

Kaan Gogcay – Infrastructuur

Inhoud

Introductie	1
[oefening] Waarom is mijn internet zo traag?.....	1
[oriëntatie] Netwerkvisualisatie en beschrijving	Fout! Bladwijzer niet gedefinieerd.
Deelproducten Oriëntatie	2
[oriëntatie] Netwerkvisualisatie en beschrijving	2
[oriëntatie] Basisnetwerkje in VMware Infrastructure virtuele omgeving.....	3
[oriëntatie] Plan van aanpak.....	4
[oriëntatie] Eigen lokale webserver	5
[oriëntatie] Secure Web Server	6
[oriëntatie] Serveromgeving	8
[oriëntatie] Beveiligingsrapportage, testen en oplevering.....	9

Introductie

In de eerste week gingen we een paar oefen opgaven maken. Een daarvan was andere landen pingen en kijken hoe lang het duurt totdat de ping terug is. Hieronder staan mijn gegevens van de opdracht.

[oefening] Waarom is mijn internet zo traag?

Hier zijn een paar pings naar andere landen.

Duitsland - Frankfurt	
Min	11 ms
Avg	184.9 ms
Max	1689 ms
Median	14.0 ms
Jitter	268.2 ms

Canada - Toronto	
Min	81 ms
Avg	111.7 ms
Max	837 ms
Median	82.0 ms
Jitter	61.3 ms

Australia - Sydney	
Min	268 ms
Avg	383.9 ms
Max	1126 ms
Median	269.0 ms
Jitter	199.3 ms

Ireland - Ireland	
Min	21 ms
Avg	77.2 ms
Max	854 ms
Median	23.0 ms
Jitter	108.8 ms

Conclusie: Hoe verder weg het van mij is, hoe langer de ping erover doet.

In de tweede opdracht moesten we kijken welke verbindingen je maakt als je wilt verbinden met de website AliExpress. Dit is wat info over het IP adres van AliExpress.

AliExpress

IP: 198.11.132.250

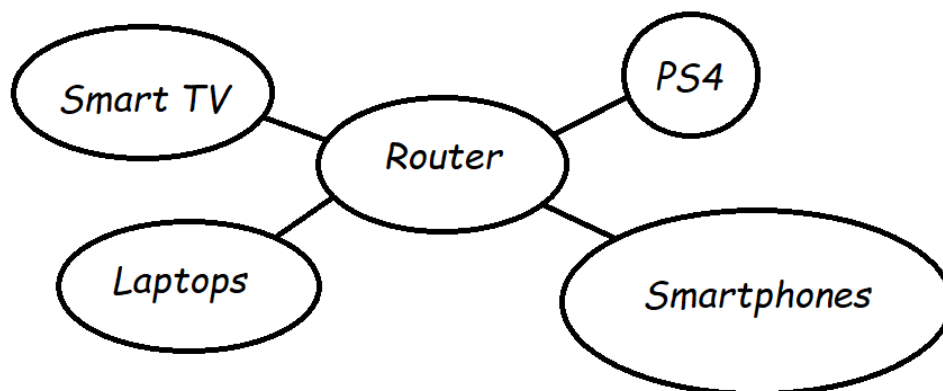
Locatie: United States - California

Verbindingen: Katwijk – Sizewell – Holyhead – Dublin - Lecanvey – Wall Township – California

