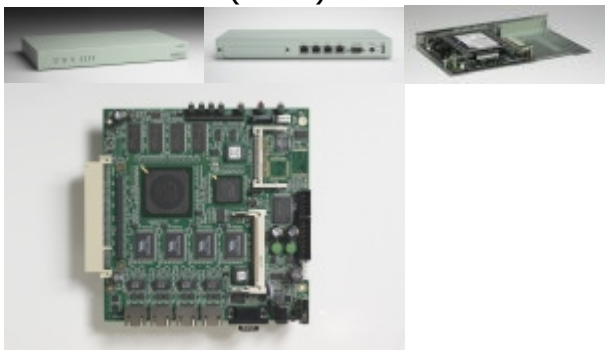
Hardware => Soekris 5501 (10W)



4/8 GB CF of grotere SSD

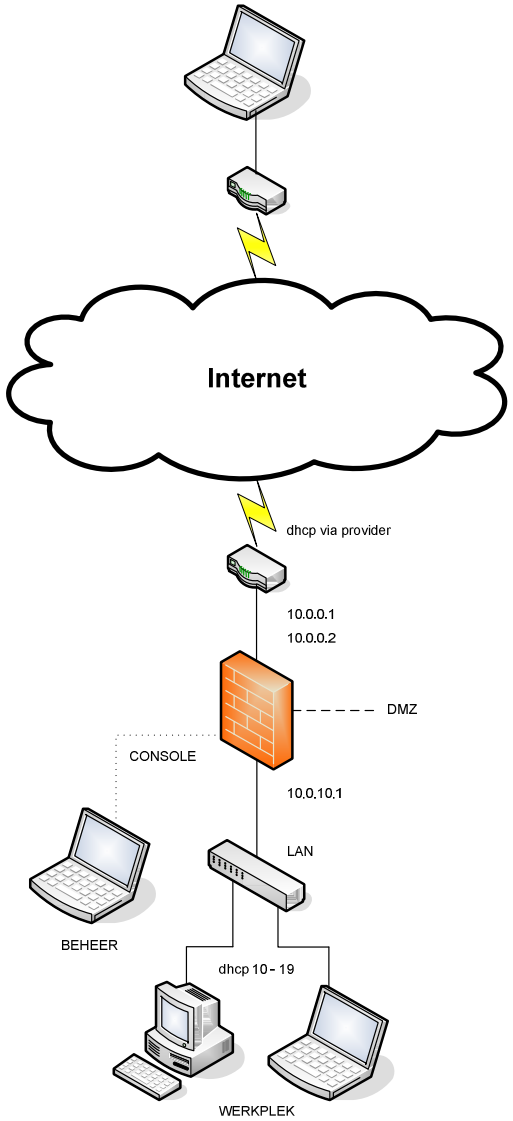
Tools	=>	USB Card Reader voor de CF USB naar Serial Adapter voor Console Een ouwe windows machine voor installatie op CF InfraRecorder voor branden ISO image Putty voor Terminal sessie middels USB Serial Adapter 7-Zip voor controleren van de sha256 hash
Operating System	=>	OpenBSD 4.8 (4.9 beschikbaar, testen)
Software	=>	PF OpenNTPD BIND of Unbound OpenVPN *bovenstaande past op 4 GB* Squid + SquidGuard TOR
HowTo's	=>	OpenBSD Basis Installatie OpenBSD Basis Packet Filter OpenBSD Tijd Synchronisatie OpenBSD Local Caching DNS + DNSSEC OpenBSD Secure Remote Access OpenBSD Proxy + Anti-Malware OpenBSD Anonymous External Access

Inleiding:

De basis is het OS, OpenBSD, met minimaal PF.
De keuze hiervoor is vanwege de designfilosofie, secure by default.
Het basissysteem is langdurig getest en bijgeschaafd in de loop der jaren.
Voor gebruik als firewall is een grafische interface niet noodzakelijk, dus geen X.
Additionele onderdelen kunnen later worden toegevoegd.
Elke toevoeging kan de integriteit aantasten, let dus altijd op wat je doet.
Om deze reden worden sommige programma's niet ondersteund, of alleen in een verouderde versie welke in de ogen van de core ontwikkelaars veilig is.
Veel programma's draaien met verminderde (non root) rechten, waar mogelijk zelfs chroot.
Ze zijn ook erg gespitst op werkelijk vrije software, dus mogelijk wel aanwezig in een externe library of bij de leverancier maar niet officieel.
Het blijft een keuze tussen paranoia en functionaliteit.

