Sprint 4 - Installatie- en configuratiehandleidingen

Installatie van LMS (moodle)

We hebben een linux server geïnstalleerd en hier gaan we eerst een LEMP op installeren

LEMP: Linux,Nignx(Engine X),Mariadb,PHP

Volg onderstaande configuratie stappen om de LEMP te installeren.

dnf update -y

dnf install nginx -y

systemctl enable nginx

systemctl start nginx

dnf install mariadb-server mariadb

systemctl enable mariadb

systemctl start mariadb

mysql_secure_installation

→ set root password : Y

Geef een rootpassword op en klik voor de rest bij alles yes aan.

dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

dnf install dnf-utils http://rpms.remirepo.net/enterprise/remi-release-8.rpm

We gaan PHP7.4 gebruiken dus we resetten de momentele actieve php versie

dnf module reset php

dnf module enable php:remi-7.4 → klik yes

Check welke php versie nu active is : # php -v

Enable en start php-fpm

systemctl enable php-fpm

systemctl start php-fpm

Open volgende file

```
# vim /etc/php-fpm.d/www.conf
```

Zoek onderstaande lijnen

```
user= apache
```

```
Group = apache
```

En vervang deze door :

```
User = nginx
```

```
group= =nginx
```

Herstart de php service

```
# systemctl restart nginx
```

```
Systemctl restart php-fpm
```

Moodle installatie

Installeer onderstaande pakketten die moodle nodig heeft om te werken:

```
# dnf install php-common php-iconv php-curl php-mbstring php-xmlrpc php-soap php-zip php-gd php-xml
php-intl php-json libpcre3 libpcre3-dev graphviz aspell ghostscript clamav
```

Nu maken we een database aan voor moodle in de mariadb

```
# mysql -u root -p (login met gekozen root pass)
```

In mariadb->>

```
→ CREATE DATABASE moodledb;
```

```
→ GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY TABLES,DROP,INDEX,ALTER ON
moodledb.* TO 'moodleadmin'@'localhost' IDENTIFIED BY 'Pxl-2021';
```

```
→ FLUSH PRIVILEGES;
```

```
→ exit
```

Haal het installatie pakket van moodle af:

```
# wget -c https://download.moodle.org/download.php/direct/stable39/moodle-latest-39.tgz
```

Pak het pakket uit:

```
# tar -xzvf moodle-latest-39.tgz
```

```
# mv moodle /var/www/html
```

```
# chmod 775 -R /var/www/html/moodle
# chown nginx:nginx -R /var/www/html/moodle

# mkdir -p /var/www/html/moodledata

# chmod 770 -R /var/www/html/moodledata

# chown :nginx -R /var/www/html/moodledata

# cd /var/www/html/moodle

# cp config-dist.php config.php

# vim config.php
```

Pas in deze file de lijnen aan naar eigen aangemaakte database

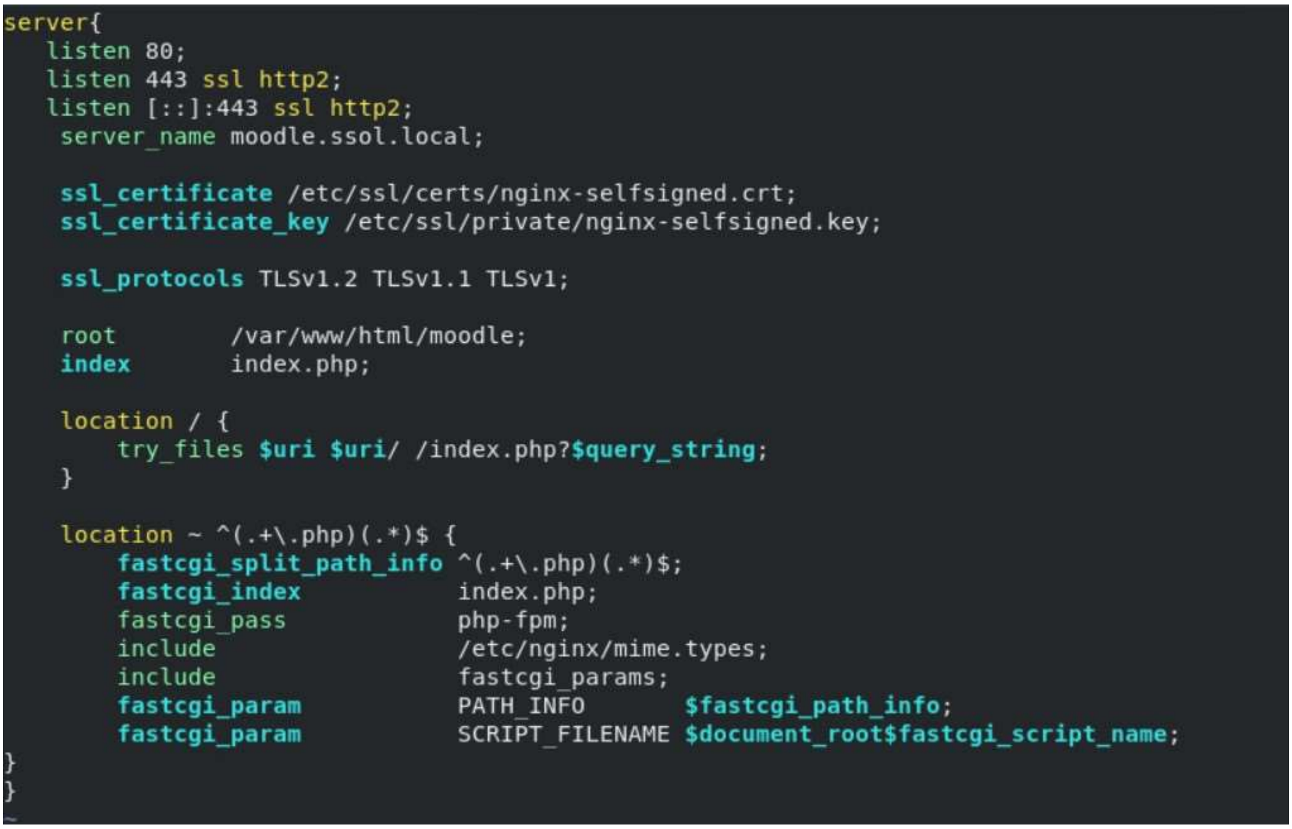
```
$CFG->dbtype    = 'mariadb';      // 'pgsql', 'mariadb', 'mysqli', 'sqlsrv' or 'oci'

$CFG->dblibrary = 'native';     // 'native' only at the moment

$CFG->dbhost    = 'localhost';  // eg 'localhost' or 'db.isp.com' or IP

$CFG->dbname    = 'moodledb';     // database name, eg moodle

$CFG->dbuser    = 'moodleadmin';   // your database username

$CFG->dbpass    = 'Pxl-2021';   // your database password

$CFG->prefix    = 'mdl_';       // prefix to use for all table names
```

Verander deze lijnen ook in de file

```
$CFG->wwwroot   = 'http://moodle.ssol.local';

$CFG->dataroot  = '/var/www/html/moodledata';
```

Configureren van nginx bestand voor moodle

vim /etc/nginx/conf.d/moodle.conf zorg dat de configuratie er uit ziet als onderstaande:



```
server{
   listen 80;
   listen 443 ssl http2;
   listen [::]:443 ssl http2;
    server_name moodle.ssol.local;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    ssl_protocols TLSv1.2 TLSv1.1 TLSv1;

    root        /var/www/html/moodle;
    index       index.php;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ ^(.+\.php)(.*)$ {
        fastcgi_split_path_info ^(.+\.php)(.*)$;
        fastcgi_index           index.php;
        fastcgi_pass            php-fpm;
        include                 /etc/nginx/mime.types;
        include                 fastcgi_params;
        fastcgi_param           PATH_INFO       $fastcgi_path_info;
        fastcgi_param           SCRIPT_FILENAME $document_root$fastcgi_script_name;
}
}
```

Hier komen we later op terug voor de https.

Om te testen dat de configuratie ok is :

```
# nginx -t
```

```
#systemctl restart nginx
```

```
#systemctl restart php-fpm
```

Voor SELinux

```
# setsebool -P httpd_can_network_connect on
```

```
# chcon -R --type httpd_sys_rw_connect_t /var/www/html
```

Open ook de firewall poorten:

```
# firewall-cmd --permanent --zone=public --add-service=http
```

```
# firewall-cmd --permanent --zone=public --add-service=https
```

```
# firewall-cmd --reload
```

Aanmaken van self signed certificate voor nginx

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt

Geef informartie op voor het cerificaat.