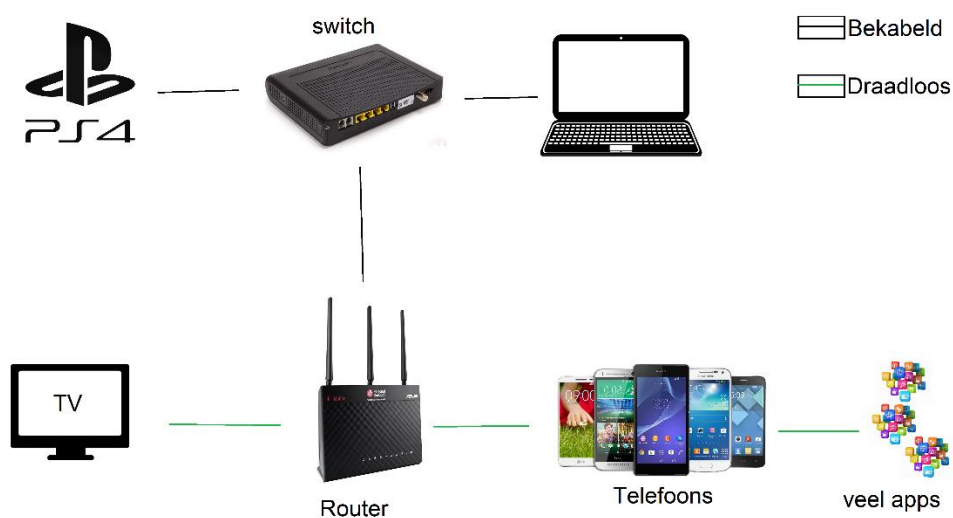
Deelproducten Oriëntatie

[oriëntatie] Netwerkvisualisatie en beschrijving

Dit is een tekening van hoe we bij mij thuis verbonden zijn met het internet.



Later heb ik een verbeterde versie gemaakt.



[\[oriëntatie\] Basisnetwerkje in VMware Infrastructure virtuele omgeving](#)

Ik ben begonnen met het aanmaken van een Ubuntu desktop, en een Ubuntu server. Ik kwam er al snel achter dat de Ubuntu server veel fijner was, dus ik ben verder gaan werken in de Ubuntu server.

Servernaam: "TestServerKG"

Desktopnaam: "UbuntuTestKG"

Via mijn Ubuntu desktop was ik nog niet verbonden met het internet. Om te verbinden met het internet moest ik het netwerk configureren. Hier heb ik bij de IPv4 Settings een paar dingen toegevoegd. Bij het adres heb ik mijn IP-adres ingevuld. Bij het subnetmask heb ik 255.255.255.0 ingevuld. De reden dat daar 24 staat is omdat 255.255.255.0 eigenlijk 11111111.11111111.11111111.00000000 is. En al die enen bij elkaar opgeteld is 24. Bij de gateway heb ik 192.168.153.1 ingevuld. En ten slotte heb ik de DNS ingevuld 192.168.200.13. Nu dat dit allemaal is ingevuld kan ik op het internet

Editing Wired connection 2

Connection name: **Wired connection 2**

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.153.40	24	192.168.153.1

DNS servers: 192.168.200.13

Search domains:

DHCP client ID:

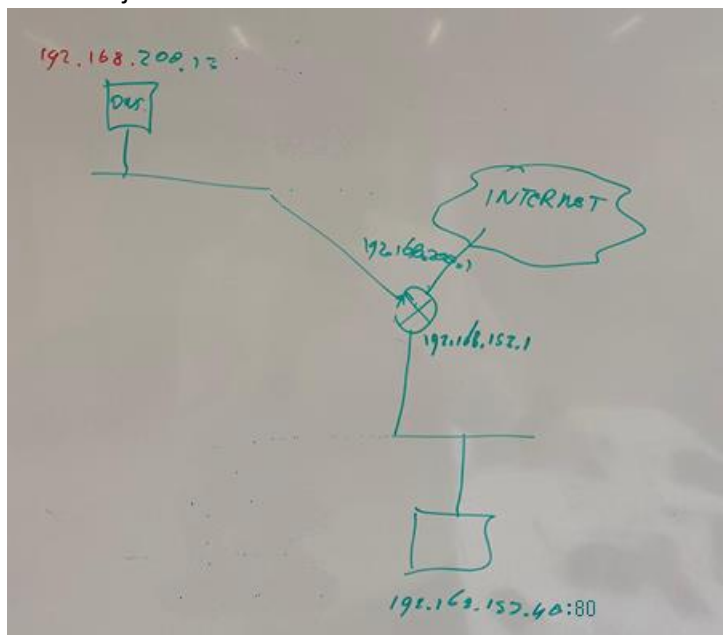
☐ Require IPv4 addressing for this connection to complete

Routes...