We proberen met ons samen te stellen systeem zoveel mogelijk de boze buitenwereld buiten te houden en bij naar buiten treden zo onzichtbaar mogelijk te blijven.
De keuze voor de Soekris is omdat deze slechts 10W verbruikt, dat er geen ventilator in zit scheelt ook.

Schema:


Internet
dhcp via provider
10.0.0.1
10.0.0.2
DMZ
CONSOLE
10.0.10.1
LAN
BEHEER
dhcp 10 - 19
WERKPLEK

Installatie:

Volg de bovenvermelde HowTo's , te starten met **OpenBSD Basis Installatie**.

Om je eigen systeem samen te stellen zijn er een aantal variabelen, deze worden in de diverse HowTo gebruikt, zie **Bijlage Variabelen**.

Beschrijving Onderdelen:

Voor een beter begrip zullen we alle onderdelen in wat meer detail beschrijven.
Als je de achtergrond begrijpt begrijp je het systeem en de samenhang ook beter.

BSD staat voor de Berkeley Software Distribution.
Het Walks and Talks als UNIX, alleen er zijn verschillen en vooral vanwege patentengedoe mag je het zo niet noemen.

OpenBSD is een afsplitsing van NetBSD, hetgeen weer is gebaseerd op 4.4BSD zoals ontwikkeld op de universiteit van Berkeley.
De nadruk van OpenBSD ligt op security en de vrije beschikbaarheid van de code.
De BSD licentie is vrijer dan de GPL van GNU(Linux).

OpenSSH is door dit project ontwikkeld, door de BSD licentie kan en wordt het vrijelijk in allerlei systemen toegepast.
Vage blobs voor bv netwerk/video drivers die onder Linux of FreeBSD wel worden geaccepteerd zul je bij OpenBSD niet tegenkomen.
Dit is zowel een voor als een nadeel, in ieder geval beperkt het de algemene toepassing ten voordele van een grotere systeemveiligheid.

De installatie is gewoon tekst gebaseerd.
Er wordt zeker enige achtergrondkennis verwacht, het is geen klik klak als Windows of een moderne Linux.
Toch valt het reuze mee, zeker als je de diverse HowTo volgt, de door mijzelf gemaakte beginnersfouten zijn hierin al gladgestreken.
Met mijn eigen AIX achtergrond voelde ik me al meteen thuis met ksh en de command history middels esc-k en vi, natuurlijk zijn er verschillen.
Een groot voordeel is de gestructureerde opbouw, alle configuratie gaat middels bestanden.
Even wennen is gebruik van netwerkdrivers, ipv de logische ETH0 is het hier bv hostname.vr0, waarbij de vr0 per leverancier anders kan zijn.
ipv root:root of root:system is er root:wheel, valt best mee.
Bij het installeren van vooral officiële Packages zul je merken dat de meesten na opstarten onder lagere rechten dan root draaien of zelfs als chroot.
Installeren van voorgeïnstalleerde Packages gaat middels pkg_get.
Natuurlijk is alles als source verkrijgbaar en kun je deze zelf compileren, eigen keuze.
De ontwikkeling gaat in een cyclus per 6 maanden.

Alle software is gratis, toch wordt aanschaf CD's, t-shirt of donatie gewaardeerd.
Geen enkele ontwikkeling is natuurlijk echt gratis.

PF

Packet Filter, de Firewall van OpenBSD.
De ontwikkeling hiervan is een direct gevolg van de strikte toepassing van vrije software.
De toenmalige IPFilter veranderde van licentie en kon dus niet meer gebruikt worden.
Direct na verwijdering uit de release tree is er een nieuw project opgestart met PF ten gevolge.
Het is ook nog steeds aan het verbeteren, dat kan soms een andere syntax betekenen.

