle_SQL_NET_v1	tcp	1024:65535	1525	static
Oracle_SQL_NET_v2	tcp	1024:65535	1521	static
POP3	tcp	1024:65535	110	static
PPTP	tcp	1024:65535	1723	static
RIP	udp	520	520	static
SMTP	tcp	1024:65535	25	static
SNMP	udp	1024:65535	161	static
SQUID	tcp	1024:65535	8080	static
SSH	tcp	0:65535	22	static
Sybase-SQL	tcp/udp	1:65535	1498	static
SYSLOG	udp	514	514	static
TCP_UDP_ALL	tcp/udp	1024:65535	1:65535	static
Telnet	tcp	1024:65535	23	static
traceroute-udp	udp	1024:65535	33000:34000	static
WHOIS	tcp	1024:65535	43	static
WHOIS_PP	tcp	1024:65535	63	static
XDMCP	tcp	1024:65535	177	static

Her ses de mest anvendte Services(port), med tilhørende protokoller, ind- og udgående portnummer

Der er pr. default defineret de mest alm. applikationer så disse ikke skal oprettes igen.

For både Network og Services, er det muligt at konstruere grupper, så man kan lave fælles regler for flere networks og services på en gang.

Users:

Det sidste punkt hør til administreringen af bruger, som skal have kontakt til firewall'en, hvad enten det vedrøre administration, PPTP eller nogle at de andre funktioner der kræver verifikation.

Network:

Her begynder så den egentlige konfiguration af firewall'en, hvor man tydeligt vil kunne se hvor fleksible Astaro Security Linux er.
Da alt hvad man ønsker at arbejde med i denne firewall netop er defineret under definitioner, er det faktisk muligt at lave næsten alt på alle de oprettede net.

Interfaces:

Dette punkt har vi allerede stiftet bekendtskab med, da det er her man opretter og konfigurere firewall'ens net/netkort.

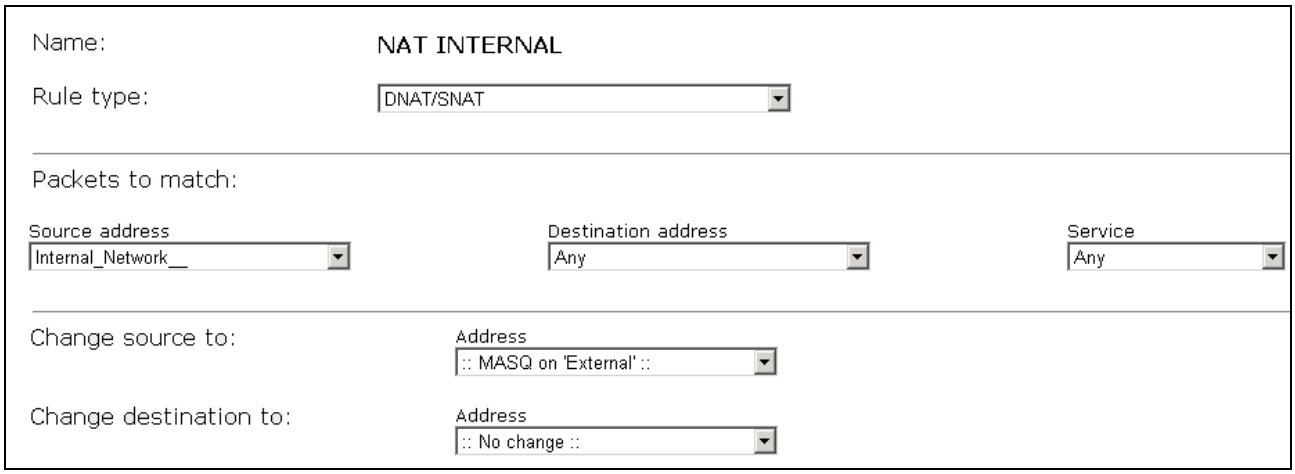
Routing:

Da der er indbygget routerfunktion i Astaro, er det her muligt at tilføje yderlige informationer, hvad angår routening af trafik på netværket.
Dette benyttes meget simpelt, ved at vælge det netværket der skal routes til, og gateway'en der skal benyttes.