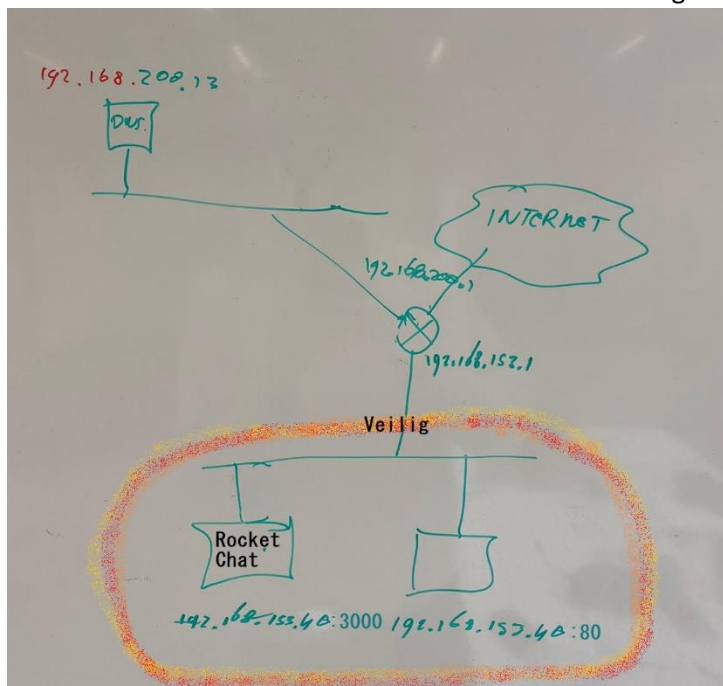
Cancel Save

[oriëntatie] Plan van aanpak

Zo ziet mijn server er nu uit.



Mijn doel nu is om mijn server te beveiligen en een chat achtig iets toe te voegen. Wat ik ook heb geleerd is dat als je je IP-adres invult je standaard naar port 80 gaat. Deze port is niet beveiligd. Maar hier ga ik nog op terugkomen bij een ander kopje. De vraag voor nu is, hoe kan ik een chat toevoegen aan mijn Ubuntu server? Door letterlijk dat op te zoeken kwam ik op iets dat Rocketchat heet. Naast het installeren van Rocketchat is het ook nog belangrijk dat de server beveiligd wordt.



[oriëntatie] Eigen lokale webserver

Zo ziet port 80 eruit



Swagg?

Yessir.



Op port 3000 heb ik rocketchat geïnstalleerd. Deze server werkt alleen als mijn firewall uitstaat. Dit heb ik opgelost door port 3000 aan de firewall toe te voegen.

```
student@student-vm-Ubuntu:/$ sudo ufw status
Status: active

To Action From
--
22/tcp LIMIT Anywhere
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
22/tcp (v6) LIMIT Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)

student@student-vm-Ubuntu:/$ sudo ufw allow 3000/tcp
ERROR: Bad port

student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$
student@student-vm-Ubuntu:/$ sudo ufw allow 3000/tcp
Rule added
Rule added (v6)

student@student-vm-Ubuntu:/$ sudo ufw status
Status: active

To Action From
--
22/tcp LIMIT Anywhere
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
3000/tcp ALLOW Anywhere
22/tcp (v6) LIMIT Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
3000/tcp (v6) ALLOW Anywhere (v6)

student@student-vm-Ubuntu:/$ sudo ufw disable
Firewall stopped and disabled on system startup
student@student-vm-Ubuntu:/$ sudo ufw enable
Firewall is active and enabled on system startup
student@student-vm-Ubuntu:/$
```