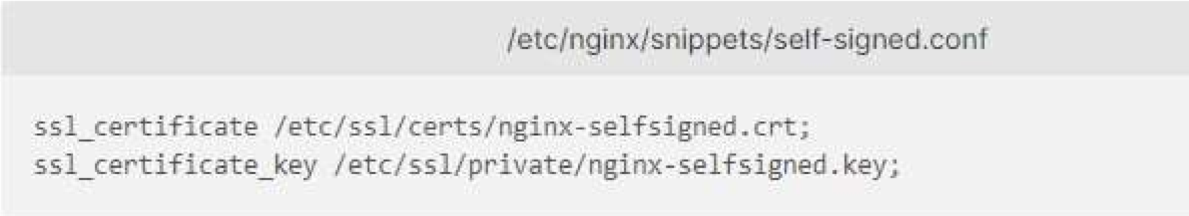
BE, LIMBURG, HASSELT, SSOL, IT, 10.14.1.19, admin@ssol.local

openssl dhparam -out /etc/nginx/dhparam.pem 4096

mkdir -p /etc/nginx/snippets

vim /etc/nginx/snippets/self-signed.conf

Hier moeten we het pad naar het certificaat definiëren en de key.



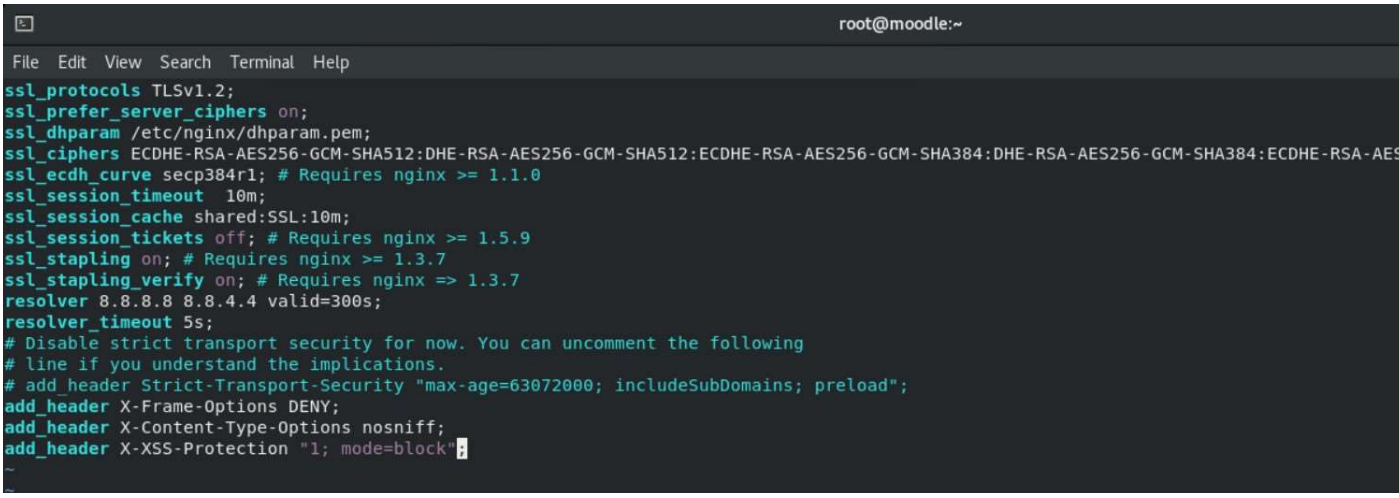
/etc/nginx/snippets/self-signed.conf

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

Nu maken we een configuratie bestand aan met sterk geëncrypteerde settings.

vim /etc/nginx/snippets/ssl-params.conf

Zie dat de configuratie er als volgende uit ziet.



```
ssl_protocols TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES
ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
ssl_session_timeout  10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off; # Requires nginx >= 1.5.9
ssl_stapling on; # Requires nginx >= 1.3.7
ssl_stapling_verify on; # Requires nginx => 1.3.7
resolver 8.8.8.8 8.8.4.4 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
# add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
~
~
```

Nginx ssl laten gebruiken.

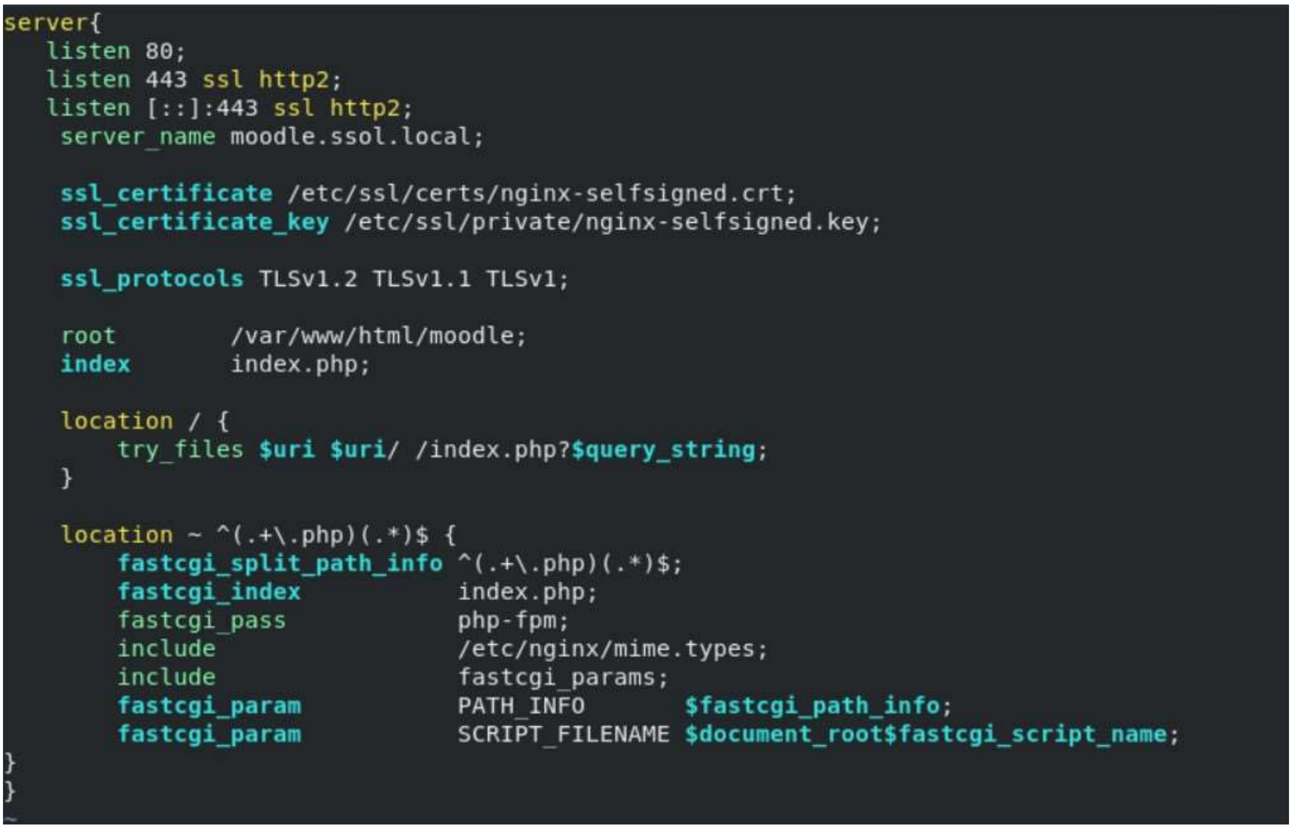
Backup het config bestand

#cp /etc/nginx/conf.d/moodle.conf /etc/nginx/conf.d/moodle.conf.bak

Open nu het moodle.conf bestand

vim /etc/nginx/conf.d/moodle.conf

Kijk nogmaals of deze staat zoals vorige keer beschreven.



```
server{
   listen 80;
   listen 443 ssl http2;
   listen [::]:443 ssl http2;
    server_name moodle.ssol.local;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    ssl_protocols TLSv1.2 TLSv1.1 TLSv1;

    root        /var/www/html/moodle;
    index       index.php;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ ^(.+\.php)(.*)$ {
        fastcgi_split_path_info ^(.+\.php)(.*)$;
        fastcgi_index           index.php;
        fastcgi_pass            php-fpm;
        include                 /etc/nginx/mime.types;
        include                 fastcgi_params;
        fastcgi_param           PATH_INFO       $fastcgi_path_info;
        fastcgi_param           SCRIPT_FILENAME $document_root$fastcgi_script_name;
}
}
```

ufw allow ‘Nginx Full’

ufw delete allow ‘Nginx HTTP’