NAT/Masquerading:

Da man for det meste kun har en ip-adresser tilgængelig på den eksterne side af firewall'en, er der mulighed for at benytte Network Adresse Translation(NAT), som sørge for at alle på den interne side at firewall'en, har mulighed for at kommunikere ud på den eksterne side, ved kun at bruge den ene ip-adresse, som firewall'en benytter.
Dette forgår ved at man definere afsender og modtager af ind- og udgående trafik, og for hvilke net applikationer(porte) det skal gælde.

Eksempel på NAT Mellem Intern- og Ekstern net



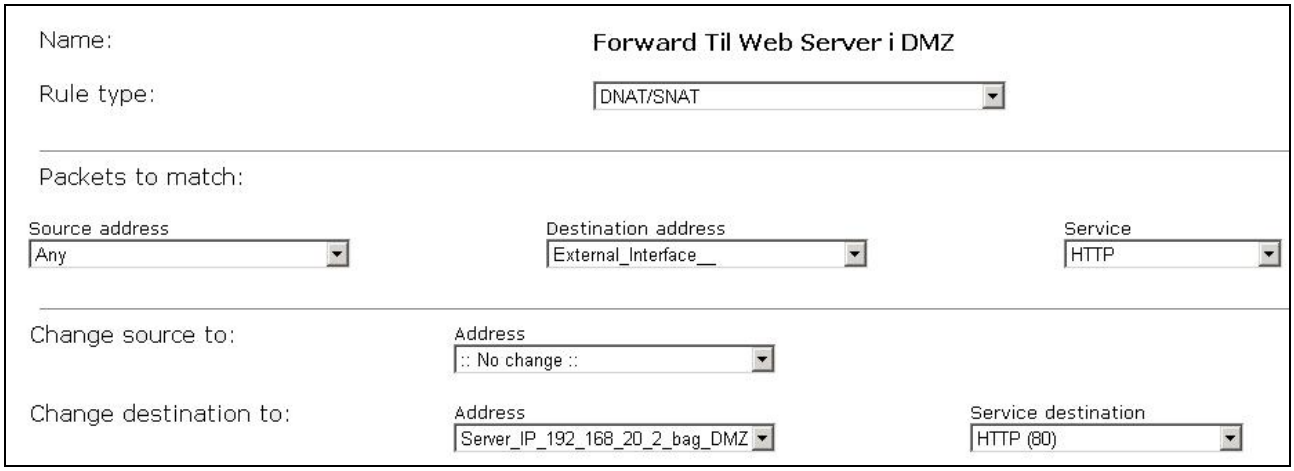
Her er bliver alt trafik fra det det interne net, MASQ på det Eksterne net, uden at Destinationen ændres, samtidig holder NAT øje med hvad der er sendt, så det kommer tilbage til den rigtige afsender!

Det betyder at man kan sætter regler op for ind og udgående trafikken, og derved bevare kontrollen og dermed sikkerheden. Hvilket er idéen med en firewall.

Port Forwarding:

Da det er her trafikken dirigeres, er det så også her man konfigurere Port Forwarding.
Port Forwarding er nødvendigt når man ønsker specifik udefrakommende trafik, sendt ind til en specifik adresse placeret på f.eks. DMZ nettet .
Det kunne f.eks. være WEB-, MAIL-, og FTP-servere.
Dette gøres på samme måde, ved at definere afsender og modtager på ind- og udgående trafik for specifikke net-applikationer(porte):