Rocket
Chat

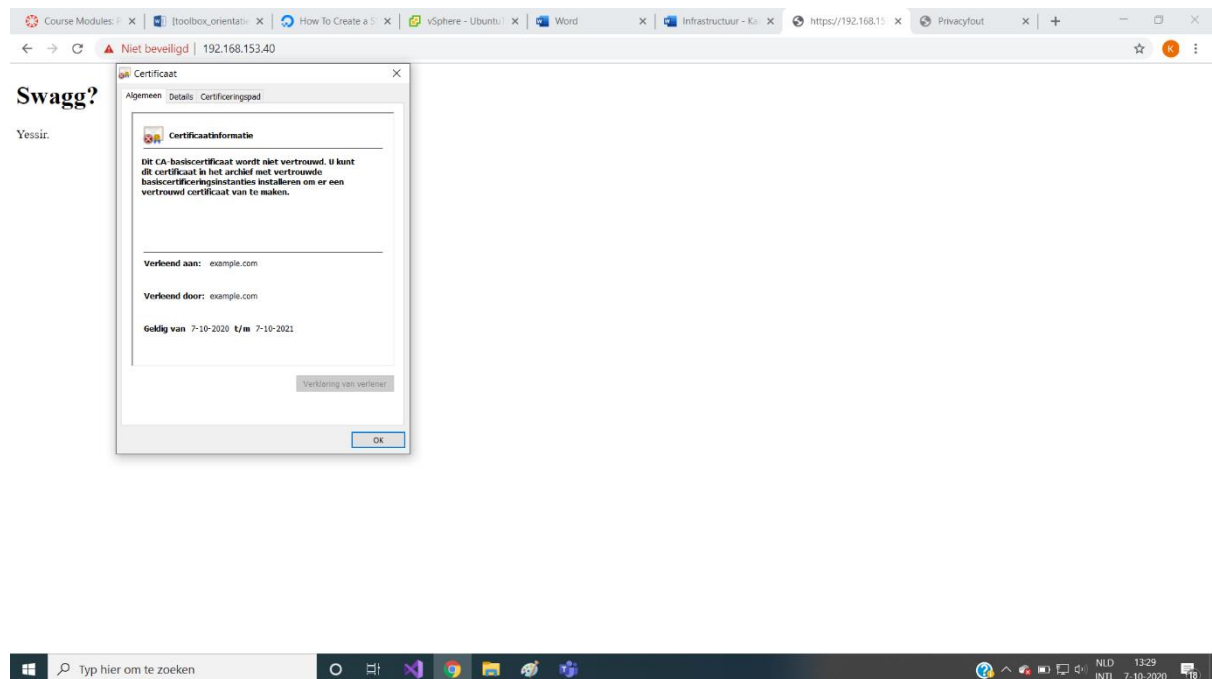
Werkt
Niet

Rocket
Chat

Werkt
Wel

[oriëntatie] Secure Web Server

Ik heb mijn server beveiligd. Ik heb nu een SSL certificaat. Dit is allemaal gelukt doordat ik deze module heb gevolgd. Mijn server heeft ook een firewall. Die heb ik kunnen installeren omdat ik een YouTube video heb gevolgd.



<https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-debian-8>

<https://youtu.be/7pJKBL9x6bY>

wat ik eigenlijk nu heb gedaan is, ik heb een nieuwe port aangemaakt namelijk :443. De port bij 443 is beveiligd met een SSL certificaat. Wat ik nu heb is mijn standaard port 80 die niet beveiligd is. Ik heb ook port 443 de veilige plek. En dan nog port 3000 de chat plek.

Als je gewoon 192.168.153.40 intypt dan kom je automatisch bij <https://192.168.153.40:443>. Dit is mijn veilige plek. Door dit te doen is het niet meer mogelijk om naar port 80 te gaan, dus je kunt niet meer naar de onveilige plek.

