FreeBSD

IPFW Firewall FreeBSD

Version 0.0.2 - 28 juli 2022

Firewall FreeBSD

Firewalls gør det muligt at filtrere den indgående og udgående trafik, der strømmer gennem et system. En firewall kan bruge et eller flere sæt "regler" til at inspicere netværkspakker, når de kommer ind eller ud af netværksforbindelser og enten tillader trafikken igennem eller blokerer den.

Firewalls kan øge sikkerheden for en vært eller et netværk. De kan bruges til at gøre en eller flere af følgende ting:

- Beskytte og isolere programmer, tjenester og maskiner i et internt netværk mod uønsket trafik fra det offentlige internet.
- Begrænse eller deaktivere adgang fra værter på det interne netværk til tjenester på det offentlige internet.
- Understøtte network address translation (NAT), som tillader et internt netværk at bruge private IP-adresser og dele en enkelt forbindelse til det offentlige internet ved hjælp af enten en enkelt IP-adresse eller en delt pulje af automatisk tildelte offentlige adresser.

FreeBSD leverer flere firewalls for at imødekomme de forskellige krav og præferencer for en lang række brugere. Hver bruger bør vurdere, hvilken firewall der bedst opfylder deres behov.

I den her vejledning gennemgås opsætning af IPFW firewall til stationær eller bærbar computer.

Note:

Da alle firewalls er baseret på inspektion af værdierne af udvalgte pakkekontrolfelter, skal skaberen af firewallregelsættet have en forståelse af, hvordan TCP/IP fungerer, hvad de forskellige værdier i pakkekontrolfelterne er, og hvordan disse værdier bruges i en normal sessionssamtale. For en god introduktion henvises til Daryls TCP/IP Primer

---

Firewall koncepter

Et regelsæt indeholder en gruppe regler, som sender eller blokerer pakker baseret på værdierne i pakken. Den tovejsudveksling af pakker mellem værter omfatter en

sessionssamtale. Firewall regelsættet behandler både de pakker, der kommer fra det offentlige internet, såvel som de pakker, der produceres af systemet som et svar på dem. Hver TCP/IP-tjeneste er foruddefineret af dens protokol og lytteport. Pakker, der er bestemt til en specifik tjeneste, stammer fra kildeadressen ved hjælp af en uprivilegeret port og målretter mod den specifikke tjenesteport på destinationsadressen. Alle ovenstående parametre kan bruges som udvælgelseskriterier til at skabe regler, som vil videregive eller blokere tjenester.

For at finde ukendte portnumre, se **/etc/services**. Alternativt, kan du besøge http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers og foretage et portnummeropslag for at finde formålet med et bestemt portnummer.

Tjek dette link for portnumre, der bruges af Trojans.

FTP har to tilstande: aktiv tilstand og passiv tilstand. Forskellen ligger i, hvordan datakanalen erhverves. Passiv tilstand er mere sikker, da datakanalen hentes af den ordinære ftp sessionsanmoder. For en god forklaring af FTP og de forskellige tilstande, se http://www.slacksite.com/other/ftp.html.

Et firewall regelsæt kan enten være "exclusive" eller "inclusive". En exclusive firewall tillader al trafik igennem undtagen den trafik, der matcher regelsættet. En inclusive firewall gør det omvendte, da den kun tillader trafik, der matcher reglerne, og blokerer alt andet.

En inclusive firewall giver bedre kontrol over den udgående trafik, hvilket gør den til et bedre valg for systemer, der tilbyder tjenester til det offentlige internet. Det styrer også typen af trafik, der stammer fra det offentlige internet, og som kan få adgang til et privat netværk. Al trafik, der ikke matcher reglerne, blokeres og logges. Inclusive firewalls er generelt mere sikre end exclusive firewalls, fordi de reducerer risikoen for at tillade uønsket trafik markant.

Sikkerheden kan skærpes yderligere ved hjælp af en "stateful firewall". Denne type firewall holder styr på åbne forbindelser og tillader kun trafik, som enten matcher en eksisterende forbindelse eller åbner en ny, tilladt forbindelse.

Stateful filtrering behandler trafik som en tovejsudveksling af pakker, der omfatter en session. Når tilstand er angivet på en matchende regel, genererer firewallen dynamisk interne regler for hver forventede pakke, der udveksles under sessionen. Den har tilstrækkelige matchningsmuligheder til at afgøre, om en pakke er gyldig til en session. Alle pakker, der ikke passer ordentligt til sessionsskabelonen, afvises automatisk.

Når sessionen er fuldført, fjernes den fra den dynamiske tilstandstabel.

Stateful filtrering giver mulighed for at fokusere på at blokere/passere nye sessioner. Hvis den nye session er bestået, tillades alle dens efterfølgende pakker automatisk, og eventuelle

bedragerpakker afvises automatisk. Hvis en ny session er blokeret, er ingen af dens efterfølgende pakker tilladt. Stateful filtrering giver avancerede matchningsevner, der er i stand til at forsvare sig mod strømmen af forskellige angrebsmetoder, der anvendes af angribere.