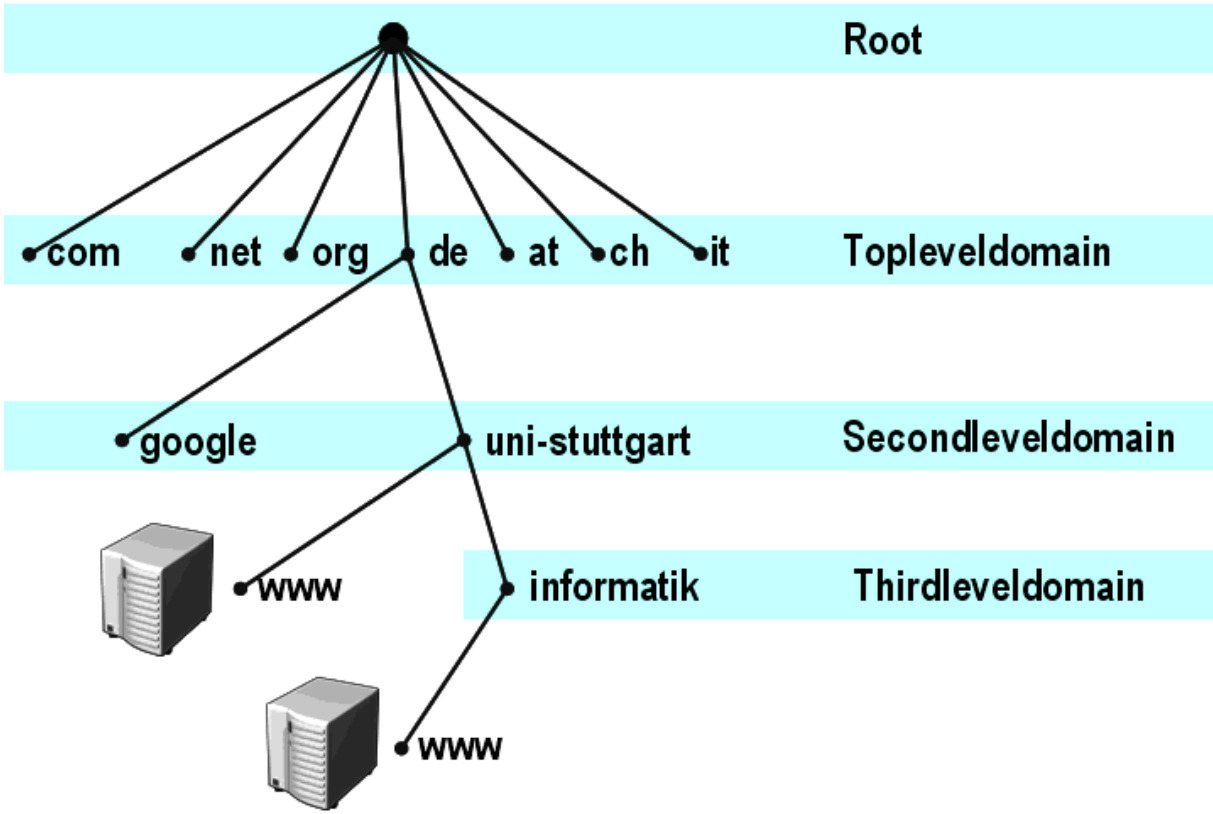
PF is een zeer geavanceerde Statefull Firewall met Antispoof, Trafic Shaping, Failover, Load Balancing, spamd, [. . .].
Momenteel heb ik een redelijk goed werkende configuratie waarbij ik vele verbeteringen heb doorgevoerd.
Het is wel met vallen en opstaan gegaan omdat soms gevonden voorbeelden niet blijken te werken, mede door in tussentijd gewijzigde syntax.
De laatste grote wijziging betrof een flinke vereenvoudiging en vermindering aantal rules door gebruik te maken van match voor natten naar externe interface.
Het is bijna een sport geworden, daarbij zijn er nog vele mogelijkheden die nog niet eens zijn toegepast.
Het is ook zeer goed mogelijk om met andere programmatuur samen te werken middels tables.
Zo kun je bv via snort/snortsam een IP blokkeren van een intruder.

