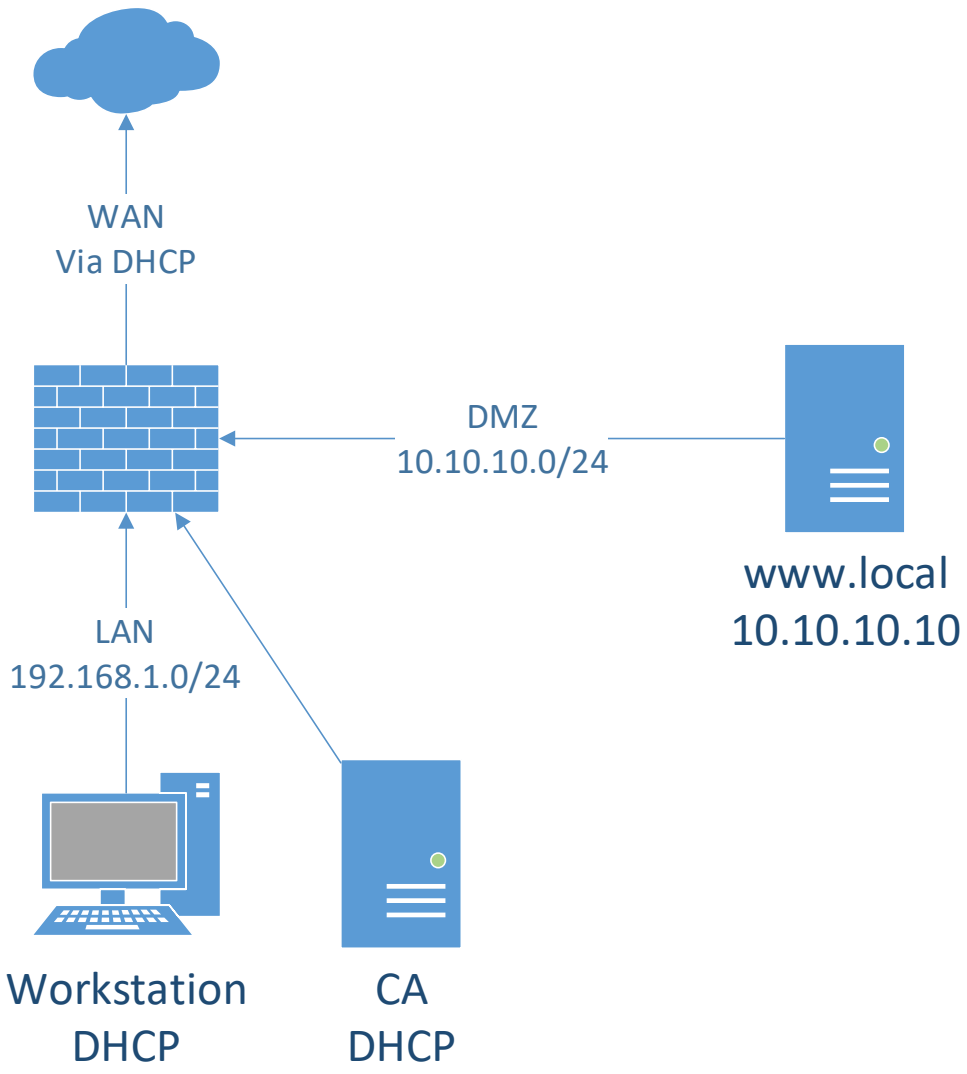
Lab2 – Certificates

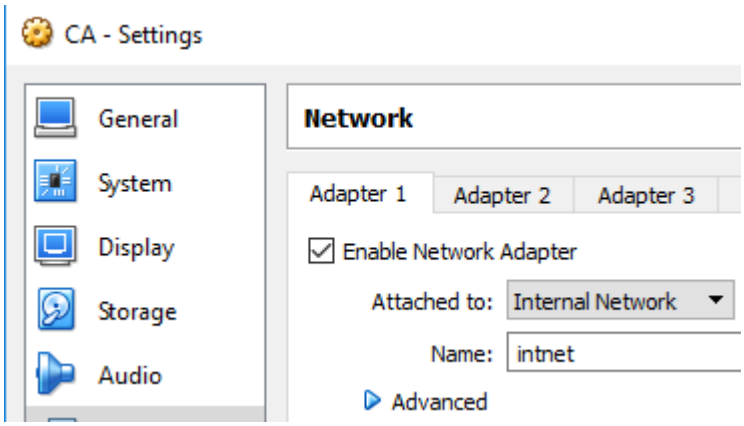
Document your commands or take screenshots. Answer questions in english or finnish. Replace your-student-id with your own student-id in the labs.

