

HowTo => OpenBSD => Basis Installatie

Hardware

=> Soekris 5501 (10W)



4/8 GB CF of grotere SSD



HowTo
OpenBSD
Basis Installatie

Tools => USB Card Reader voor de CF
USB naar Serial Adapter voor Console
InfraRecorder voor branden ISO image
Putty voor Terminal sessie middels USB Serial Adapter
7-Zip voor controleren van de sha256 hash
VirtualBox

Operating System => OpenBSD 4.8



HowTo OpenBSD Basis Installatie

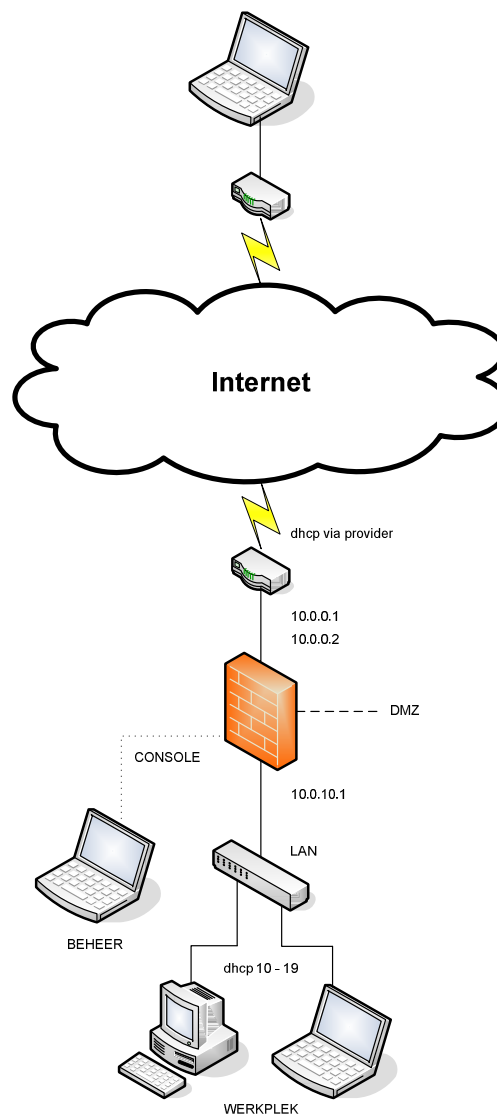
Inleiding:

Bekijk het schema en volg de stappen in dit document.
Het resultaat is een Soekris met OpenBSD.
Het is nog tamelijk kaal, bekijk andere HowTo's voor benodigde specifieke toevoegingen.



HowTo OpenBSD Basis Installatie

Schema:



HowTo OpenBSD Basis Installatie



Pre-install:

Installeer de met de USB Serial Adapter meegeleverde software op de BeheerPC.

De meest veilige optie is als deze niet is aangesloten op het LAN.

Installeer InfraRecorder op de BeheerPC (zie links).

Installeer Putty op de BeheerPC (zie links).

Installeer 7-Zip op de BeheerPC (zie links).

Installeer VirtualBox op de BeheerPC (zie links).

Aanpassen console speed in bios van de Soekris in 19200.

Haal eerst de ISO op

<http://ftp.nluug.nl/pub/OpenBSD/4.8/i386/install48.iso>

Controleer de sha256 hash van dit bestand met 7-Zip => bestand / checksum berekenen.

Vergelijk de berekende sha256 met wat is aangegeven in het additionele `SHA256` bestand, wijkt dit af dat is er mogelijk mee geknutseld, kijk dan bij een andere source.

Brand de ISO middels InfraRecorder op CD of DVD.

Sluit de USB Card Reader aan op de BeheerPC en stop de CF erin.

Het spreekt voor zich dat de SSD middels een kabeltje op de SATA interface aangesloten wordt.



HowTo OpenBSD Basis Installatie

Voor de Proxy met Cache moeten we bij de volgende stap wat schijfruimte herverdelen.

Pak van /home, /usr/local, /usr/obj en /usr/src en geef dit aan extra filesystems /var/squid/cache en een aparte log (**controleer**).

Mogelijk cache0 en cache1 indien we kleine en grote blokken apart kunnen afhandelen in squid.

Dit heb ook gevolgen voor fstab, dus aanpassen.

Houdt de ingevulde variabelenlijst van de **Bijlage Variabelen** in het inleidende document **HowTo OpenBSD Firewall met Secure Anonymous Access** bij de hand tijdens instalatie/configuratie.