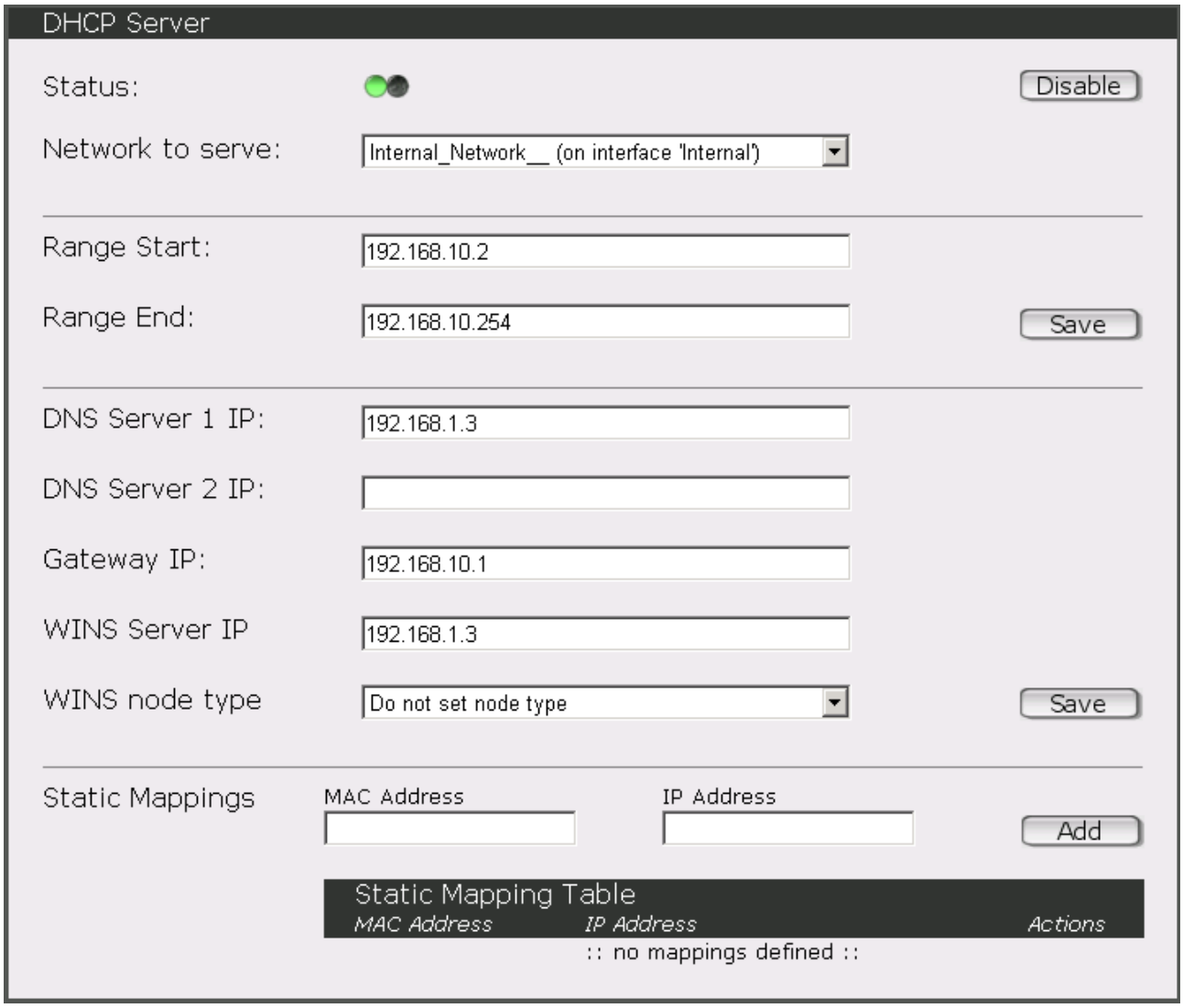
Eksempel på port Forwarding til en Web-server:



Her bliver alt http(80) trafik, som er blevet sendt til firewall'ens eksterne side, videresendt til den defineret destination på port 80.

DHCP Server:

I Astaro er det muligt at konfigurere en DHCP server, som automatisk tildeler oplysninger som f.eks. IP-adresse, gateway, DNS server m.m., til maskiner på et netværk.
Det valgte net vil normalt være det interne net, da maskinerne på DMZ netværket altid skal befinde sig på den samme IP-adresse, og derfor vil være konfigureret manuelt med statiske ip-adresser.



På Billedet ses en konfiguration af DHCP-Serveren, der er aktiveret på det intene netværk!