NAT står for Network Address Translation. NAT-funktionen gør det muligt for det private LAN bag firewallen at dele en enkelt ISP tildelt IP-adresse, selvom denne adresse er dynamisk tildelt. NAT tillader hver computer i LAN at have internetadgang uden at skulle betale internetudbyderen for flere internetkonti eller IP-adresser.

NAT vil automatisk oversætte den private LAN IP-adresse for hvert system på LAN til den enkelte offentlige IP-adresse, efterhånden som pakker forlader firewallen, der er bundet til det offentlige internet. Den udfører også den omvendte oversættelse for returnerende pakker.

Ifølge RFC 1918 er følgende IP-adresseområder reserveret til private netværk, som aldrig vil blive dirigeret direkte til det offentlige internet, og derfor er tilgængelige til brug med NAT:

- 10.0.0.0/8.
- 172.16.0.0/12.
- 192.168.0.0/16.

Advarsel:

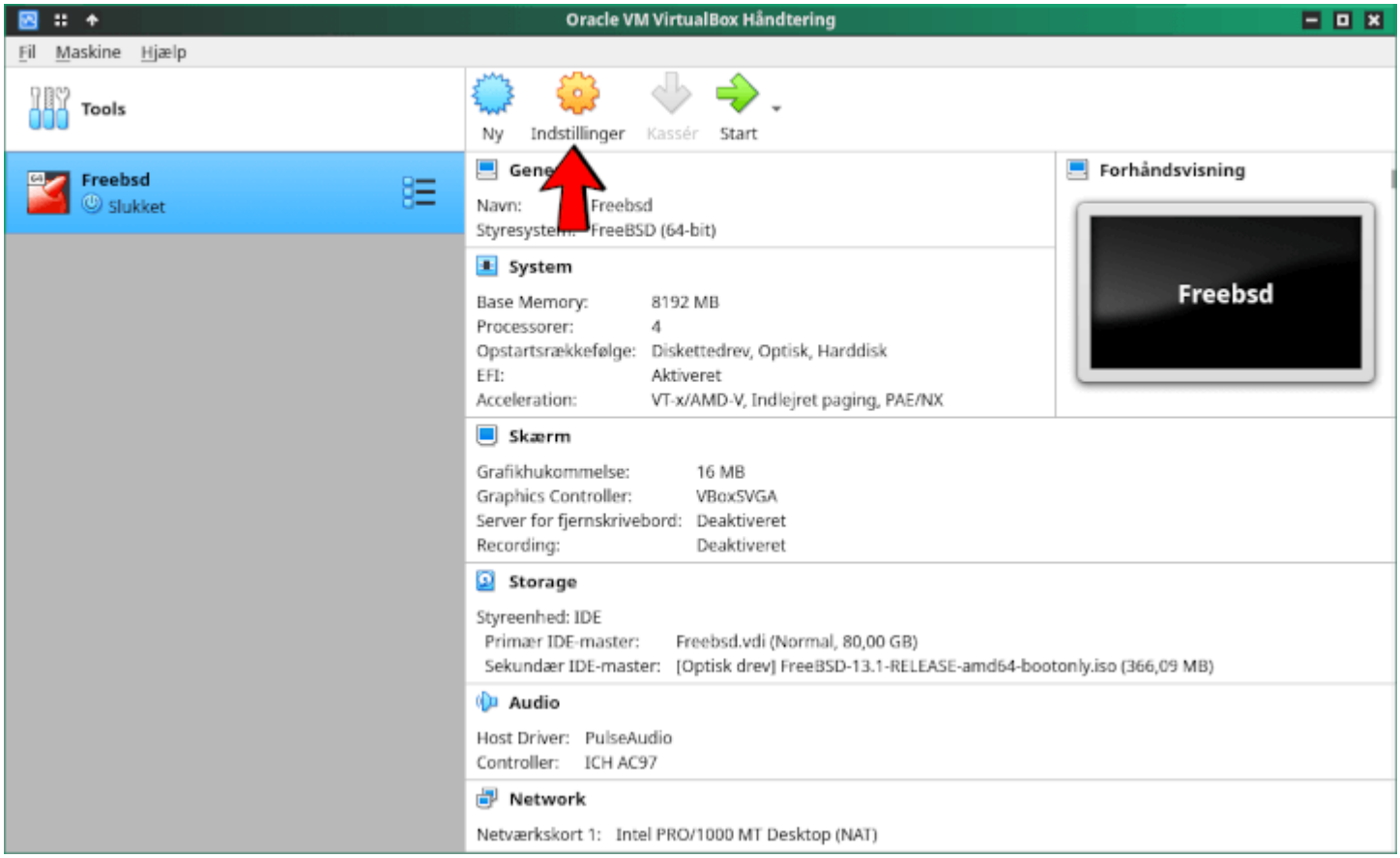
Når du arbejder med firewall reglerne, skal du være meget forsigtig. Nogle konfigurationer kan låse administratoren ude. For at være på den sikre side bør du overveje at udføre den indledende firewall konfiguration fra den lokale konsol i stedet for at gøre det eksternt via ssh.