nginx -t

#systemctl restart nginx

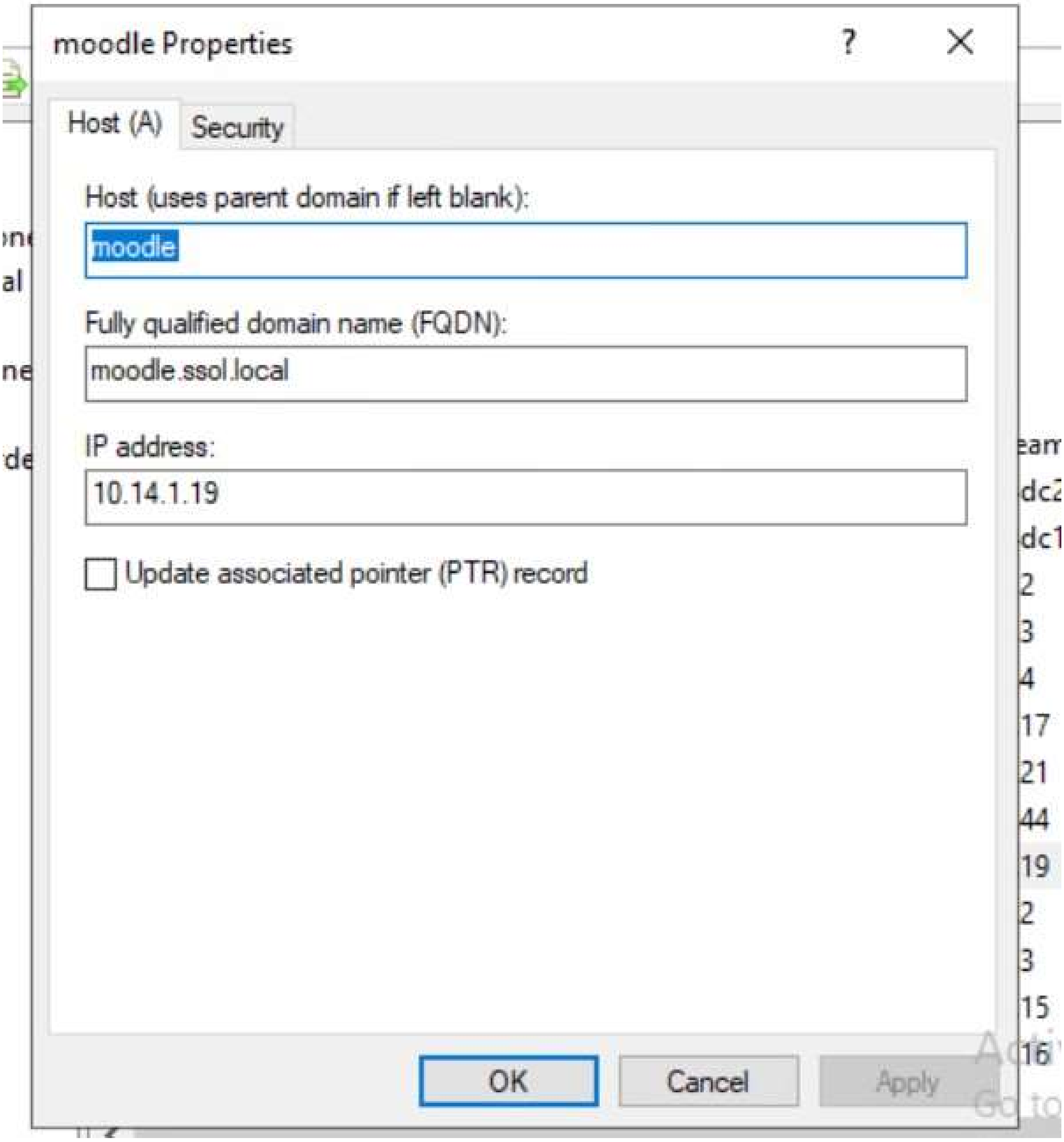
Aanmaken van dns record.

Ga naar de windows server met de dns zone van je domain.

DNS > forward lookup zones > ssol.local

RMK > New host (A or AAAA)...

Geef de naam die je wilt voor je moodle server & koppel het ip van de server:



Host (uses parent domain if left blank):
moodle

Fully qualified domain name (FQDN):
moodle.ssol.local

IP address:
10.14.1.19

□ Update associated pointer (PTR) record

Surf nu naar https://moodle.ssol.local:

Volg de op de site de setup verder.

Connect moodle met LDAP zodat gebruikers van het domain kunnnen inloggen.

Navigeer naar Site administration > plugins > Authentication.

Enable de LDAP server en klik op settings.

Vul in zoals onderstaande :

LDAP Server settings

Host url : url naar de AD = ldap://10.14.2.2

Version 3

Use lts :no

LDAP encoding: utf-8

Bind settings

Prevent password caching: yes

Distinguised name: cn=Administrator,cn=Users,dc=ssol,dc=local

Password: geeft het wachtwoord van de gekozen user hierboven.

User lookup settings

User type: MS ActiveDirectory

Contexts: ou=school,dc=ssol,dc=local

Search subcontexts: yes

Dereference aliases: no

User attribute: samaccountname

Member attribute uses dn: no

Object class : (objectClass=user)

Force change password

Force change password: no

Use standard page for changing password: no

Password format: plain text

Password-change URL: 10.14.2.2

LDAP password expiry settings

Expiry: no

Grace logins: no

Enable user creation

Create users externally: no

System role mapping

Mangager context: ou=Domain Admins,ou=SCHOOL,dc=ssol,dc=local

User account synchronisation

Removed ext user: Keep internal

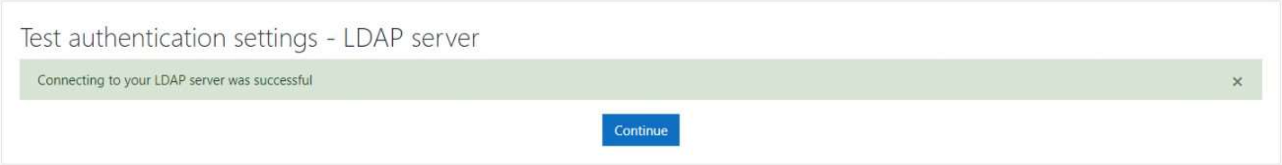
Synchronise local user suspension status: no

NTLM SSO

Enable:no

Save changes!

Klik op test settings:

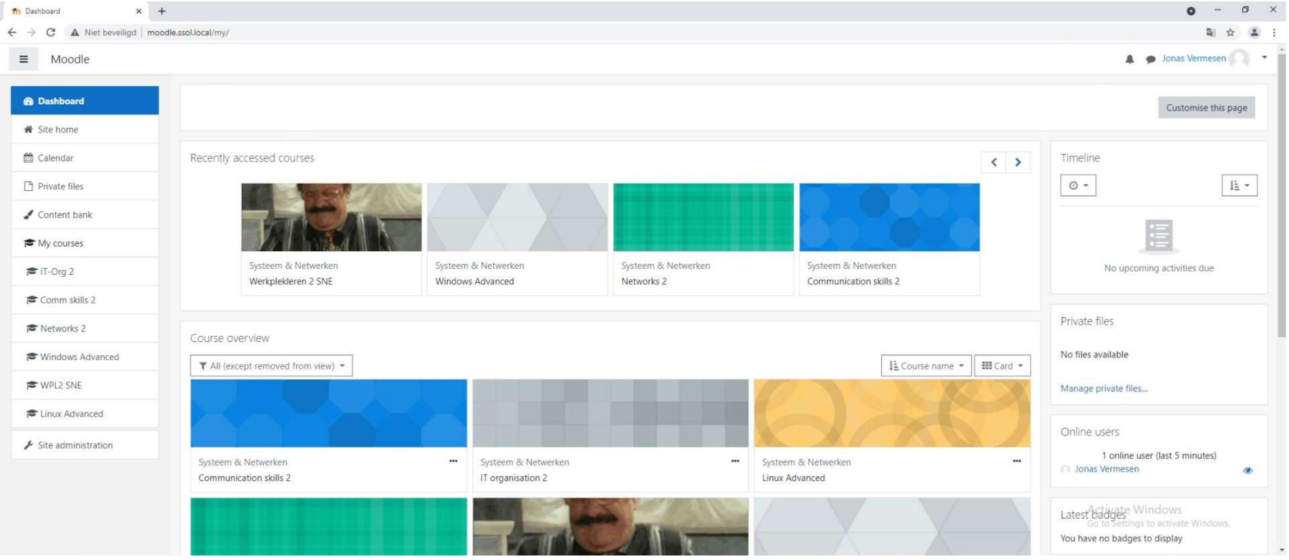


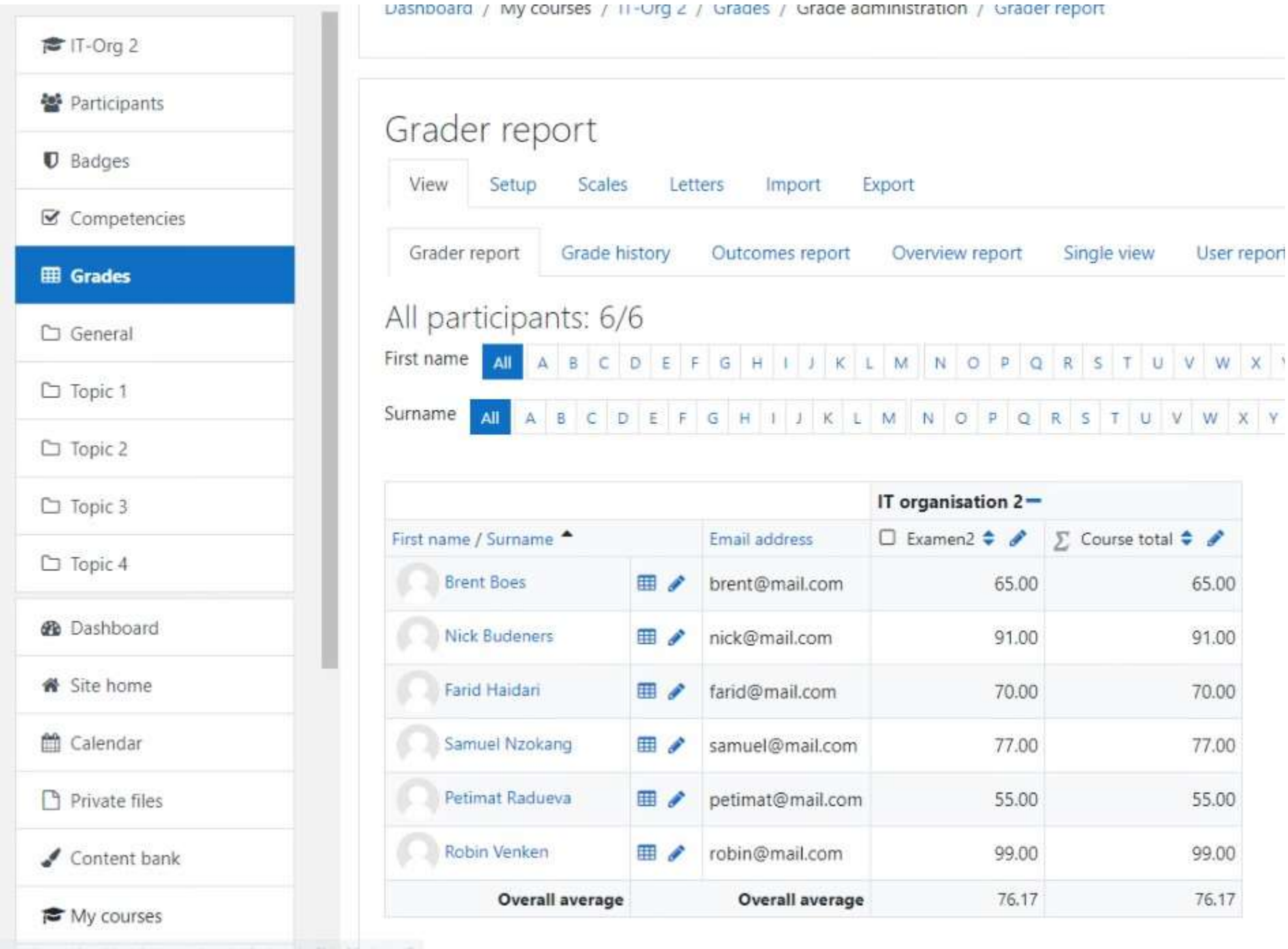
Test authentication settings - LDAP server

Connecting to your LDAP server was successful

Nu kan je inloggen via AD users.

Op de moodle kan je verschillende soorten vakken aanmaken en users bepaalde rollen geven zoals student of teachers. Hier kan dan les materiaal aan toegevoegd worden en punten op worden geplaatst!





Grader report

All participants: 6/6

		IT organisation 2	
First name / Surname	Email address	Examen2	Course total
Brent Boes	brent@mail.com	65.00	65.00
Nick Budeners	nick@mail.com	91.00	91.00
Farid Haidari	farid@mail.com	70.00	70.00
Samuel Nzokang	samuel@mail.com	77.00	77.00
Petimat Radueva	petimat@mail.com	55.00	55.00
Robin Venken	robin@mail.com	99.00	99.00
Overall average	Overall average	76.17	76.17

Aanmaken van publieke school website

Ook hier hebben we linux server voor aan gemaakt.

Op deze server gaan we een LAMP installeren, deze gebruikt dan Apache ipv Nginx

Volg onderstaande stappen

dnf update -y

dnf install httpd httpd-tools

systemctl start httpd

#systemctl enable httpd

#firewall-cmd --permanent --zone=public --add-service=http

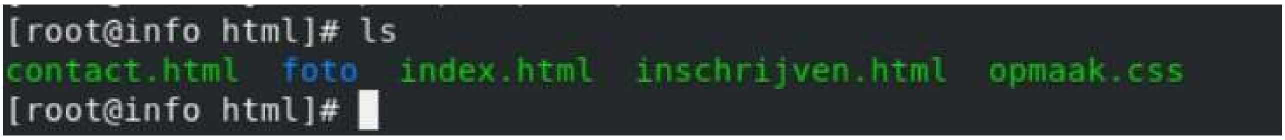
#firewall-cmd --permanent --zone=public --add-service=https

systemctl reload firewalld

chown apache:apache /var/www/html -R

cd /var/www/html

Ik heb een kleine website gemaakt en die in deze map geplaatst.cd



```
[root@info html]# ls
contact.html  foto  index.html  inschrijven.html  opmaak.css
[root@info html]#
```

#systemctl reload httpd.

Self signed certificate voor https

Maken van het certificaat.