PPTP RoadWarrior Access

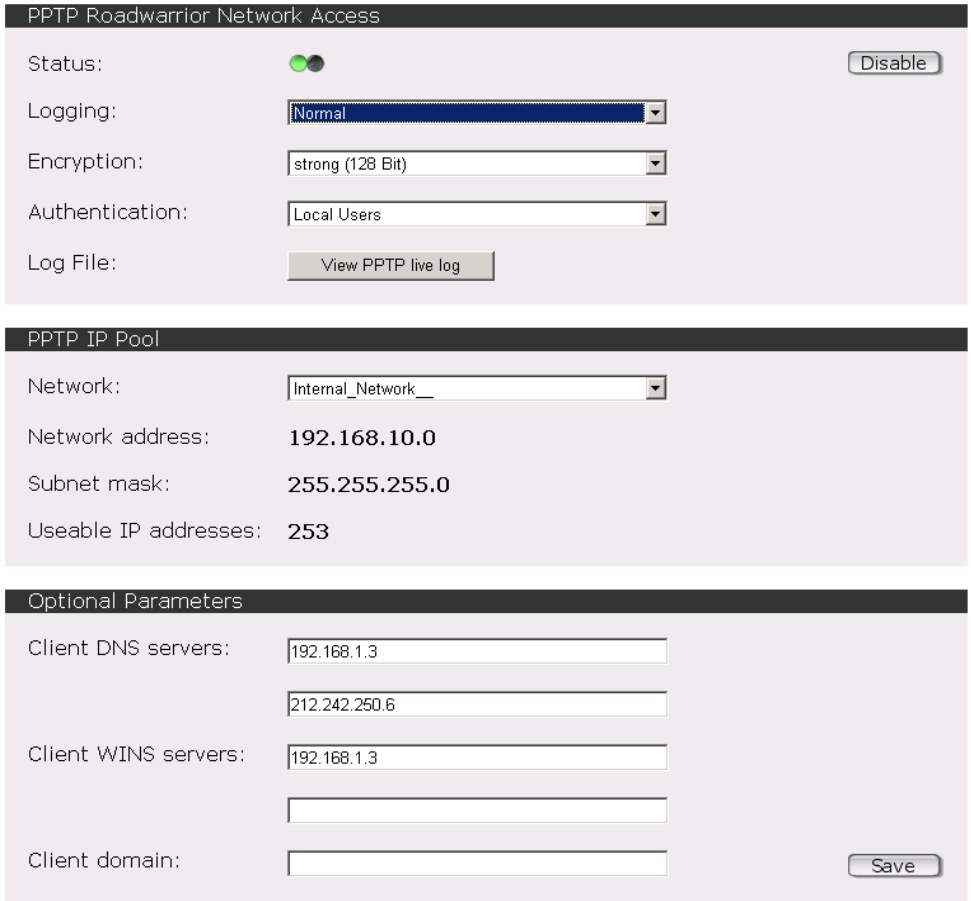
Når PPTP (Point-to-Point tunneling protokol) er aktiveret, er det muligt for enkeltstående klienter at etablere en krypteret tunnel forbindelse til netværket fra f.eks. det eksterne net.

Disse Klienter vil typisk være Microsoft Windows klienter. For at etablere en PPTP Forbindelse, er det nødvendigt at oprette en bruger med rettigheder til dette, se Definitions->Users.
Klienterne skal dog understøtte MSCHAPv2 godkendelse.

Du kan sætte tunnel krypteringen (MPPE) til enten strong(128 Bit) eller weak(40 Bit).
Det anbefales dog ikke at bruge weak, med mindre endepunktet ikke understøtter 128 Bit!

Når du aktiverer PPTP første gang, genereres et tilfældig netværk, som vil blive brugt udelukket til de klienter der etablere sådanne forbindelser.
Det er muligt at konstruere sit eget Netværk under Definitions->Networks, eller bare vælge et af de i forvejen konstruerede net, som f.eks. Intern.

En anden mulighed er, at specificere en ip-adresse til hver enkelt oprettet bruger under oprettelsen af brugeren. Denne ip behøver ikke være fra det, i PPTP-opsætningen, valgte Netværk, og klienten behøver heller ikke at konfigureres med denne ip, dette tildeles automatisk under etableringen af forbindelsen!



Ovenfor ses opsætningen af PPTP-Serveren, som gør det muligt for et utal at enkeltstående klienter, at koble sig til netværket via en PPTP-Tunnel Forbindelse!