Hvis du vil vide mere om firewall, så læs afsnittet om Blacklistd og Avanceret netværk.

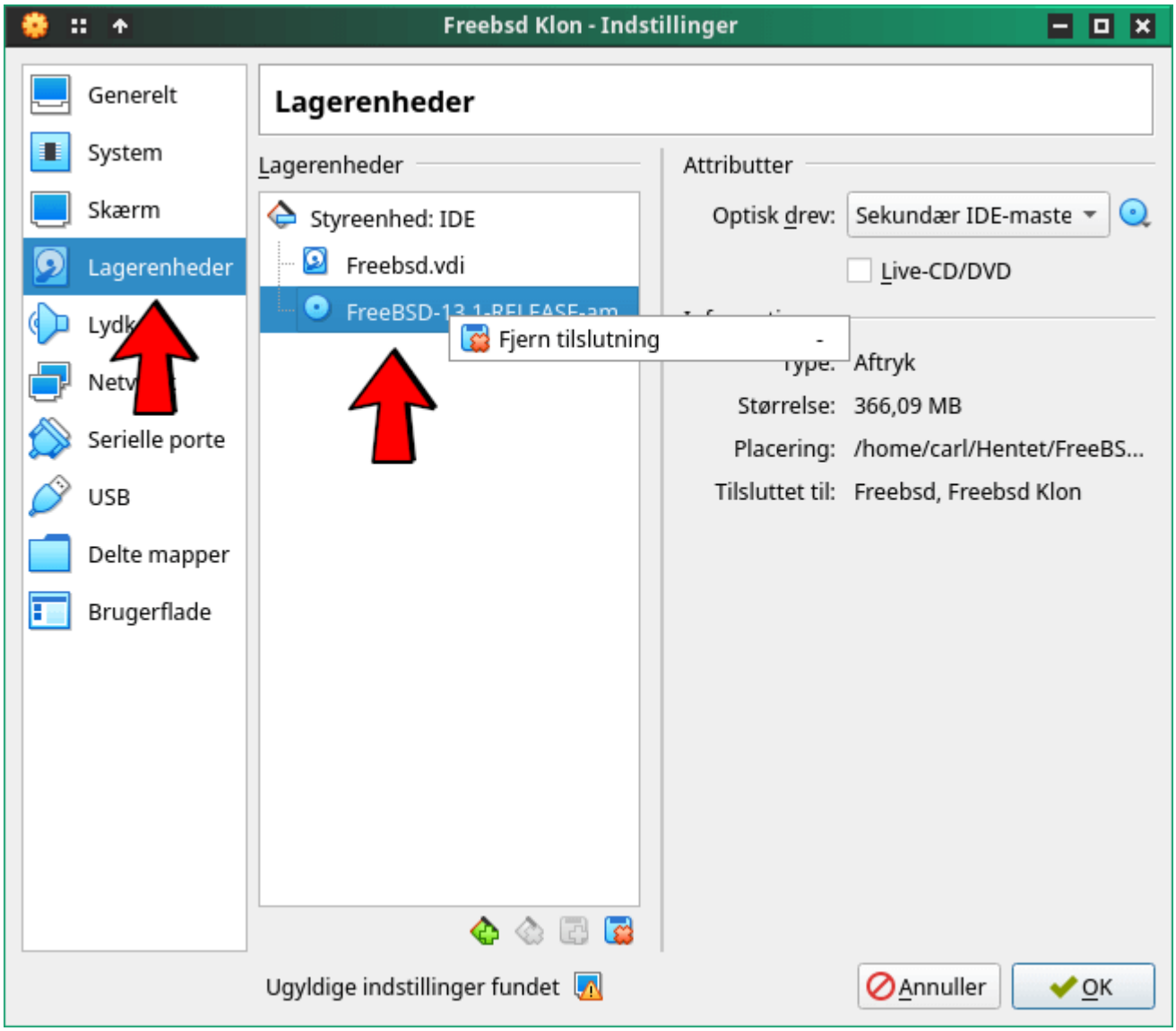
VirtualBox

Hvis der bruges VirtualBox til at installere FreeBSD er der noget der skal tilrettes. Hvis der ikke bruges VirtualBox kan dette afsnit springes over.

Åbn VirtualBox og klik på **Indstillinger**.



Du vil så komme frem til dette skærmbillede.



Klik på **Lagerenheder**, og højreklik på **FreeBSD** og vælg **Fjern tilslutning**.

VirtualBox kommer med virtuelle grafik/lyddrivere, som FreeBSD kan have problemer med at identificere. For at løse problemer der kan opstå, skal der installeres **virtualbox-ose-additions**. log ind som **almindelig bruger** og skift til root med **su**.