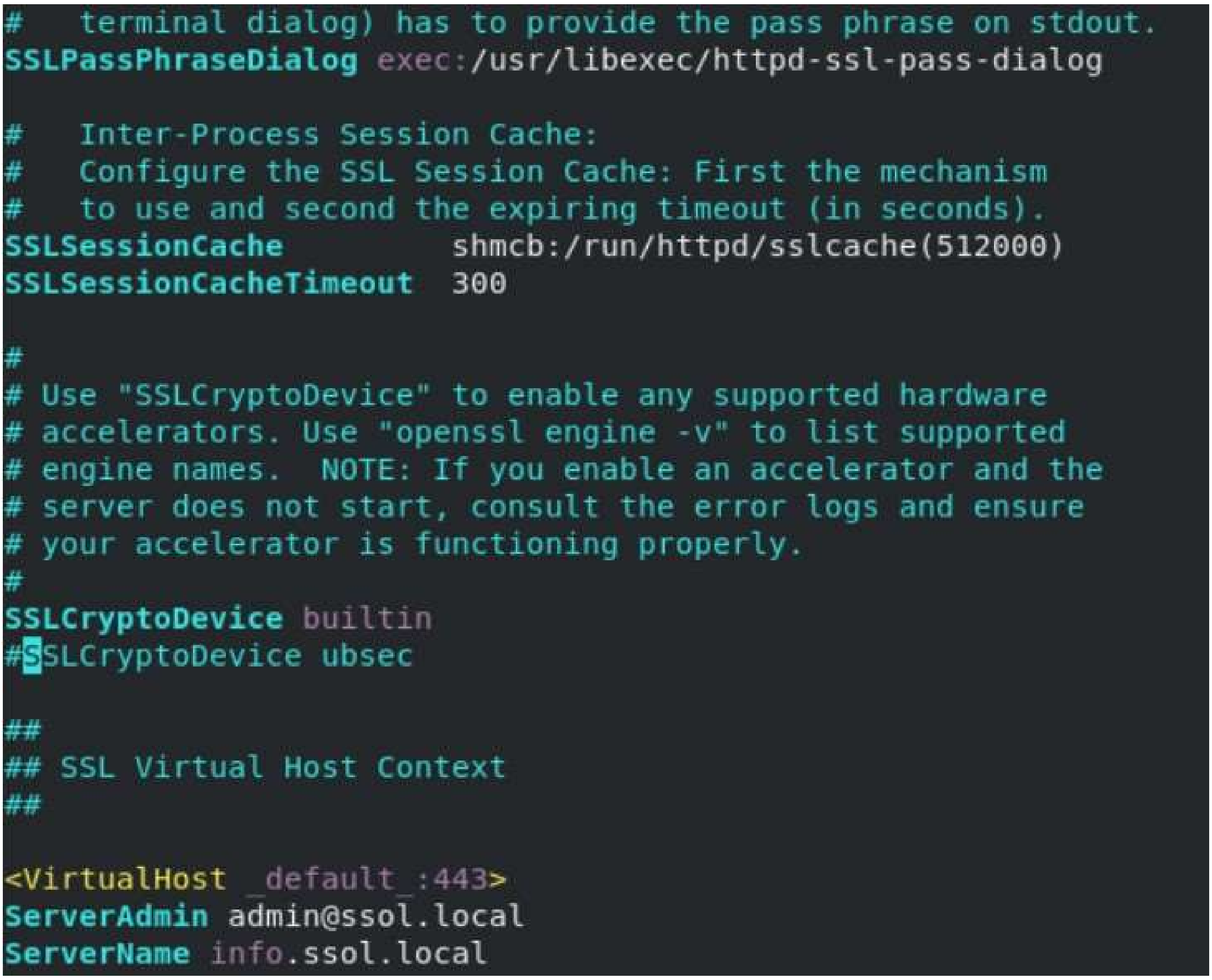
dnf install mod_ssl -y

#mkidr -p /etc/ssl/private

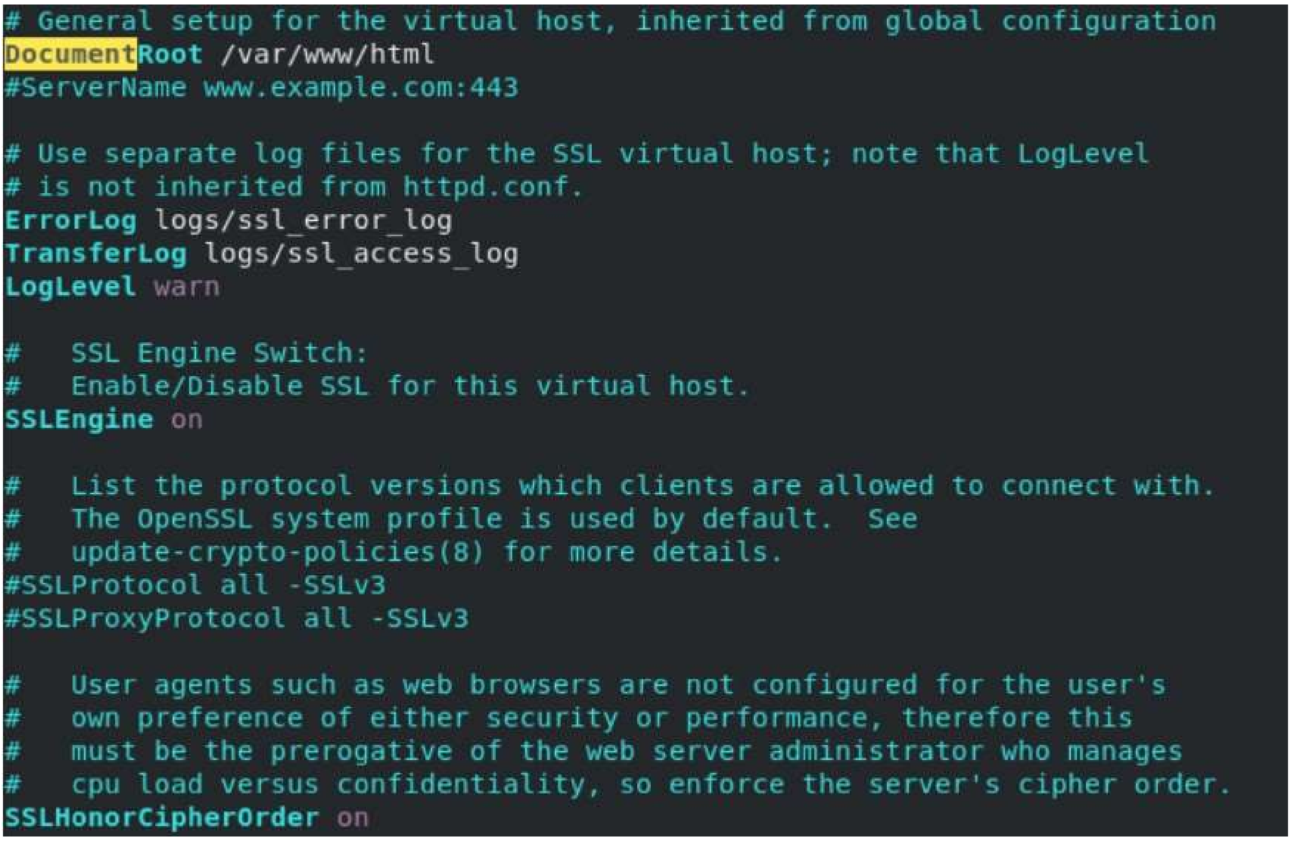
openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/ssl/private/site00.key -out /etc/ssl/certs/site00.crt

#vim /etc/httpd/conf.d/ssl.conf

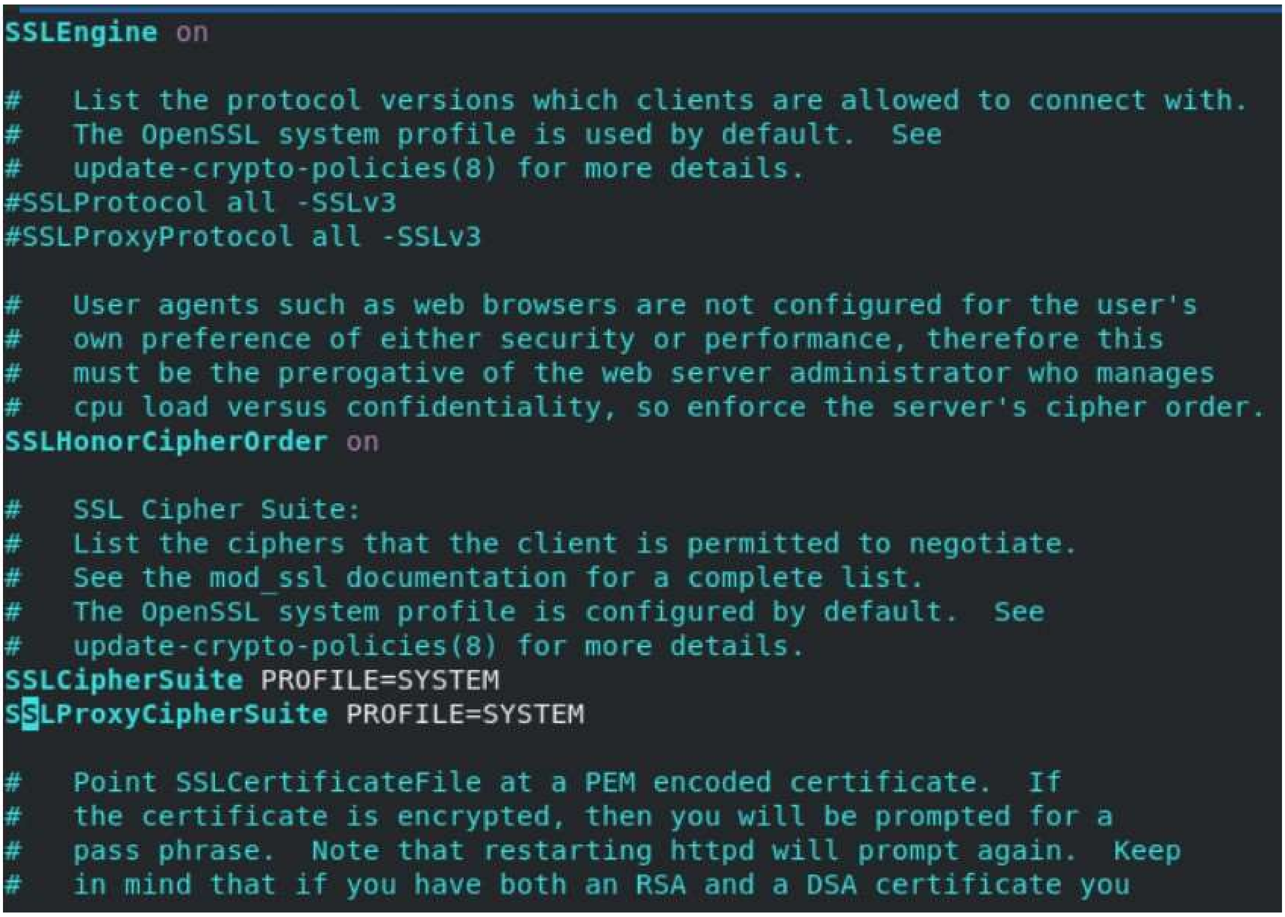
ZORG dat de config er als volgend uit ziet.