Zodra je een variabele ziet, bv %HOST% vervang dit dan in zijn geheel door wat je had ingevuld, dus zeker geen %-tekens achterlaten.



HowTo OpenBSD Basis Installatie

In mijn geval [r10] <enter>
Nu het IPv4 nummer, none <enter>
IPv6 hoeft niet, done <enter> **is er ook none optie voor geen IP6 nummers?**
Je lokale domein, voor mij %**DOMEIN**% <enter>
Nameservers, none <enter>
Netwerk configuratie, no <enter>
root password voorlopig, geheim <enter>, of geef direct de juiste.
sshd starten, [default] <enter> **controleer wat wordt aangegeven!**
ntpd starten, nu niet, zie document **HowTo OpenBSD Tijd Synchronisatie**, [no] <enter>
X window activeren, niet noodzakelijk op server, no <enter>
Veranderen console, [no] <enter>
Aanmaak user, [no] <enter> **user beheer aanmaken, aangeven hoe!**
Nu goed opletten, bij fout is je systeem vernacheld, geef de device
voor CompactFlashCard, sd1 <enter>
Gebruik gehele disk, [w] <enter>
Er volgt een standaard schijfindeling met diverse filesystems,
accepteer dit, a <enter>
Ondanks mijn gedachte X niet te installeren omdat het overbodig is
doen we dit toch, dit is best practise omdat sommige additionele
programma's de libraries mogelijk nodig kunnen hebben.
De CF wordt nu ingedeeld met filesystems.
Andere schijven willen we niet, alleen de CF, done <enter>
Locatie installatiepackages, [cd] <enter>
Install media, [cd0] <enter>
Waar staan de packages, [4.8/i386] <enter>
Er volgt een lijst met packages, verwijder games.
-game* <enter>
[done] <enter>



HowTo

OpenBSD

Basis Installatie

Packages worden op CF gekopieerd.

Timezone, Europe/Amsterdam <enter>

Klaar, [done] <enter>

Er volgt nu een # prompt, sluit niet af en ga verder met de post acties.

Zolang nog niet aan internet gebruiken we root, daarna user beheer met sudo.

Beter inloggen als beheer en dan sudo overal gebruiken. Hiertoe aanpassen install en alle andere documenten.
Controleer of je zelf de user aan sudo moet toevoegen voor rechten of dat dit gebeurt in eerdere deel tijdens toevoegen user!



HowTo OpenBSD Basis Installatie

Post-Installatie OpenBSD:

Aangezien we straks gebruik maken van andere hardware dan tijdens installatie dienen we nu eerst handmatig een aantal wijzigingen door te voeren, doe je dit niet dan zie je de bootinfo niet.

De benodigde filesystems zijn nog gemount op `/mnt` voor de installatie.

Om verder te kunnen werken veranderen we de root (`/`).

```
root @ 10.0.10.1 - PuTTY [ksh]
# /mnt/usr/sbin/chroot /mnt
```



HowTo
OpenBSD
Basis Installatie

Middels `vi` passen we de configuratie aan, deze bevindt zich in diverse tekstbestanden:

Aangezien we de installatie middels de USB adapter van een Windows PC met VirtualBox op de CF hebben gezet dienen we de boot device aan te passen, `sd1` vervangen door `wd0`
Zet Soft Updates aan voor `ffs` type filesystem, (`softdep`).

```
root @ 10.0.10.1 - PuTTY [vi /etc/fstab]
/dev/wd0a / ffs rw,softdep 1 1
/dev/wd0h /home ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0d /tmp ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0f /usr ffs rw,nodev,softdep 1 2
/dev/wd0g /usr/X11R6 ffs rw,nodev,softdep 1 2
/dev/wd0h /usr/local ffs rw,nodev,softdep 1 2
/dev/wd0j /usr/obj ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0i /usr/src ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0e /var ffs rw,nodev,nosuid,softdep 1 2
```

Pas de console speed aan.