Packet Filter:

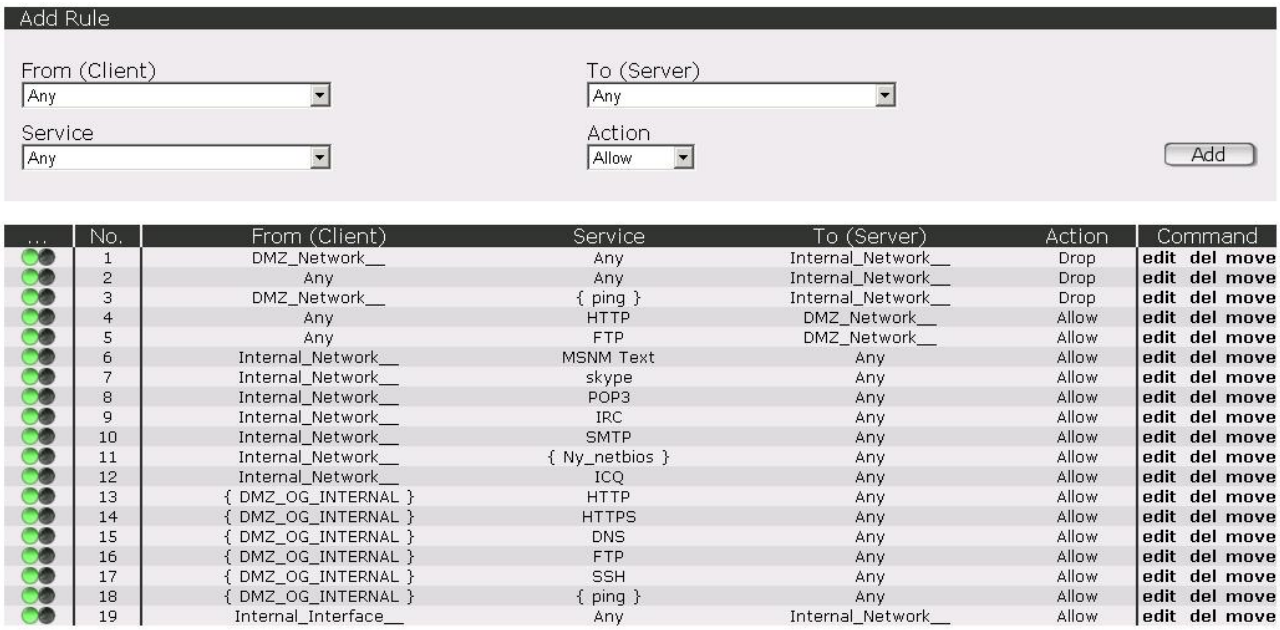
Ud over at en firewall kan administrere og videresende Netværks trafik til bestemte destinationer, er dens primær opgave at kontrollere indholdet i denne trafik. Astaro giver os her mulighed for at tillade eller nægte adgang af specificeret trafik(porte).
Dette gør en firewall ved at opsamle alt transmitteret data, og sammenligne det med de regler som er fastsat, og så enten stoppe det, eller lade det fortsætte vidre.

Disse regler er forholdsvis nemme at konstruere. Det kræver selvfølgelig, at man kender de fornødne informationer om den trafik man ønsker at sætte regler for.

From(Afsender) – To(Modtager):
Her vælges afsenderen og modtager for de pakke man ønsker reglen skal gælde for. Disse skal som næsten alt andet, defineres under definitioner enten som enkeltstående, en gruppe eller begge dele. Derved behøver man normalt kun at lave en regel for hver type trafik (port).

Service(Port):
Under Service vælger man den ønskede profil, som reglen skal gælde for.
Det er her selve indholdet af trafikken vælges. Denne parameter skal også defineres under definitioner.

Action:
Her vælger man hvad der skal ske når netop denne form for trafik forekommer.
Normalt vil man vælge ”allow” eller ”drop”, men der er også mulighed for at få specielle data registreret i logfiler, hvor man så har mulighed for at overvåge trafikken.