Men inden vi gør noget skal du først opdatere arkivet og kontrollere om der er opdateringer.

Opdater arkivet:

pkg update

```
carl@andersen:~ $ su
Password:
Jul 19 14:01:44 andersen su[7236]: carl to root on /dev/ttyv0
root@andersen:/home/carl # pkg update
The package management tool is not yet installed on your system.
Do you want to fetch and install it now? [y/N]: y
Bootstrapping pkg from pkg+http://pkg.FreeBSD.org/FreeBSD:13:amd64/quarterly, please
wait...
Verifying signature with trusted certificate pkg.freebsd.org.2013102301... done
Installing pkg-1.18.3...
Extracting pkg-1.18.3: 100%
Updating FreeBSD repository catalogue...
Fetching meta.conf: 100%    163 B   0.2kB/s    00:01
Fetching packagesite.pkg: 100%    6 MiB   6.6MB/s    00:01
Processing entries: 100%
FreeBSD repository update completed. 31616 packages processed.
All repositories are up to date.
```

Her får jeg så at vide:

The pacage mangement tool is not yet installed on your system. Do you want to fetch and install it now? Det vil jeg selvfølgelig, så jeg indtaster **y** og slår Enter.

Kontroller om der er opdateringer til systemmet:

freebsd-update fetch install

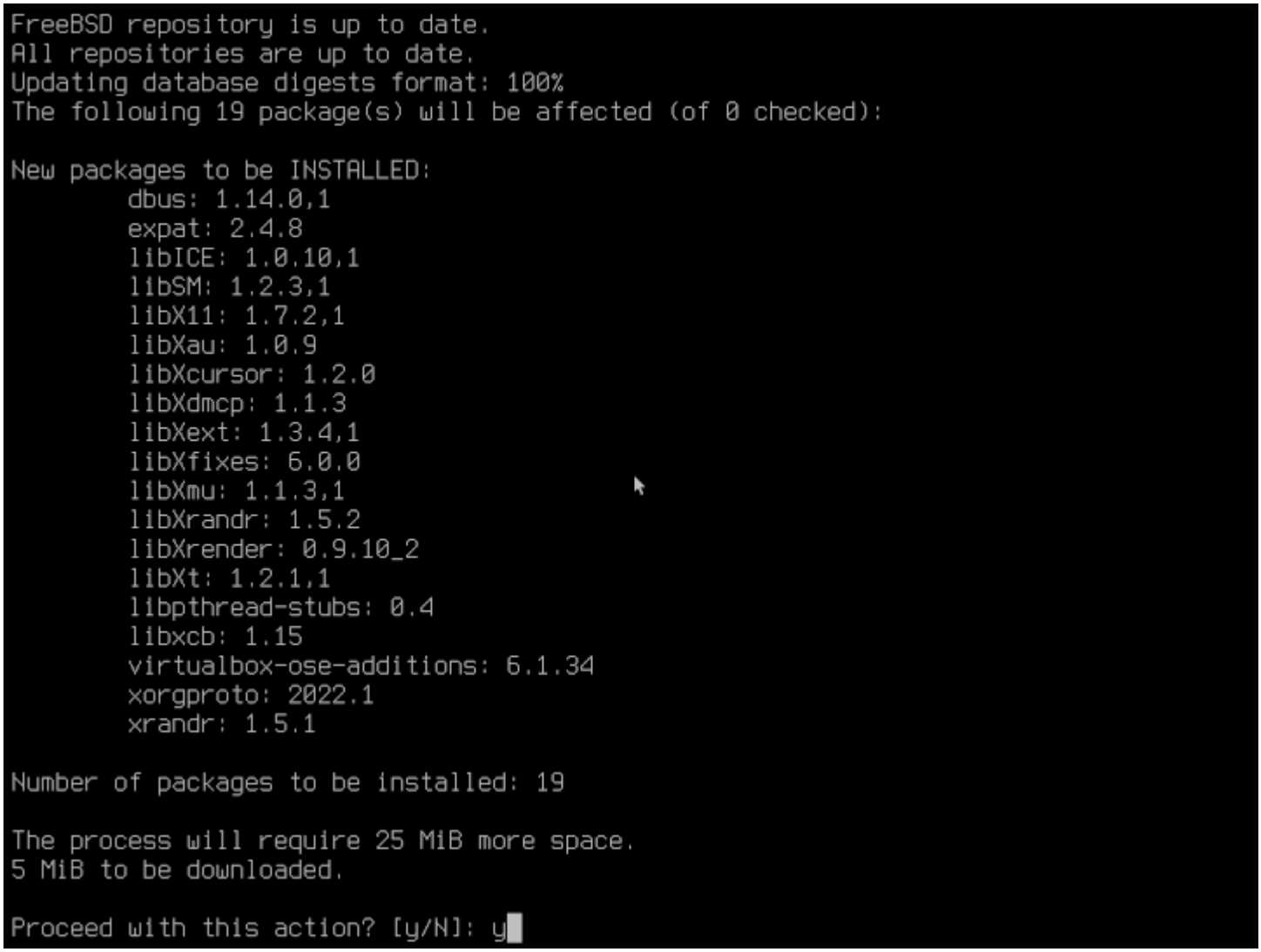
```
root@andersen:/home/carl # freebsd-update fetch install
src component not installed, skipped
Looking up update.FreeBSD.org mirrors... 2 mirrors found.
Fetching public key from update2.freebsd.org... done.
Fetching metadata signature for 13.1-RELEASE from update2.freebsd.org... done.
Fetching metadata index... done.
Fetching 1 metadata files... done.
Inspecting system... done.
Preparing to download files... done.

No updates needed to update system to 13.1-RELEASE-p0.
No updates are available to install.
```