Toevoegen als je de boot messages wilt zien via console.

```
root @ 10.0.10.1 - PuTTY [vi /etc/boot.conf]
stty com0 19200
set tty com0
```



Zet de console aan met de juiste snelheid, doe je dit niet dan stopt de informatie op het scherm aan einde boot proces.

```
root @ 10.0.10.1 - PuTTY [vi /etc/ttys]
console "/usr/libexec/getty std.19200" vt220 on secure
```

Aanpassen hostname indien anders dan aangegeven tijdens installatie.

```
root @ 10.0.10.1 - PuTTY [vi /etc/myname]
%HOST%. %DOMEIN%
```

Instellen van je lokale domein.
Je eerste reflex zou zijn .nl, echter deze staat geregistreerd bij je provider.
Pas hiermee op omdat anders je eigen externe sites niet bereikbaar zijn.

```
root @ 10.0.10.1 - PuTTY [vi /etc/domainname]
%DOMEIN%
```



HowTo OpenBSD Basis Installatie

Maak een apart bestand voor elke gebruikte interface.

```
vr0 (WAN) => inet 10.0.0.2 255.255.255.0 NONE
vr1 (LAN) => inet 10.0.10.1 255.255.255.0 NONE
vr2 (vrij)
vr3 (vrij)
```

De vrije interfaces kunnen later worden toegevoegd voor bv DMZ.

```
root @ 10.0.10.1 - PuTTY [vi /etc/hostname.vr0]
```

```
inet 10.0.0.2 255.255.255.0 NONE
```

```
root @ 10.0.10.1 - PuTTY [vi /etc/hostname.vr1]
```

```
inet 10.0.10.1 255.255.255.0 NONE
```

Instellen Default Gateway.

```
root @ 10.0.10.1 - PuTTY [vi /etc/mygate]
```

```
10.0.0.1
```



Als je wilt kun je de login boodschap aanpassen, gebruik hoofdletters voor **%EIGENAAR%**.

```
root @ 10.0.10.1 - PuTTY [vi /etc/motd]
```

```
Dit system is eigendom van %EIGENAAR%.
```

```
Toegang is alleen toegestaan voor wie hiertoe expliciet toestemming heeft verkregen.  
Ieder ander die zich ongeautoriseerd toegang verschaft zal worden vervolgd.  
Indien u meent bij toeval op dit systeem gekomen te zijn verbreek dan nu de verbinding.
```

Hierin komen lokale toevoegingen voor tijdens opstarten. bv Static Routes.

```
root @ 10.0.10.1 - PuTTY [vi /etc/rc.local]
```

```
route add 10.0.10.0/24 10.0.10.1
```



HowTo OpenBSD Basis Installatie

tbv hardening kunnen onnodige services hier worden uitgezet.

Zet bv een # voor de verouderde time en daytime (wij gaan timed toepassen).

Indien je toch van een service gebruik maakt pas dan een tcp wrapper toe, dit geeft syslog entries en gebruik host.allow en host.deny.

Controleer tijdens installatie!

```
root @ 10.0.10.1 - PuTTY [vi /etc/inetd.conf]
#daytime      stream  tcp    nowait  root    internal
#daytime      stream  tcp6   nowait  root    internal
#time         stream  tcp    nowait  root    internal
#time         stream  tcp6   nowait  root    internal
#daytime      dgram  udp    wait    root    internal
#daytime      dgram  udp6   wait    root    internal
#time         dgram  udp    wait    root    internal
#time         dgram  udp6   wait    root    internal
```

Deze informatie wordt doorgegeven als je middels dhcp een nummer aanvraagt.

```
root @ 10.0.10.1 - PuTTY [vi /etc/dhclient.conf]
initial-interval 1;
send host-name "%HOST%";
request subnet-mask, broadcast-address, time-offset, router, domain-
name, domain-name-servers, host-name;
```



HowTo OpenBSD Basis Installatie

Toevoegen te gebruiken dhcp range.
Vul hier je eigen domein in.

```
root @ 10.0.10.1 - PuTTY [vi /etc/dhcpd.conf]
```

```
option domain-name "%DOMEIN%";  
option domain-name-servers 10.0.10.1;  
  
subnet 10.0.10.1 netmask 255.255.255.0 {  
    option routers 10.0.10.1;  
    range 10.0.10.10 10.0.10.199;  
}
```

Instellen startparameters en zorgt voor opstarten bij boot.

```
root @ 10.0.10.1 - PuTTY [vi /etc/rc.conf.local]
```

```
dhcpd_flags=""          # Start dhcpd
```

Default zoekdomein en nameservers van je provider.
Eerst lokaal in /etc/hosts kijken en dan pas extern middels DNS.

```
root @ 10.0.10.1 - PuTTY [vi /etc/resolv.conf]
```

```
search %DOMEIN%  
nameserver %NS1%  
nameserver %NS2%  
lookup file bind
```



Voor aan/uit zetten diverse subsystemen.