Het principe is dat je initieel alles blokkeert en dan selectief opent.
Filteren kan obv tcp/udp/icmp.
Deze filters worden gevormd door Rules die het in en uitgaan van een interface beïnvloeden.
Je kunt in de rules zelf aangeven of je wilt loggen.
Uitlezen van deze log gaat real-time middels tcpdump.
Dit laatste is belangrijk om te zien of je nieuwe rule werkt als verwacht.
Je kunt ook alle verkeer rechtstreeks op de interface bekijken.
De kunst is om het eerst te laten werken en daarna de rule steeds strakker te trekken, bv van alle naar slechts een specifieke interface.

OpenNTPD

NTP maakt gebruik van servers die de tijd doorgeven van een atoomklok, deze zijn dus zeer nauwkeurig.
OpenNTPD kan zelf ook dienen als server om de tijd intern door te geven.
De reden voor een eigen ontwikkeling was dat de bestaande NTP daemons moeilijk te configureren waren, daarbij was ook de licentie niet voldoende open.
Tijdens boot kan de klok al ongeveer gelijkgesteld worden aan de externe klok, door in kleine stapjes sneller of langzamer te lopen zijn de interne en externe klok na verloop van tijd gelijk.
Voor de veiligheid wordt gestart met root waarna het teruggaat naar een gewone user _ntp.
Tevens draait het als chroot.

BIND

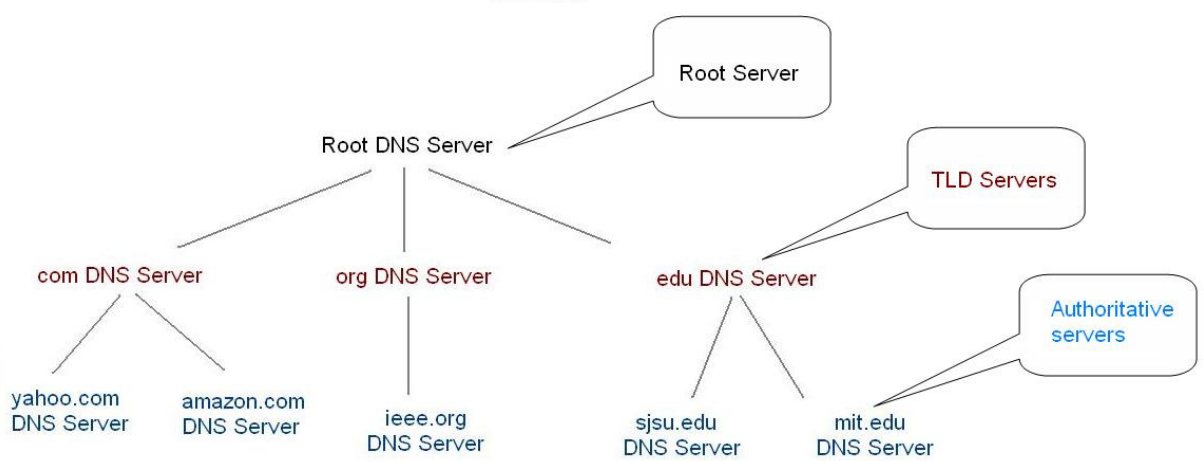

Root
com
net
org
de
at
ch
it
Topleveldomain
google
uni-stuttgart
Secondleveldomain
www
informatik
Thirdleveldomain
www

BIND is de meest bekende en tevens meest toegepaste DNS (Domain Name System).
Een DNS is een hiërarchische boomstructuur waarin Fully Qualified Domain Names en bijbehorende IP nummers zijn opgeslagen.
Er zijn verwijzingen naar diverse soorten servers mogelijk, bv webservers of ftp.
Tevens zijn er zogenaamde MX records die naar de mailserver verwijzen.
Alle namen dienen eerst middels DNS request te worden omgezet in een IP nummer om te kunnen communiceren.
Het kan dus een aantal stappen kosten voordat je het nummer terugkrijgt, tenzij een eerdere aanvraag in cache is opgeslagen.