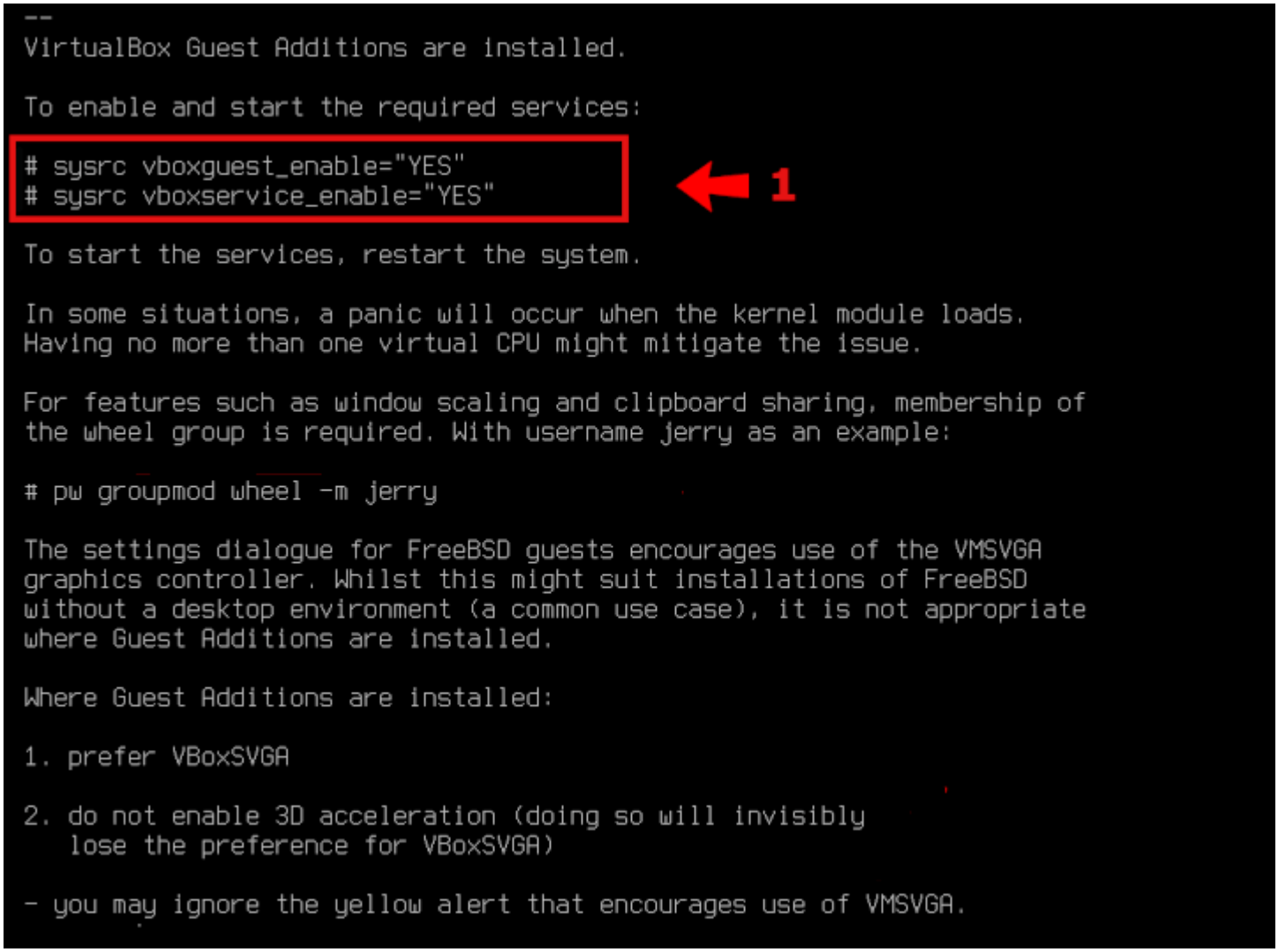
Der var så ingen opdateringer i det her tilfælde.