Instellen routing voor IP4.

Geen IP6 verkeer. Is dit al standaard na installatie?
Kijk of toekenning IP6 adres op interface nog uitgezet
kan worden.

```
root @ 10.0.10.1 - PuTTY [vi /etc/sysctl.conf]
```

```
net.inet.ip.forwarding=1  
#net.inet6.ip6.forwarding=1
```

De ssh server alleen toestaan voor interne connecties,
anders extern risico op kraak!

```
root @ 10.0.10.1 - PuTTY [vi /etc/ssh/sshd.conf]
```

```
listenAddress 10.0.10.1
```

tbv installatie additionele programmatuur en updates
dient de bron te worden toegevoegd in de root profile.
Tevens is hergebruik shell history handig door toevoegen.

```
root @ 10.0.10.1 - PuTTY [vi ~/.profile]
```

```
export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/4.8/packages/i386/  
set -o vi
```



HowTo OpenBSD Basis Installatie

We doen hetzelfde voor de user beheer omdat deze middels sudo ook kan installeren en beheertaken uitvoeren.

```
root @ 10.0.10.1 - PuTTY [vi /home/beheer/.profile]
export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/4.8/packages/i386/
set -o vi
```

Aanmaken directory voor packages die je eerst download alvorens te installeren.

```
root @ 10.0.10.1 - PuTTY [ksh]
# mkdir -p /home/install
```



HowTo OpenBSD Basis Installatie

Toevoegen wget voor downloaden bestanden.
Eerst profile opnieuw inlezen voor activeren PKG_PATH.

```
root @ 10.0.10.1 - PuTTY [ksh]
# . ~/.profile
# pkg_add wget
```

Na de installatie systeem afsluiten.

```
root @ 10.0.10.1 - PuTTY [ksh]
# shutdown -h now
```

Hierna nemen we de CF uit de reader en stoppen deze in de connector op het moederbord van de Soekris.
De Soekris is middels de USB serial adapter verbonden met een BeheerPC, in dit geval ook met Windows, heb je een andere functionele oplossing, prima.
Reboot nu en log in als root met eerder ingevoerde password.
Indien je tijdelijk geheimhad ingevuld pas het dan nu aan, in iets niet makkelijk te raden.

```
root @ 10.0.10.1 - PuTTY [ksh]
# passwd root jouw_password
```



HowTo OpenBSD Basis Installatie

De router/firewall die je van de provider kreeg blijft aangesloten voor de verbinding.
Wat je wel moet aanpassen is de LAN interface, ipv dhcp geef je het een vast nummer, 10.0.0.1
De dhcp server van dit kastje dient ook te worden uitgeschakeld, doe je dit niet dan kan deze interfereren met de dhcp server die we zelf hebben geïnstalleerd.
Laatste waarschuwing voor aanpassing password indien je dat nog niet heb gedaan.
Plaats de Soekris nu zoals aangegeven in het schema.
Poorten van rechts naar links; WAN/LAN/[VPN]/[DMZ]
De laatste twee zijn nog optioneel, VPN of DMZ zou een logische keuze zijn.



HowTo OpenBSD Basis Installatie

Controle werking:

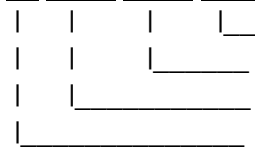
Aangezien de firewall nog niet is geconfigureerd kijken we eerst of we op het LAN een dhcp adres krijgen toegewezen voor een werkplek.
Dit impliceert dat we nu eerst verder gaan met de **HowTo Packet Filter Firewall**.



HowTo
OpenBSD
Basis Installatie

IP codering:

10.XXX.YYY.ZZZ



identifier (0 en 255 niet gebruikt)

functie

locatie (0 = hoofdkantoor)

testserie voor intern gebruik

XXX = YYY = ZZZ 0 t/m 255

Dit is een voorbeeld nummerplan waar je gerust van af mag wijken:

Systeem (bv router/carp) 1 t/m 9

Variabel (dhcp) 10 t/m 199

Fixed (bv server) 200 t/m 254

Links:

<http://www.openbsd.org/>

<http://infrarecorder.org/>

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

<http://www.7-zip.org/>

<http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>

Boeken:

Secure Architectures with OpenBSD



HowTo

**OpenBSD
Basis Installatie**