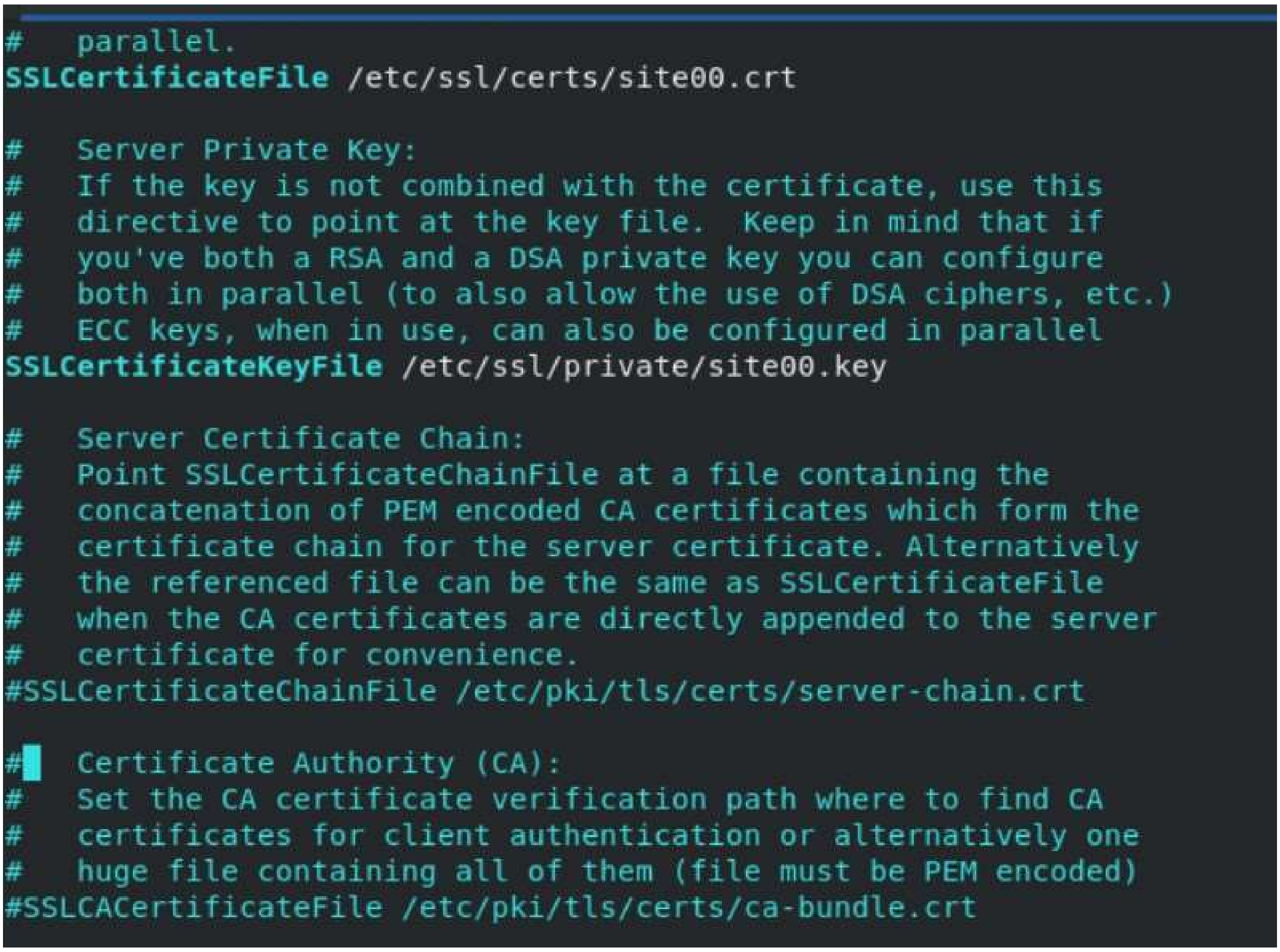
```
#   terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog

#   Inter-Process Session Cache:
#   Configure the SSL Session Cache: First the mechanism
#   to use and second the expiring timeout (in seconds).
SSLSessionCache         shmcb:/run/httpd/sslcache(512000)
SSLSessionCacheTimeout  300

#
# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names.  NOTE: If you enable an accelerator and the
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
ServerAdmin admin@ssol.local
ServerName info.ssol.local
```



```
# General setup for the virtual host, inherited from global configuration
DocumentRoot /var/www/html
#ServerName www.example.com:443

# Use separate log files for the SSL virtual host; note that LogLevel
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   List the protocol versions which clients are allowed to connect with.
#   The OpenSSL system profile is used by default.  See
#   update-crypto-policies(8) for more details.
#SSLProtocol all -SSLv3
#SSLProxyProtocol all -SSLv3

#   User agents such as web browsers are not configured for the user's
#   own preference of either security or performance, therefore this
#   must be the prerogative of the web server administrator who manages
#   cpu load versus confidentiality, so enforce the server's cipher order.
SSLHonorCipherOrder on
```



```
SSLEngine on

#   List the protocol versions which clients are allowed to connect with.
#   The OpenSSL system profile is used by default.  See
#   update-crypto-policies(8) for more details.
#SSLProtocol all -SSLv3
#SSLProxyProtocol all -SSLv3

#   User agents such as web browsers are not configured for the user's
#   own preference of either security or performance, therefore this
#   must be the prerogative of the web server administrator who manages
#   cpu load versus confidentiality, so enforce the server's cipher order.
SSLHonorCipherOrder on

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#   The OpenSSL system profile is configured by default.  See
#   update-crypto-policies(8) for more details.
SSLCipherSuite PROFILE=SYSTEM
SSLProxyCipherSuite PROFILE=SYSTEM

#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that restarting httpd will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
```

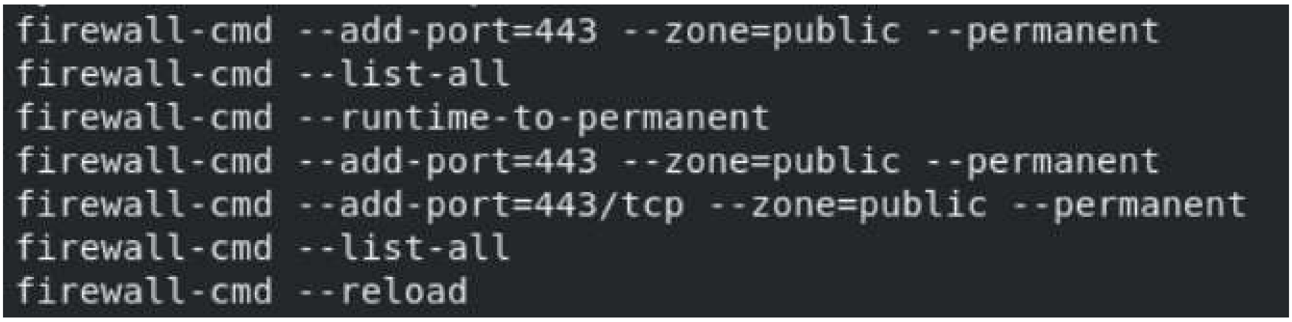


```
#   parallel.
SSLCertificateFile /etc/ssl/certs/site00.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#   ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile /etc/ssl/private/site00.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convenience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

:wq

systemctl restart httpd

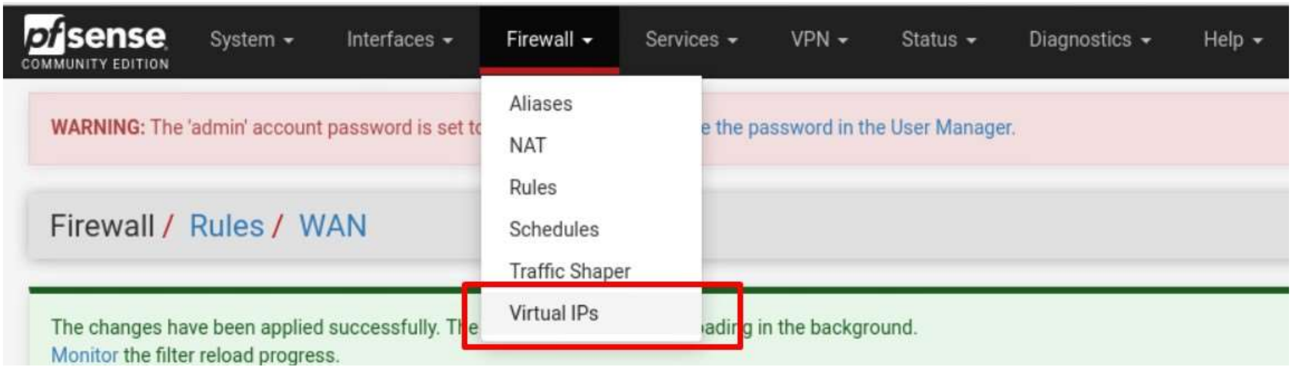
Firewall settings:



```
firewall-cmd --add-port=443 --zone=public --permanent
firewall-cmd --list-all
firewall-cmd --runtime-to-permanent
firewall-cmd --add-port=443 --zone=public --permanent
firewall-cmd --add-port=443/tcp --zone=public --permanent
firewall-cmd --list-all
firewall-cmd --reload
```

PFsense Natting

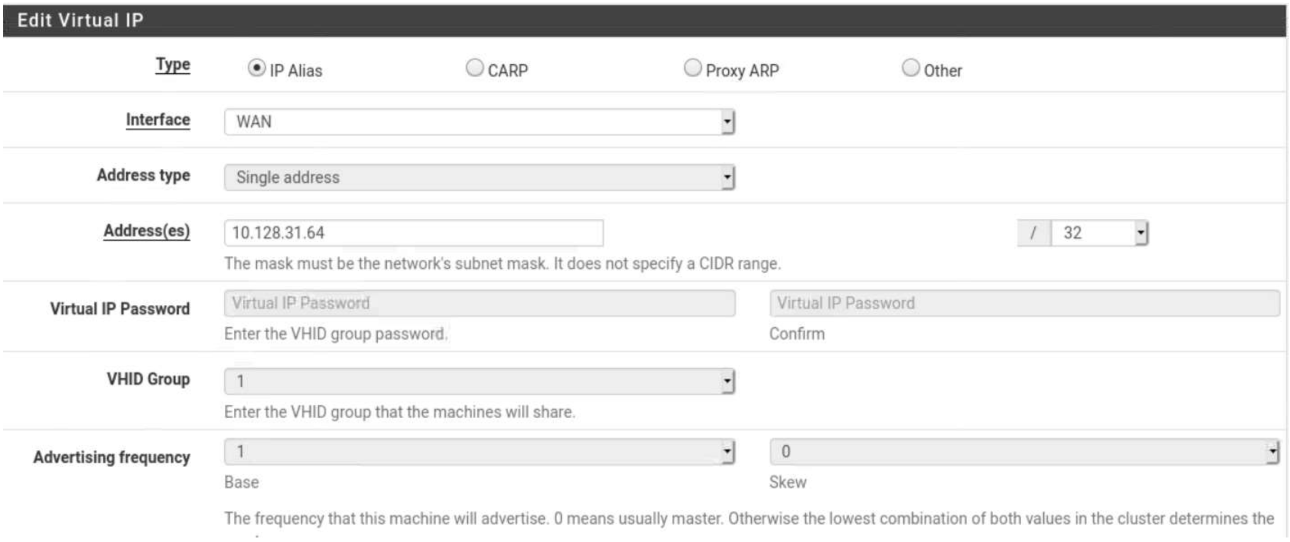
Maak een virtual IP aan



WARNING: The 'admin' account password is set t… …e the password in the User Manager.

Firewall / Rules / WAN

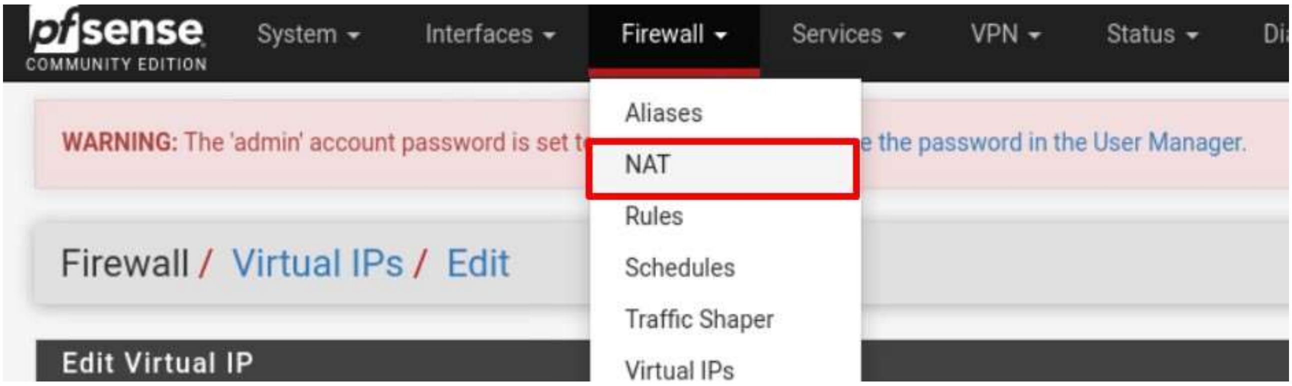
The changes have been applied successfully. Th… …ading in the background.
Monitor the filter reload progress.



Edit Virtual IP

Type	● IP Alias ○ CARP ○ Proxy ARP ○ Other
Interface	WAN
Address type	Single address
Address(es)	10.128.31.64 / 32 The mask must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password	Virtual IP Password Enter the VHID group password. Virtual IP Password Confirm
VHID Group	1 Enter the VHID group that the machines will share.
Advertising frequency	1 Base 0 Skew The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the

Opslaan en navigeer naar NAT



WARNING: The 'admin' account password is set t… …e the password in the User Manager.

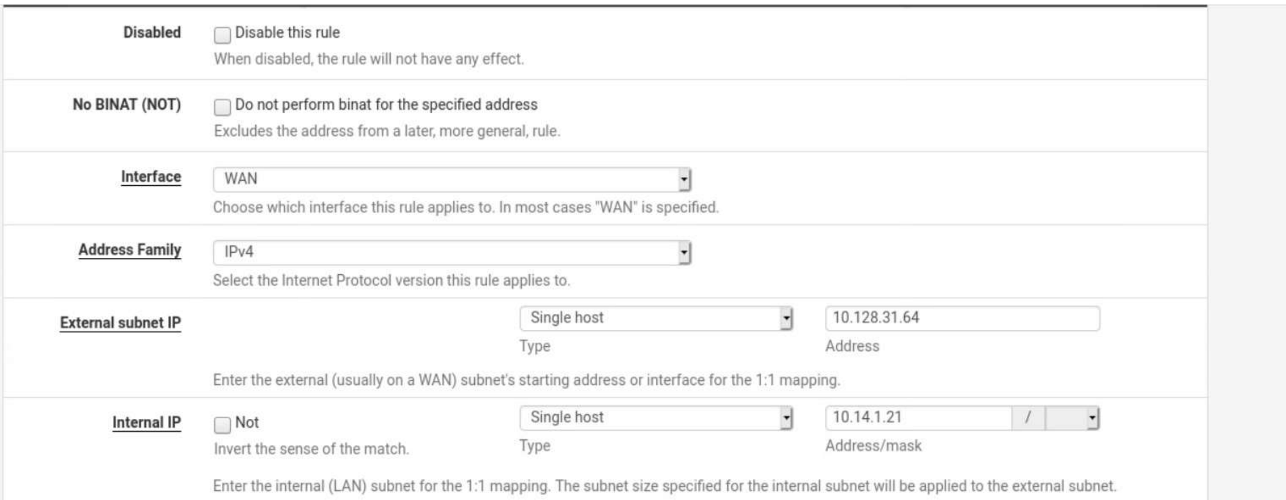
Firewall / Virtual IPs / Edit

Edit Virtual IP

Ga naar 1:1 en klik op Add

Bij external subnet ip geef je virtual ip adres op.

Bij internal ip het ipadres van je webserver.



Disabled □ Disable this rule
When disabled, the rule will not have any effect.

No BINAT (NOT) □ Do not perform binat for the specified address
Excludes the address from a later, more general, rule.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

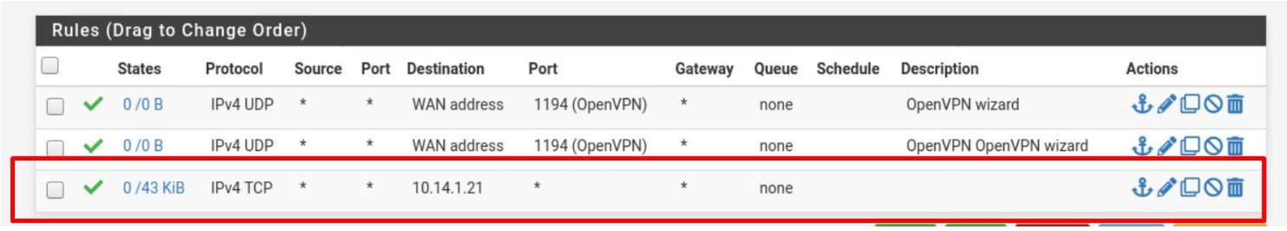
Address Family IPv4
Select the Internet Protocol version this rule applies to.

External subnet IP Single host (Type) 10.128.31.64 (Address)
Enter the external (usually on a WAN) subnet's starting address or interface for the 1:1 mapping.

Internal IP □ Not — Invert the sense of the match. Single host (Type) 10.14.1.21 / (Address/mask)
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Save & apply changes!

En maak een nieuwe rule aan op de WAN interface zodat de webserver bezocht kan worden.



Rules (Drag to Change Order)

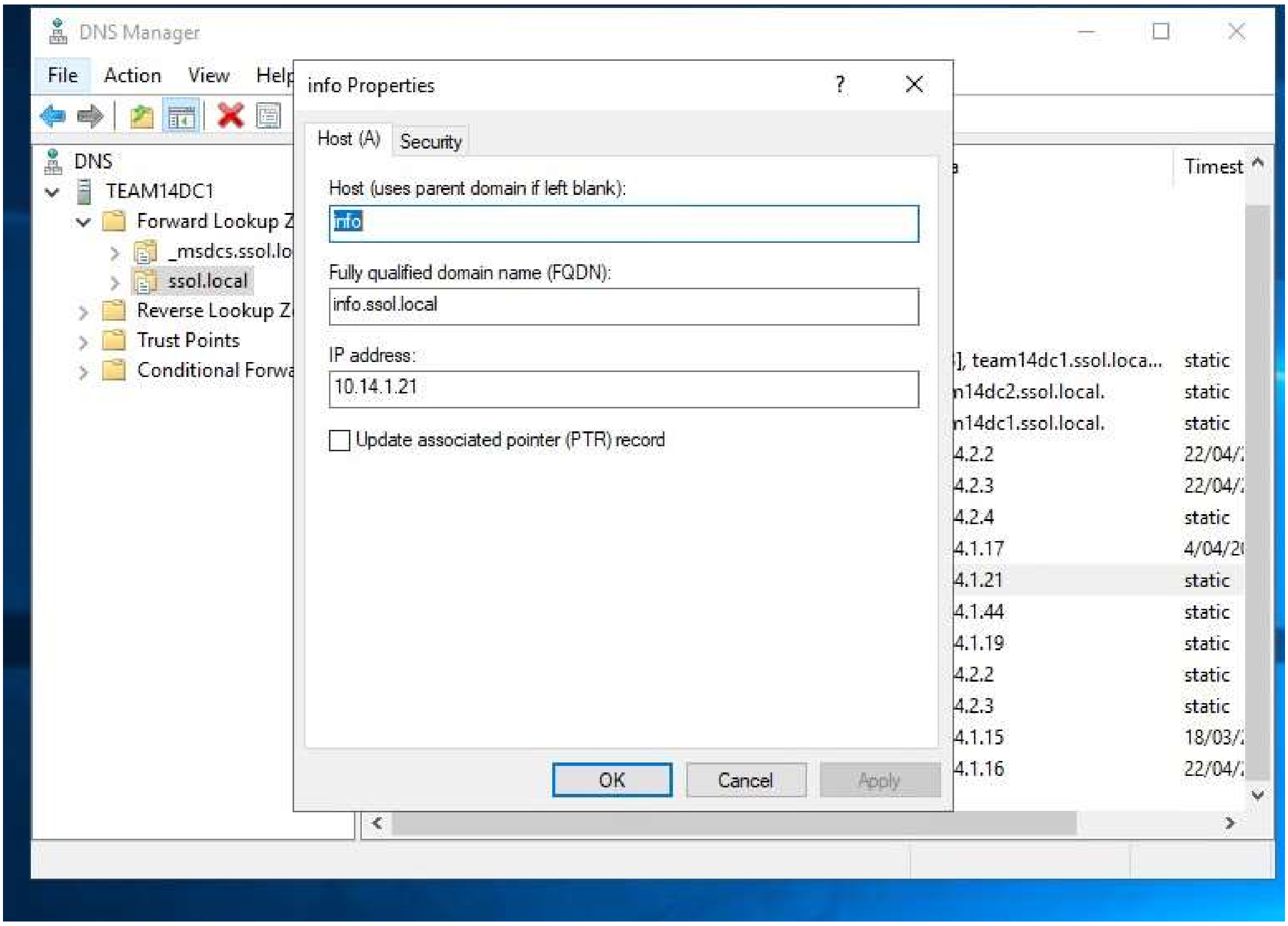
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	
□	✓	0 /0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN wizard	
□	✓	0 /43 KiB	IPv4 TCP	*	*	10.14.1.21	*	*	none			

Save & apply changes!

DNS record aanmaken.

Onder DNS > forward lookup zones> ssol.local> new Host A

Geef een naam op en koppel het IP adres.



info Properties

Host (A) | Security

Host (uses parent domain if left blank):
info

Fully qualified domain name (FQDN):
info.ssol.local

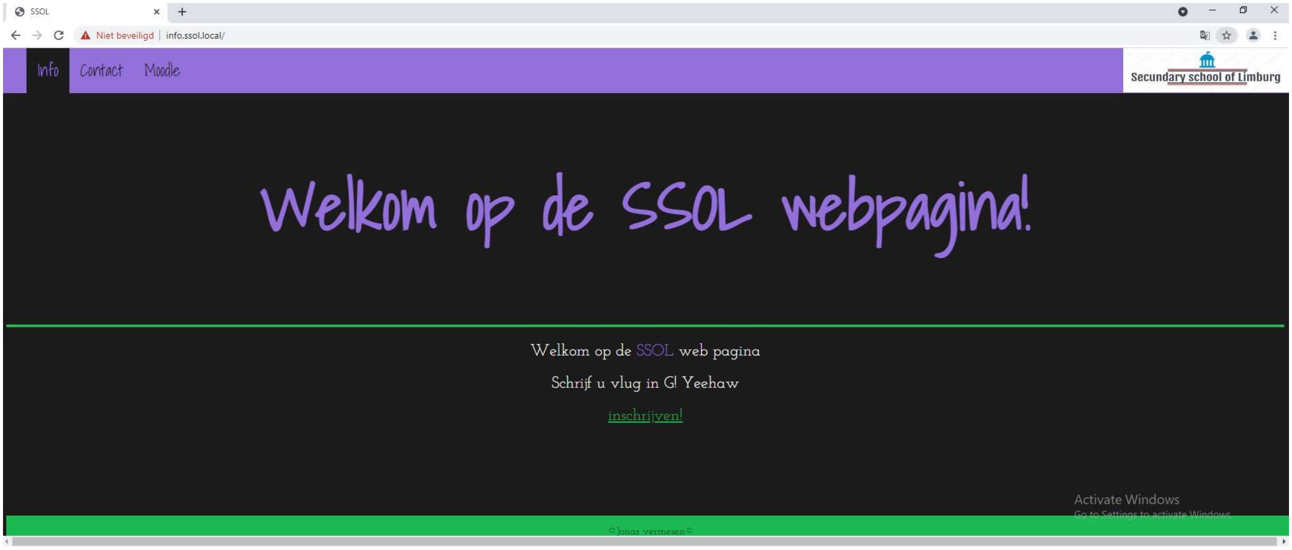
IP address:
10.14.1.21

□ Update associated pointer (PTR) record

OK
Cancel
Apply