Ook heb ik geprobeerd om Rocketchat te beveiligen. Om Rocketchat te beveiligen heb ik gewoon opgezocht, How to secure Rocketchat. Ik heb gedaan wat er in de tutorial stond maar de site is niet veilig. Misschien is er een veilige versie van de site op een andere port ik heb echt geen idee, maar mijn normale website is veilig <https://192.168.153.40> en dat is voor nu het belangrijkste.

Hier laat ik nog even zien hoe ik dat heb gedaan dat die van port 80 naar 443 gaat. In witte letters zie je 'Redirect permanent' daarnaast staat waar je naartoe wordt doorverwezen.

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    ServerName 192.168.153.40

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    Redirect permanent / https://192.168.153.40/

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
student@student-vm-Ubuntu:~$ cd ../../
student@student-vm-Ubuntu:/$ ls
bin  cdrom  etc  initrd.img  lib  lost+found  mnt  mydomain.com.csr  opt
Rocket.Chat-root.crt  Rocket.Chat-root.srl  run  snap  srv  sys  usr  vmlinuz
boot  dev  home  initrd.img.old  lib64  media  mydomain.com.crt  mydomain.com.key  proc
Rocket.Chat-root.key  root  sbin  snap_backup  swapfile  tmp  var  vmlinuz.old
student@student-vm-Ubuntu:/$ s
```

Zoals je kunt zien heb ik wel de keys voor Rocketchat aangemaakt. Maarja ik laat het zoals het is.

[oriëntatie] Serveromgeving

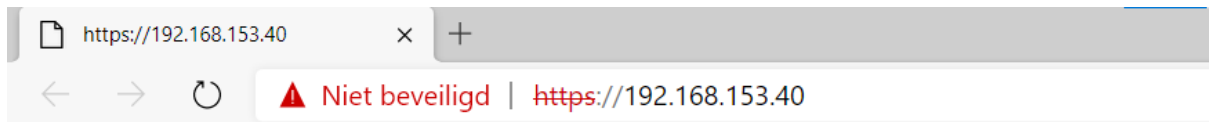
Andere kunnen mijn server bereiken door te gaan naar <https://192.168.153.40>. Zoals je kunt zien heb ik mijn naam en klas op de site gezet. ook zijn er 2 linkjes op de site. Naast de linkjes staat er ook wat ze doen en of ze veilig zijn. Het bedrijf linkje stuurt je door naar mijn YouTube kanaal.

```
GNU nano 4.0 index.html
<!DOCTYPE html>
<html>

<head>
<meta http-equiv="refresh" contents="10 URL='http://192.168.153.40:3000' />
</head>

