2. CA

Introduction

Please ensure that you have already set up DNS.

**Objective:**

At the end of this guide, you will learn to setup OpenSSL CA which includes Root and SubCA.

**Login**

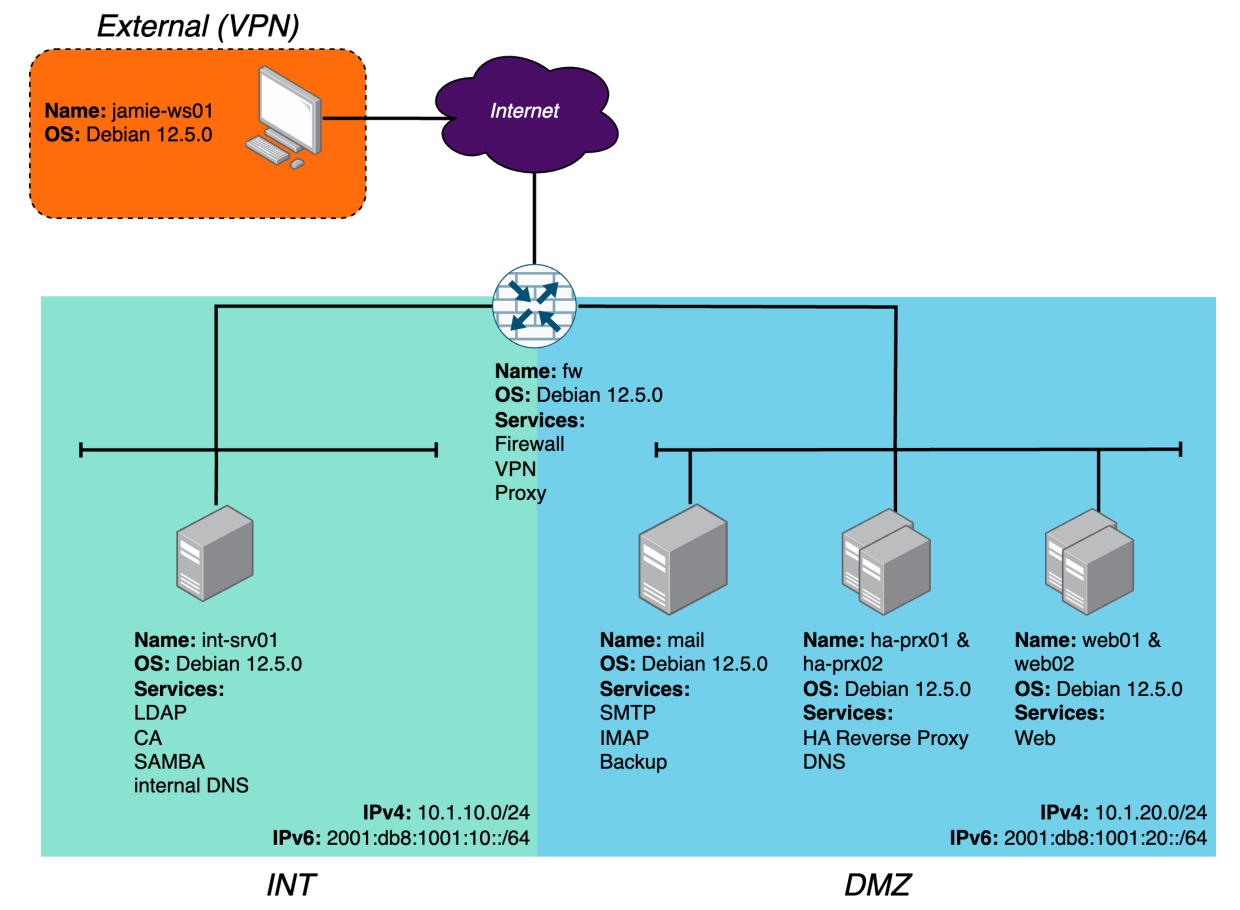
The login credential for all server and client machines:

Username: root / user

Password: Skill39@Lyon

**Network Topology**

This will be the network topology that will be referenced for setting up the infrastructure.