```
], team14dc1.ssol.loca...   static
n14dc2.ssol.local.          static
n14dc1.ssol.local.          static
4.2.2                       22/04/:
4.2.3                       22/04/:
4.2.4                       static
4.1.17                      4/04/2(
4.1.21                      static
4.1.44                      static
4.1.19                      static
4.2.2                       static
4.2.3                       static
4.1.15                      18/03/:
4.1.16                      22/04/:
```

Als we nu in het domain surfen naam https://info.ssol.local:


SSOL
Niet beveiligd | info.ssol.local/
Info
Contact
Moodle
Secundary school of Limburg
Activate Windows
Go to Settings to activate Windows.

Welkom op de SSOL webpagina!

Welkom op de SSOL web pagina

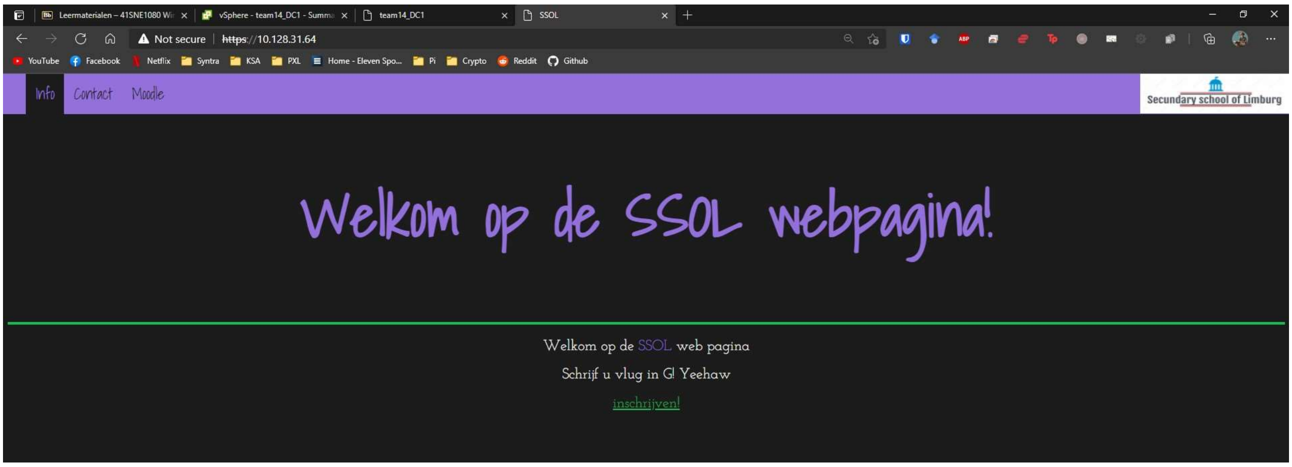
Schrijf u vlug in G! Yeehaw

inschrijven!

©Jonas vermeesen©

En als we op het pxl netwerk surfen naar het virtual IP adres dat we aangemaakt hebben in Pfsense

https://10.128.31.64



Welkom op de SSOL webpagina!

Welkom op de SSOL web pagina

Schrijf u vlug in G! Yeehaw

inschrijven!