<body>
<h1>Kaan Gogcay - PD03</h1>
<p>Swagg?</p>
<p>Yessir.</p>
<br>
<br>
<br>
<p>(niet veilig) RocketChat: <a href="http://192.168.153.40:3000"> http://192.168.153.40:3000 </a></p>
<br>
<p>Bedrijf: <a href="https://www.youtube.com/channel/UCSStYsZ5BEOI3iatCiAQAhA"> https://www.youtube.com/channel/UCSStYsZ5BEOI3iatCiAQAhA </a><p>
</body>
</html>
```

Hier zie je hoe ik de links heb toegevoegd. Was simpel weg even op internet iets als 'link html' opzoeken. Hieronder zie je hoe mijn site er nu uit ziet.



Kaan Gogcay - PD03

Swagg?

Yessir.

(niet veilig) RocketChat: <http://192.168.153.40:3000>

Bedrijf: <https://www.youtube.com/channel/UCSStYsZ5BEOI3iatCiAQAhA>

[oriëntatie] Beveiligingsrapportage, testen en oplevering

Wat is een sterk wachtwoord en noem enkele voorwaarden waar een sterk wachtwoord aan moet voldoen?

Een sterk wachtwoord bestaat uit meerdere tekens. En er moet afgewisseld worden tussen getallen letters en speciale tekens.

Welke veiligheid geeft een digitaal certificaat van een website?

Een digitaal certificaat zorgt ervoor dat de gegevens op de desbetreffende site ge-encrypt blijven. Zo kunnen hackers niet bij de gegevens.

Wat is patchmanagement is waarom is dit belangrijk?

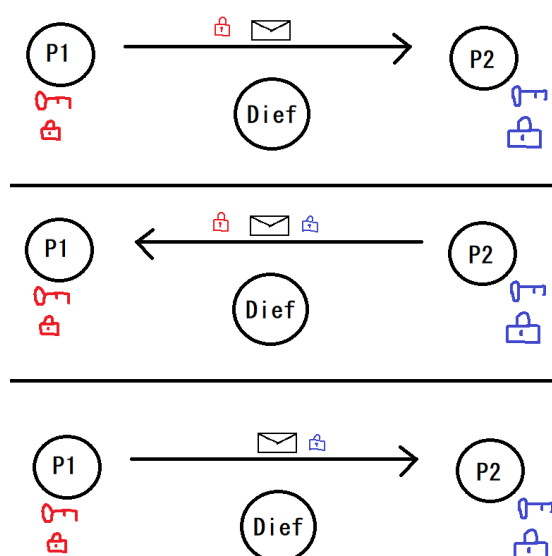
Patch management, het woord zegt het zelf al. Regelmatig van tijd tot tijd even de server een update geven, eventuele bugs eruit halen. Gewoon de server bijhouden en verzorgen.

Wat is hashing en het gebruik van salts hierbij en hoe maakt dit de opslag van wachtwoorden veiliger?

Met salt komen er random tekens voor het wachtwoord, met hashing wordt het wachtwoord dat opgeslagen is in een random code veranderd met random tekens die niet terugkeerbaar is. De wachtwoorden worden hierdoor veilig omdat het onomkeerbaar is.

Wat is een typische toepassing van symmetrische versleuteling?

Symmetrische versleuteling wordt gebruikt door de regering van de Verenigde Staten. Maar wat is symmetrische versleuteling. Stel dat er 2 mensen zijn die allebei een key hebben. Persoon 1 wilt een bericht sturen naar persoon 2. Tussen persoon 1 en 2 staat een dief te wachten die alles bekijkt wat er tussen persoon 1 en 2 verstuurt wordt. Als persoon 1 een bericht stuurt naar persoon 2, die hij vergrendelt met zijn key. Dan kan de dief niet zien wat er is gestuurd naar persoon 2. Het enige probleem is dat persoon 2 dit bericht niet kan lezen. Wat persoon 2 nu moet doen is het bericht vergrendelen met zijn eigen key en terug sturen. De dief ziet nu een bericht met 2 sloten en kan weer niks doen. Persoon 1 heeft het bericht weer en haalt de key eraf en stuurt het bericht weer naar persoon 2. De dief ziet nu alleen een slot van persoon 2. En nu kan persoon 2 het bericht veilig lezen. Hier heb ik het uitgetekend om overzichtelijker te maken.



Wat is een typische toepassing van asymmetrische versleuteling?

Voorbeelden van waar asymmetrische versleuteling wordt gebruikt zijn bij het verzenden van e-mails en internet browsen via https. Maar wat is asymmetrische versleuteling? Je kunt dit vergelijken met je brievenbus. Stel ik woon in een huis en ik heb een brievenbus. Iedereen die iets door mijn brievenbus wilt gooien weet waar het ligt. De locatie van mijn brievenbus is dus eigenlijk mijn public key. Maar om te zien wat er in mijn brievenbus zit hebben ze mijn huissleutel nodig (private key). Dus bij asymmetrische versleuteling. Gebruik je de public key van iemand om iets te versleutelen, vervolgens stuur je het naar die persoon die het alleen kan ontgrendelen met de private key.