Het Root domein bestaat uit een aantal zwaar beveiligde servers waarin de Top Level Domains zijn geregistreerd, hier start dus de aanvraag.
Elk land beheert zijn eigen TLD, waarin opgeslagen alle domeinen binnen dat land.
Het volgende niveau wordt beheerd door de eigenaar van het domein in zijn eigen DNS, andere mogelijkheid is dat een registrar dat voor je regelt.

Een laatste nieuwe optie die momenteel wordt ingevoerd is DNSSEC, een systeem obv cryptografische sleutels die aangeeft dat een antwoord correct is.
Het is een beveiliging tegen Cache Poisoning, het als het ware stiekem implanteren van foute doorverwijzingen.

Unbound



Unbound is van de grond af aan opnieuw ontwikkeld door oa NLnetLabs.
Reden is dat BIND een beetje opgeblazen is van de vele wijzigingen.
Een nieuwe frisse start zorgt tevens voor een betere security.
Unbound kan gebruikt worden voor je lokale LAN, verder is het gemaakt als resolver.
Het wordt gebruikt samen met NSD indien tevens eigen domeinen host.
In vergelijking met andere DNS systemen is deze combinatie extreem snel.
De ondersteuning van DNSSEC is zeer eenvoudig, ophalen en gebruik van nieuwe keys gaat automatisch.

Aangezien DNS een standaard is verwijs ik voor de algemene werking naar het verhaal van BIND.

OpenVPN

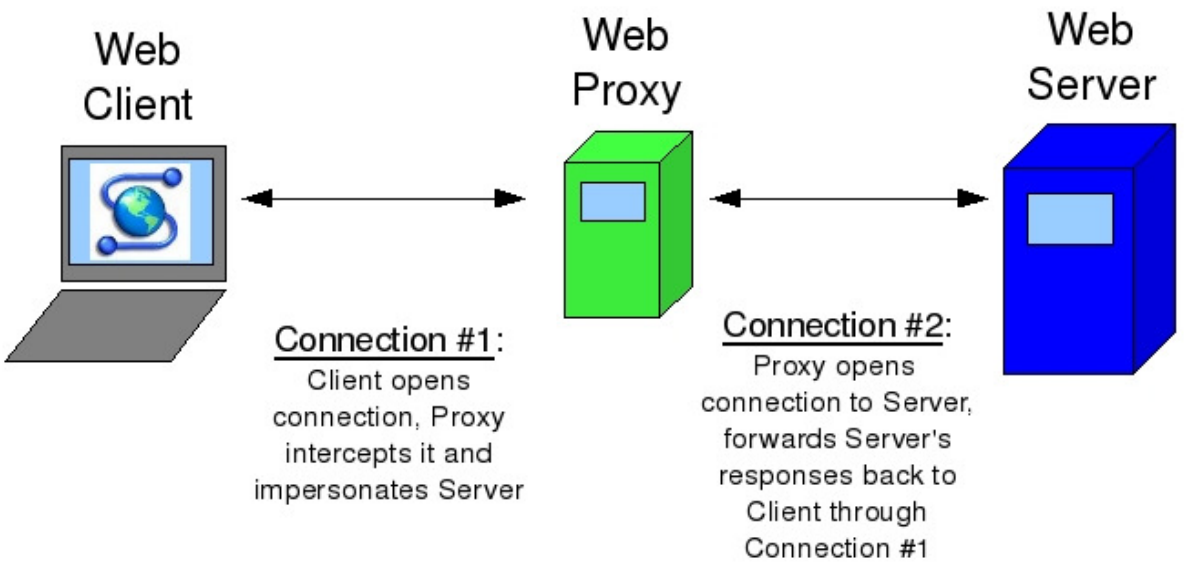
OpenVPN bestaat uit een server waar meerdere clients gelijktijdig mee kunnen connecten.
De verbindingen zijn cryptografisch beveiligd middels SSL/TLS.
Hoe meer bits gebruikt hoe meer moeite het kost de verbinding te kraken.
Helaas kost meer bits veel rekenkracht en werkt dus vertragend, daarbij is de overhead van te versturen pakketjes ook groter.