...	No.	From (Client)	Service	To (Server)	Action	Command
	1	DMZ_Network__	Any	Internal_Network__	Drop	edit del move
	2	Any	Any	Internal_Network__	Drop	edit del move
	3	DMZ_Network__	{ ping }	Internal_Network__	Drop	edit del move
	4	Any	HTTP	DMZ_Network__	Allow	edit del move
	5	Any	FTP	DMZ_Network__	Allow	edit del move
	6	Internal_Network__	MSNM Text	Any	Allow	edit del move
	7	Internal_Network__	skype	Any	Allow	edit del move
	8	Internal_Network__	POP3	Any	Allow	edit del move
	9	Internal_Network__	IRC	Any	Allow	edit del move
	10	Internal_Network__	SMTP	Any	Allow	edit del move
	11	Internal_Network__	{ Ny_netbios }	Any	Allow	edit del move
	12	Internal_Network__	ICQ	Any	Allow	edit del move
	13	{ DMZ_OG_INTERNAL }	HTTP	Any	Allow	edit del move
	14	{ DMZ_OG_INTERNAL }	HTTPS	Any	Allow	edit del move
	15	{ DMZ_OG_INTERNAL }	DNS	Any	Allow	edit del move
	16	{ DMZ_OG_INTERNAL }	FTP	Any	Allow	edit del move
	17	{ DMZ_OG_INTERNAL }	SSH	Any	Allow	edit del move
	18	{ DMZ_OG_INTERNAL }	{ ping }	Any	Allow	edit del move
	19	Internal_Interface__	Any	Internal_Network__	Allow	edit del move

Oven for ses et opbygget regelsæt, hvor der bl.a. er givet adgang til MSN Messenger, Web, FTP og mail m.m..

Listen er prioritets opbygget, så de regler der er placeret øverst, overskriver dem under.
Derfor er alle nægtelserne placeret først, og så bliver der tildelt adgang efterfølgende.

Log funktioner:

Ud over alle de nævnte funktioner i Astaro, findes der et utal at ”værktøjer”.
Da Astaro er baseret på en Linux-kerne, er der bl.a. mange muligheder for at få lavet logfiler over services og andre aktiviteter.
Dette gør overskueligheden, og muligheden for selv at vælge hvilke informationer man ønsker, meget stor.

På billedet ovenfor, ses et udsnit af de log-muligheder der findes i Astaro. Yderligere er der i nogle af dem mulighed for ”LIVE-Log”, hvor man kan følge med i Trafikken i Real-time!

Konklusion:

Fantastisk!!
Dette er kort og godt hvad jeg kan konkludere efter at have haft den store fornøjelse med at arbejde med netop Astaro Security Linux V4.

En nem, hurtig og overskuelig installation, hvor installation mildest talt klare det hele selv, både selve installationen, detektering og konfigurering af hardware. Hvorefter det faktisk ikke er nødvendigt at benytte maskinen lokalt mere.

En simpelt og overskuelig opbygget konfigurations manager, som er tilgængelig via enhver lokal Web-browser.
Dernæst syntes jeg det er et rigtig effektivt princip, hvor man definere alle parameter og værdier en gang, og så ellers kan kombinere og bruge disse overalt i opsætningen.

Dette overflødig gøre behovet for at skulle huske et utal at adresser, port nummer og subnet.
Alle disse værdier bliver lageret i profiler, med mulighed for at give dem et passende navn. Dette overskueliggør virkelig opsætningen meget, og evt. om konfigurering på et senere tidspunkt.

Ud over at Astaro Security Linux indeholder alt hvad man kunne ønske af en firewall, findes der et utal af små hjælpe værktøjer, hvilket medføre at man ikke behøver at hoppe til andet software for f.eks. at lave en trace-route, eller en ping.

Astaro Security Linux V4, er helt klart et stykke software jeg kan anbefale, da det køre meget stabilt på selv forholdsvis små maskiner, er Linux Baseret, og kræver ikke det mindste kendskab til Linux, for at udnytte dette softwaren.