## Openssl CA

**Do the following on int-srv01**

cd /etc/ssl

mkdir CA

#openssl configuration file

vim openssl.cnf

|  |
| --- |

cd CA

mkdir certs crl newcerts private

touch index.txt

echo 1000 > serial

echo 1000 > crlnumber

#generating and signing cert

#RootCA cert

openssl genrsa -out private/ca.key 2048

openssl req -new -x509 -days 3650 -config .../openssl.cnf -extensions v3\_ca -key private/ca.key -out certs/ca.crt

Country: FR

Organization: ClearSky

Common Name: ClearSky Root CA

openssl ca -gencrl -config ../openssl.cnf -cert certs/ca.crt -keyfile private/ca.key -out crl/ca.crl.pem

openssl crl -inform PEM -in crl/ca.crl.pem -out crl/ca.crl -outform DER

#subca

openssl genrsa -out private/subca.key

openssl req -new -nodes -key private/subca.key -out mail.csr

openssl ca -config ../openssl.cnf -extensions v3\_intermediate\_ca -policy policy\_anything -in subca.csr -out certs/subca.crt

#generate cert for web and email

vim req.ext

[ req\_ext ]

subjectAltName=DNS:www.dmz.worldskills.org #change this accordingly

openssl genrsa -out private/web.key

openssl req -new -nodes -key private/web.key -out web.csr

openssl x509 -req -in web.csr -out certs/web.crt -CA certs/ca.crt -CAkey private/ca.key -CAcreateserial -sha256 -days 3650 -extensions req\_ext -extfile req.ext

vim req.ext

[ req\_ext ]

subjectAltName=DNS:mail.dmz.worldskills.org

openssl genrsa -out private/mail.key

openssl req -new -nodes -key private/mail.key

opensslx509 -req -in mail.csr -out certs certs/mail.crt -CA certs/ca.crt -CAkey private/ca.key -CAcreateserial -sha256 -days 3650 -extensions req\_ext -extfile req.ext

#cp the cert to /opt/grading/ca as required in the paper

mkdir -p /opt/grading/ca

cp certs/ca.crt /opt/grading/ca/campem

cp certs/mail.crt /opt/grading/ca/mail.pem

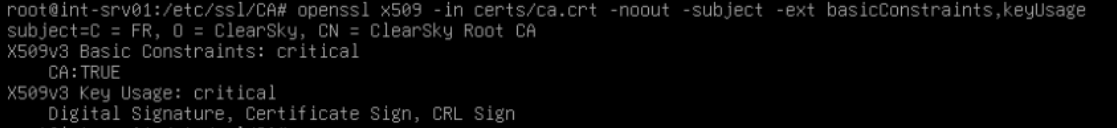
cp certs/web.crt /opt/grading/ca/web.pem

cp certs/subca.crt /opt/grading/ca/services.pem

Test

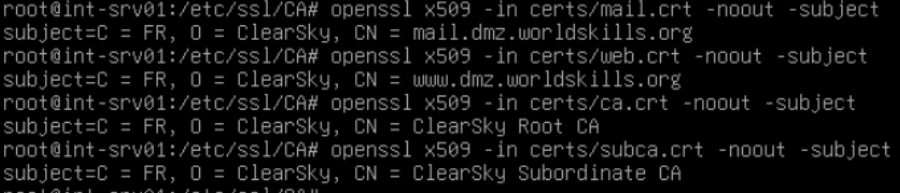
**Cert Subject and Attributes**

openssl x509 -in <file name> -noout -subject -ext basicConstraints,keyUsage



To check the CN of the cert

openssl x509 -in <cert> -noout -subject



**Certificate Validity**

1. Check if the SubCA cert is valid

openssl verify -CAfile certs/ca.crt certs/subca.crt



1. Check if the mail and web certs are valid

openssl verify -CAfile <(cat certs/subca.crt certs/ca.crt) <cert>