Er worden twee methodes ondersteund; Bridged en Routed.
Bij bridged krijg je een verbinding rechtstreeks in het remote netwerk, dit is handig voor Netbios van Windows.
Routed werkt prima in een unix/linux omgeving, zonder de overhead van Broadcasts.

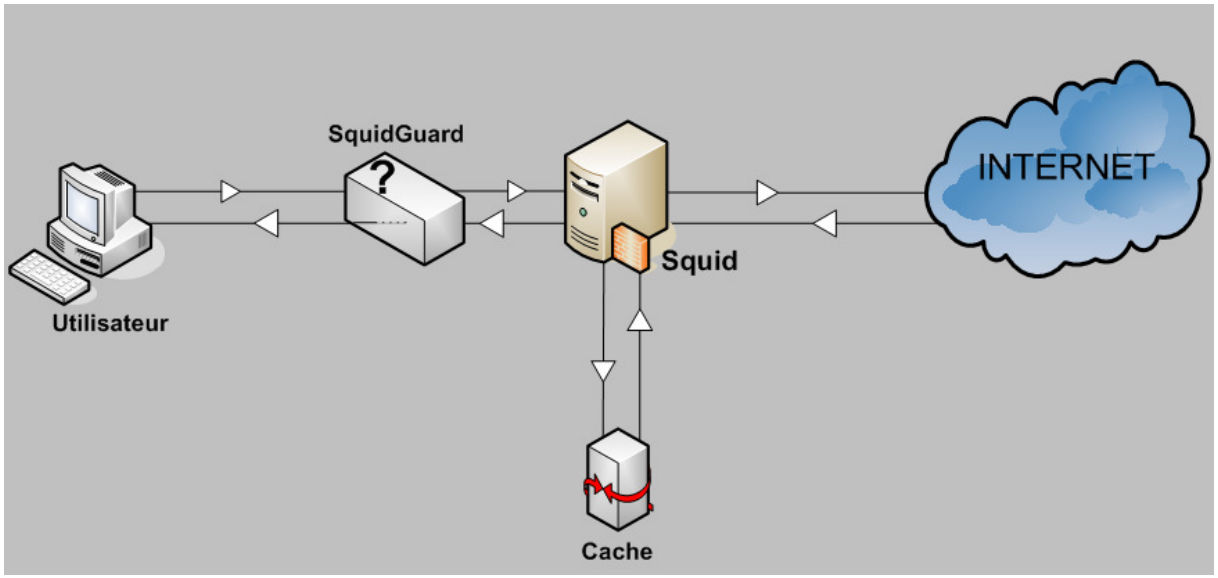
Er zijn vele parameters om de verbinding te tunen.
Uiteindelijk kun je voor een gelijkwaardige nieuwe Client gewoon een kopie maken en de specifieke zaken aanpassen.

Elke gebruiker krijgt natuurlijk wel zijn eigen keys, Public en Private.
De keys worden gemaakt en beheerd met XCA.
Aangemaakte keys kunnen ook weer worden ingetrokken, bv iemand die ergens anders gaat werken.

Squid



Squid zorgt voor centraal punt waar mee verbonden moet worden.
De requests worden dan van hieruit gedaan en uiteindelijk bij jou afgeleverd.
Door gebruikmaking van een cache kan bandbreedte worden bespaard en snelheid gewonnen.



Tevens kun je restricties opleggen vwb wie wat mag en wanneer, wij gebruiken hiertoe SquidGuard.
Dit werk obv White- en Blacklists icm ACL (Access Control List).
De whitelist vul je zelf, de blacklists kun je op diverse plaatsen ophalen.
Niet alle blacklists worden direct actief, je bepaalt zelf welke.
De volgorde bepaalt ook de wijze van afhandelen.
Elke request begint van links naar rechts in jouw lijst.
Je start met de whitelist en dan de lijst waar je de meeste hits verwacht.
Zodra er een hit is stopt de actie, dit spaart onnodige tijd en rekenkracht.