Installer VirtualBox gæstetilføjelsespakkerne:

pkg install emulators/virtualbox-ose-additions



Der er 19 programpakker der skal installeres. Indtast **y** og slå Enter.



- 1. Så skal der aktiveres og startes de nødvendige service til VirtualBox.

Indtast **sysrc vboxguest_enable="YES"** og slå Enter.

```
root@andersen:/home/carl # sysrc vboxguest_enable="YES"
vboxguest_enable:  -> YES
```

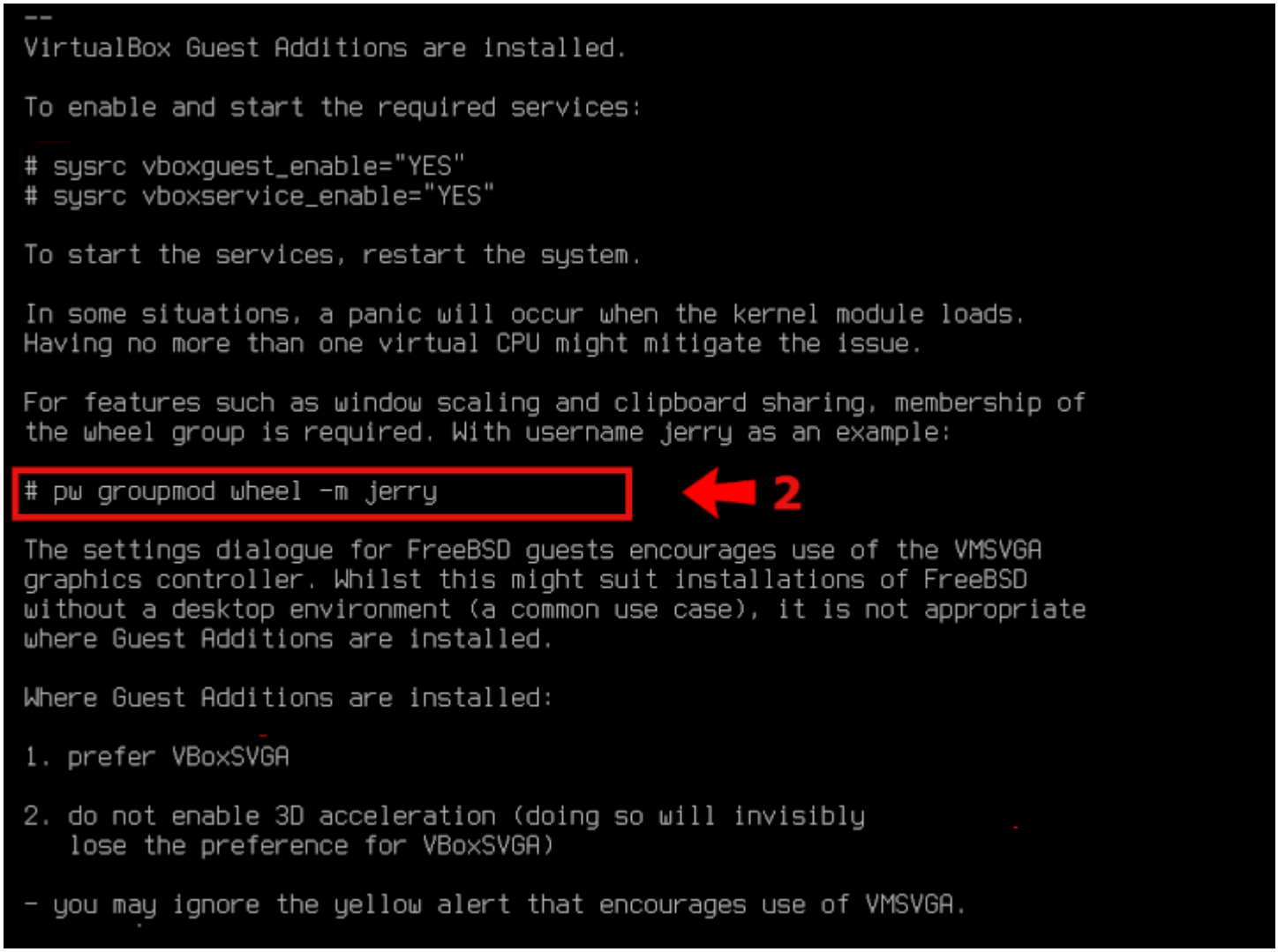
Indtast **sysrc vboxservice_enable="YES"** og slå Enter.

```
root@andersen:/home/carl # sysrc vboxservice_enable="YES"
vboxservice_enable:  -> YES
```

Nu skal computeren genstartes, så det kan træde i kraft. Indtast **reboot** og slå Enter.

```
carl@andersen:~ $ cat /etc/rc.conf
clear_tmp_enable="YES"
syslogd_flags="-ss"
sendmail_enable="NONE"
hostname="andersen"
keymap="dk.kbd"
ifconfig_em0="DHCP"
moused_enable="YES"
ntpdate_enable="YES"
powerd_enable="YES"
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable
dumpdev="AUTO"
zfs_enable="YES"
vboxguest_enable="YES"
vboxservice_enable="YES"
```

Log ind som almindelig bruger og indtast **cat /etc/rc.conf** Som det kan ses er **vboxguest** og **vboxservice** aktiveret ved opstart af computeren.