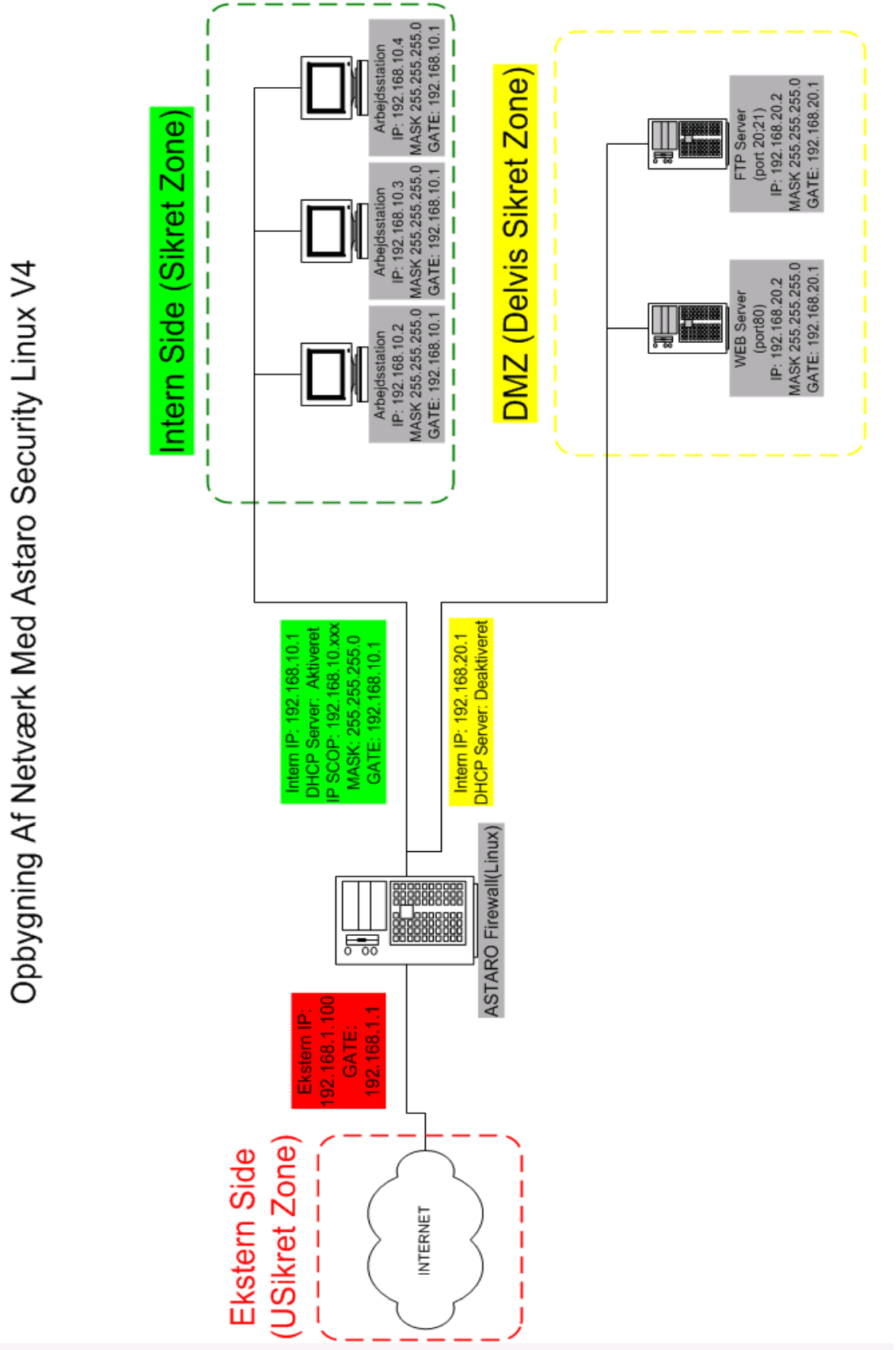
Kilder:

Bøger:
Datakommunikation

Web-Sites:
www.tdc.dk
www.astaro.com
www.google.dk
www.net-faq.dk

Hjælp-funktionen i Astaro Security Linux V4.

Bilag 1.


Opbygning Af Netværk Med Astaro Security Linux V4
Intern Side (Sikret Zone)
Arbejdsstation
IP: 192.168.10.2
MASK 255.255.255.0
GATE: 192.168.10.1
Arbejdsstation
IP: 192.168.10.3
MASK 255.255.255.0
GATE: 192.168.10.1
Arbejdsstation
IP: 192.168.10.4
MASK 255.255.255.0
GATE: 192.168.10.1
DMZ (Delvis Sikret Zone)
WEB Server
(port80)
IP: 192.168.20.2
MASK 255.255.255.0
GATE: 192.168.20.1
FTP Server
(port 20:21)
IP: 192.168.20.2
MASK 255.255.255.0
GATE: 192.168.20.1
Intern IP: 192.168.10.1
DHCP Server: Aktiveret
IP SCOP: 192.168.10.xxx
MASK: 255.255.255.0
GATE: 192.168.10.1
Intern IP: 192.168.20.1
DHCP Server: Deaktiveret
ASTARO Firewall(Linux)
Ekstern IP:
192.168.1.100
GATE:
192.168.1.1
Ekstern Side
(USikret Zone)
INTERNET