TOR

TOR is een netwerk van Entry en Exit Nodes welke er middels beveiligde tunnels voor zorgt dat je anoniem kunt browsen, de exit node is echter zonder encrypty.
Het systeem zorgt zelf voor de koppelingen met de tussenliggende nodes.
Door deze encrypty is niet te zien wat je doet, door de stappen ertussen niet wie of waar je bent.

Het is in eerste instantie ontwikkeld vanuit de US Navy, nu veelal gebruikt door dissidenten en anderen sterk aan privacy hechten.
Nu zijn wij niet echt uit de bange of stiekeme hoek, toch is er een voordeel voor ons, je bent niet te volgen door hen die Statistiek over je willen bijhouden.
Dit kan voor Marketing zijn of toch door overijverige Overheden.

Deze laatste kun je natuurlijk niet tegenhouden als je al in beeld bent.
Ons gaat het dus vooral om niet achtervolgd te worden door bedrijven met hun marketing en reclame, zij gebruiken hiervoor cookies danwel je IP.
Door je IP te koppelen aan door jou uitgevoerde acties en zoekopdrachten weten ze veel over je, meer dan je zou moeten willen.
Denk aan de Google's van deze wereld, alles beschikbaar voor NSA/CIA en dergelijke.
Vindt je dit niet van belang, gebruik dan gewoon geen TOR.

Gebruik als Client de TOR Browser Bundle , de speciaal geconfigureerde Firefox browser met alles voor correcte werking van TOR ingebouwd.
Tevens is de configuratie dusdanig aangepast dat er geen sporen worden achtergelaten, bv door cookies.

Wat wij gaan installeren is TOR als Gateway voor onze interne clients.
Je kunt er tevens voor kiezen een deel van je eigen bandbreedte ter beschikking te stellen aan anderen als een Relay.

Een nadeel van TOR is de verminderde snelheid tov normaal, dit omdat de tussenliggende bandbreedte wordt afgestaan door vrijwilligers en gebruik van encryptie.
Bedenk ook dat de exit nodes Plain Text zijn en niet iedereen is even betrouwbaar, dus let op met je gegevens over de lijn.

Bijlage Variabelen:

Vul ze hier vast in voor gebruik bij installatie/configuratie.

Variabele	*Hier Invullen*	*Omschrijving*	*Voorbeeld*
%HOST%		Server Naam	wodan
%DOMEIN%		Lokaal Domein	securitate.lan
%ROOTPWD%		Root Password	geheim
%BEHEERUSR%		Beheer User	beheer
%BEHEERPWD%		Beheer Password	tsPW0947
%EIGENAAR%		Systeem Eigenaar	SECURITATE
%NS1%		1e Name Server	194.109.6.66
%NS2%		2e Name Server	194.109.9.99
%VOORNAAM%		Jouw Voornaam	Patrick
%ACHTERNAAM%		Jouw Achternaam	Molier

Zorg dat je lokale domein eindigt op .lan voor een juiste werking intern.

Passwords blijken steeds eenvoudiger en sneller te kraken, gebruik dus minimaal 8 karakters in een mix van kleine letters, hoofdletters en cijfers.
Aangezien je middels de user beheer tevens rootrechten kunt krijgen middels sudo is ook hier een sterk password noodzakelijk, het is gewoon voor alle gebruikers noodzakelijk.

Gebruik de IP nummers van DNS servers die je van je eigen provider krijgt.

Links:

http://www.openbsd.org/
http://home.nuug.no/~peter/pf/en/
http://www.openvpn.net/index.php/open-source.html
http://www.squid-cache.org/
http://www.squidguard.org/index.html
https://www.torproject.org/index.html.en
http://infrarecorder.org/
http://www.chiark.greenend.org.uk/~sgtatham/putty/
http://www.7-zip.org/

Boeken:

Secure Architechtures with OpenBSD