- 2. Et eksempel på at tilføje jerry til gruppen wheel **pw groupmod wheel -m jerry**. Men **carl** blev tilføjet til "whell grup" under installationen, så det springer vi over.

- 3. Hvor der er gæstetilføjelse installeret som her, foretrækker FreeBSD VboxSVAG. VboxSVAG kører vi også med i den her installation af FreeBSD.

  Aktiver heller ikke 3D accleration i VirtualBox. hvis du gør det, vil du miste henvisning til VirtualBox. Så gør det ikke.

IPFW firewall

Der er tre firewall muligheder på FreeBSD. Den internt byggede IPFW, den 'gamle' IPF (kendt som IP Filter) og PF som er porteret fra OpenBSD. Her gennemgår vi opsætning af IPFW firewall til stationær og bærbar computer (arbejdsstation). IPFW er en stateful firewall". Denne type firewall holder styr på åbne forbindelser og tillader kun trafik, som enten matcher en eksisterende forbindelse eller åbner en ny, tilladt forbindelse.

IPFW er skrevet til FreeBSD, som understøtter både IPv4 og IPv6. Den består af flere komponenter: kernel firewall filter rule processor og dens integrerede integrated packet accounting facility, logningsfaciliteten, NAT, dummynet(4) traffic shaper, en forward facility, en bridge facility, og en ipstealth facility.

Blandt de tre mulige firewalls på FreeBSD er IPFW den internt byggede som standard, og en nem måde at opsætte en firewall på. Men hvis man har brug for at bygge en boks til at fungere som en dedikeret netværksenhed med pakkefiltrering kapacitet, er finjustering af IPFW firewall konfigurationen nødvendig. Det kan du læse mere om i afsnit 31.4.2. IPFW Rule Syntax i FreeBSD håndbogen. Hvis du tilfældigvis har Michael W. Lucas' sidste udgave af ' Absolute FreeBSD, kan en genlæsning af kapitel 7 og 8 være nyttig. Jeg har selv anskaffet bogen. Albert Valbuena har også skrevet en god vejledning til hvordan IPFW firewallen på FreeBSD konfigureres.

FreeBSD leverer et eksempelregelsæt i **/etc/rc.firewall**, som definerer flere firewalltyper for almindelige scenarier for at hjælpe nybegyndere med at generere et passende regelsæt. IPFW giver en kraftfuld syntaks, som avancerede brugere kan bruge til at lave tilpassede regelsæt, der opfylder sikkerhedskravene i et givet miljø.

IPFW er som sagt inkluderet i den grundlæggende FreeBSD installation som et kerneindlæsbart modul, hvilket betyder, at en brugerdefineret kerne ikke er nødvendig for at aktivere IPFW.

Opsætning af IPFW firewall

```
carl@andersen:~ $ su
Password:
Jul 25 11:11:56 andersen su[19669]: carl to root on /dev/ttyv0
```

Log ind som almindelig bruger og skift til **root** med **su**.

Vejledning til opsætning af firewall finder du herunder når de forskellige kommandoer er udført.

```
root@andersen:/home/carl # sysrc firewall_enable="YES"
firewall_enable: NO -> YES
```

Så skal firewall aktiveres ved at du indtaster **sysrc firewall_enable="YES"** og slår Enter.

```
root@andersen:/home/carl # sysrc firewall_quiet="YES"
firewall_quiet: NO -> YES
```

Næste skridt er indtast **sysrc firewall_quiet="YES"** og slå Enter.

```
root@andersen:/home/carl # sysrc firewall_type="workstation"
firewall_type: UNKNOWN -> workstation
```

Næste skridt er indtast **sysrc firewall_type="workstation"** og slå Enter.

```
root@andersen:/home/carl # sysrc firewall_logdeny="YES"
firewall_logdeny: NO -> YES
```

Næste skridt er indtast **sysrc firewall_logdeny="YES"** og slå Enter

```
root@andersen:/home/carl # service ipfw start
ipfw2 (+ipv6) initialized, divert loadable, nat loadable, default to deny, logging di
sabled
Firewall rules loaded.
```

Næste skridt er at starte firewall. indtast **service ipfw start** og slå Enter.

Du får så at vide at **Firewall rules er loaded**.

```
root@andersen:/home/carl # service ipfw status
ipfw is enabled
```

Næste skridt er at se status på firewall. indtast **service ipfw status** og slå Enter.

Du får så at vide at **ipfw is enabled**. D.V.S. at firewall er aktiveret.

Hvis du vil se om firewall reglerne er loaded under opstart, så indtast **cat /etc/rc.conf | grep firewall** og slå Enter.

```
root@andersen:/home/carl # cat /etc/rc.conf | grep firewall
firewall_enable="YES"
firewall_quiet="YES"
firewall_type="workstation"
firewall_logdeny="YES"
```

Og som du kan se er firewall reglerne aktiveret i **/etc/rc.conf** ved opstart af computeren.

Hvis du vil se standard reglerne for IPFW firewall, så indtast **grep firewall /etc/defaults/rc.conf | less** og slå Enter.

```
### Basic network and firewall/security options: ###
firewall_enable="NO"            # Set to YES to enable firewall functionality
firewall_script="/etc/rc.firewall" # Which script to run to set up the firewall
firewall_type="UNKNOWN"         # Firewall type (see /etc/rc.firewall)
firewall_quiet="NO"             # Set to YES to suppress rule display
firewall_logging="NO"           # Set to YES to enable events logging
firewall_logif="NO"             # Set to YES to create logging-pseudo interface
firewall_flags=""               # Flags passed to ipfw when type is a file
firewall_coscripts=""           # List of executables/scripts to run after
                                # firewall starts/stops
firewall_client_net="192.0.2.0/24" # IPv4 Network address for "client"
                                # firewall.
#firewall_client_net_ipv6="2001:db8:2:1::/64" # IPv6 network prefix for
                                # "client" firewall.
firewall_simple_iif="em1"       # Inside network interface for "simple"
                                # firewall.
firewall_simple_inet="192.0.2.16/28" # Inside network address for "simple"
                                # firewall.
firewall_simple_oif="em0"       # Outside network interface for "simple"
                                # firewall.
firewall_simple_onet="192.0.2.0/28" # Outside network address for "simple"
                                # firewall.
#firewall_simple_iif_ipv6="em1" # Inside IPv6 network interface for "simple"
                                # firewall.
#firewall_simple_inet_ipv6="2001:db8:2:800::/56" # Inside IPv6 network prefix
                                # for "simple" firewall.
#firewall_simple_oif_ipv6="em0" # Outside IPv6 network interface for "simple"
                                # firewall.
#firewall_simple_onet_ipv6="2001:db8:2:0::/56" # Outside IPv6 network prefix
                                # for "simple" firewall.
firewall_myservices=""          # List of ports/protocols on which this host
:
```

Forklaring på opsatte firewall regler:

- **sysrc firewall_enable="YES":** Hver gang du kører **sysrc** for at ændre din konfiguration, vil du modtage output, der viser ændringerne.
- **sysrc firewall_quiet="YES":** Dette fortæller ipfw ikke at udsende noget til standard out, når det udfører bestemte handlinger. Dette kan virke som et spørgsmål om præference, men det påvirker faktisk ikke firewallens funktionalitet.

  To faktorer kombineret tilsammen, gør dette til en vigtig indstilling. Den første er, at firewallkonfigurationsscriptet udføres i det aktuelle shell miljø, ikke som en baggrundsopgave. Den anden er, at når **ipfw** kommandoen læser et konfigurationsscript uden "**quiet**" flag, læser og udsender den hver linje igen til standard out. Når den udsender en linje, **udfører den straks** den tilknyttede handling.

De fleste firewall konfigurationsfiler tømmer de nuværende regler øverst i scriptet for at starte på en frisk. Hvis ipfw firewallen støder på en linie som denne uden quiet flag, vil den straks fjerne alle regler og vende tilbage til sin standardpolitik, som normalt er at nægte alle forbindelser. Hvis du konfigurerer firewallen over SSH, ville dette afbryde forbindelsen, lukke den aktuelle shell session, og ingen af de følgende regler vil blive behandlet, hvilket effektivt låser dig ude. Quiet flag gør det muligt for firewallen at behandle reglerne som et sæt, i stedet for at implementere hver enkelt individuelt.

- **sysrc firewall_type="workstation":** Dette indstiller firewallen til at beskytte en enkelt computer, og kun en, hvorfra du konfigurerer firewallen ved hjælp af stateful regler. En stateful firewall overvåger tilstanden af netværksforbindelser over tid og gemmer information om disse forbindelser i hukommelsen i kort tid. Som et resultat kan der ikke kun defineres regler for, hvilke forbindelser firewallen skal tillade, men en stateful firewall kan også bruge de data, den har lært om tidligere forbindelser, til at evaluere, hvilke forbindelser der kan oprettes.

  Filen **/etc/rc.conf** giver dig også mulighed for at tilpasse de tjenester, du ønsker, at computeren skal have adgang til ved at bruge firewall_myservices og firewall_allowservices mulighederne.
- **sysrc firewall_logdeny="YES":** Firewall_logdeny indstillingen fortæller **ipfw** at logge alle forbindelsesforsøg, der nægtes adgang til filen **/var/log/security**.

Det var så opsætning af IPFW til stationær eller bærbar computer.

Det næste er at installere MATE Desktoppen efter opsætning af firewall.