The labs use the following topology, some VMs are already installed in the previous labs:



- ## Install CA (1p)

Using the Centos7 tempalte from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\, clone another VM with the name CA. Remember to set "Reinitialize the MAC address…" tickbox in the import wizard. Set VM interface as *Internal network (intnet)*



Boot up the VMs shown in the topology and login to the new CA VM (**root/root66**). Check that it has got an IP.

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.102  netmask 255.255.255.0  broadcast 192.168.1.255
```

Download the *ca.cnf* and

usr.cnf files from http://student.labranet.jamk.fi/~jojuh/ttks/. You can use *wget* for this. (*wget <URL of the file>*)

```
[root@localhost ~]# wget http://student.labranet.jamk.fi/~jojuh/ttks/ca.cnf
```

First, lets create the CA:

```
openssl req -new -newkey rsa:4096 -keyout ca.key -config ca.cnf -
extensions v3_ca -x509 -out ca.pem
echo 01 > serial
touch index.txt
```

```
[root@localhost ~]# openssl req -new -newkey rsa:4096 -keyout ca.key -config ca.
cnf -extensions v3_ca -x509 -out ca.pem_
```

```
passphrase = root66
```

When asked for a passphrase for the key, use **root66**. Fill in the information, set CN (Common Name) as your-student-id-CA. Now check the contents of the CA certificate:

```
Country Name (C) [FI]:FI
Locality Name (L) [Default City]:JKL
Organization Name (O) [Default Company Ltd]:RommiOy
Organizational Unit Name (OU) []:Tupakki
Common Name (CN) []:K1521
Email Address []:aaaa@aaaa
```

```
openssl x509 -text -noout -in ca.pem
```

```
[root@localhost ~]# openssl x509 -text -noout -in ca.pem
```

```
Signature Algorithm: sha256WithRSAEncryption
     54:1a:b3:5d:5f:69:0c:d2:bf:63:e5:47:28:af:58:2d:35:cc:
     56:e4:5b:e8:d9:63:95:d9:47:3a:b0:09:58:5b:59:2c:81:73:
     06:99:e3:ad:a6:c0:25:36:de:03:88:b0:fa:aa:7e:33:36:c2:
     83:a0:52:9b:94:f2:77:8e:26:45:73:7f:92:93:ec:03:9d:29:
     0c:de:fe:1f:a9:0d:eb:54:7b:0a:3a:c4:a0:5d:42:66:c6:8e:
     27:36:1e:9e:42:5c:bd:29:6b:9b:2f:8e:ca:47:c3:4e:27:7c:
     d6:ca:d3:df:21:5b:f2:a4:d7:13:f1:99:a2:55:c9:d4:83:88:
     1d:0b:19:25:0b:3c:ab:26:e0:55:41:36:ba:22:81:aa:09:8e:
     07:f0:b8:66:b1:c3:70:3f:a4:d3:01:04:65:3d:03:43:26:5c:
     53:54:39:a5:77:1e:bc:d4:65:4b:d5:ba:3a:b3:d3:fe:9e:e5:
     f4:50:9c:76:28:a7:dd:77:2a:41:fd:4c:1f:c0:55:c8:33:8c:
     4a:42:34:d8:62:6e:75:ce:f4:8a:3f:5d:6d:1f:40:53:5a:23:
     ae:e1:2b:24:77:3f:92:ee:e7:de:53:c5:0f:71:3d:8e:e2:09:
     60:47:2a:7c:58:93:75:0c:da:d3:4e:cc:42:17:a9:3c:85:1b:
     44:ad:94:9a:92:79:65:5e:e3:f9:55:5e:c3:32:71:a5:b9:57:
     6c:04:37:c7:67:63:38:86:7f:aa:ac:41:a8:5f:b2:04:72:81:
     5b:16:d1:f5:b3:c4:1a:d2:78:5c:d0:34:17:92:19:34:66:14:
     81:b0:6e:a2:bc:41:88:b5:63:6d:f6:98:22:60:6a:49:77:27:
```

You should see the info you typed, public key is 4096bits and the most important part: CA:TRUE in Basic constraints. Without this, your CA cert will not be trusted by the clients.

- ## Creating a CSR (1p)

Boot up the Webserver VM. Create a new RSA key and CSR for the webserver. We will use the default openssl config. Set CN as www.your-student-id.com, other fields as you wish:

```
openssl req -new -newkey rsa:2048 -keyout www.key -nodes -out www.csr
```

Webserver [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
localhost login: root
Password:
Last login: Thu Jan 12 13:57:01 from 192.168.39.39
[root@localhost ~]#
[root@localhost ~]# openssl req -new -newkey rsa:2048 -keyout www.key -nodes -ou
t www.csr
Generating a 2048 bit RSA private key
.....................................................................
.............+++
.........+++
writing new private key to 'www.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FI
State or Province Name (full name) []:JKL
Locality Name (eg, city) [Default City]:JKL
Organization Name (eg, company) [Default Company Ltd]:RommiOY
Organizational Unit Name (eg, section) []:Tupakka
Common Name (eg, your name or your server's hostname) []:www.k1521.com_
```

On the CA VM, copy the csr from the webserver to the CA machine (you may have to create a firewall rule for TCP/22 in the PfSense VM):

Firewall / Rules / LAN

The settings have been applied. The firewall rules are now reloading in the background.
Monitor the reload progress.

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	1/75 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✔	0/0 B	IPv4 TCP	*	*	10.10.10.10	22 (SSH)	*	none			

```
scp root@10.10.10.10:www.csr ./
```

CA [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
[root@localhost ~]# scp root@10.10.10.10:www-csr ./
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
ECDSA key fingerprint is 7f:a5:01:31:4a:ab:76:66:3f:d9:74:86:b7:81:89:b6.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.10.10.10' (ECDSA) to the list of known hosts.
root@10.10.10.10's password: _
```

```
root@10.10.10.10's password:
www.csr                                       100% 1041     1.0KB/s   00:00
```

Check the contents of the CSR:

```
openssl req -noout -text -in www.csr
```

```
[root@localhost ~]# openssl req -noout -text -in www.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=FI, ST=JKL, L=JKL, O=RommiOY, OU=Tupakka, CN=www.k1521.com/em
ailAddress=dddd@dddd.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9a:81:5a:70:a1:12:33:e9:55:e6:14:4d:c2:97:
                    5f:e1:e8:61:89:69:ec:02:4d:4b:6c:c4:f7:3a:2a:
                    20:08:1f:1c:cf:14:9b:70:3c:d9:89:dd:1e:a9:a6:
                    9b:46:de:89:c0:d9:2e:14:12:ed:93:5b:b5:0f:65:
                    44:66:75:aa:c0:b9:17:93:26:ea:73:d6:a4:40:73:
                    77:8e:2f:e0:fc:2d:7b:c8:7a:ae:4b:1d:2d:b3:4e:
                    95:2a:39:8c:5a:db:6f:ea:8e:71:2d:7d:9b:58:12:
                    58:3d:c9:96:ba:70:92:03:38:f9:0c:8b:36:b1:b2:
                    f9:88:95:26:11:3c:52:cf:ce:d1:fc:c0:15:fd:4a:
                    6e:78:64:9b:67:d3:8e:8f:e3:16:0b:c7:b8:84:8c:
                    c3:df:d3:53:c6:da:58:40:4a:bf:0a:11:23:4b:8b:
                    08:1b:ec:84:36:7e:c0:9e:20:f2:45:b9:54:ba:38:
                    66:1f:bd:87:d8:80:e0:bf:a9:67:7b:60:ca:3b:98:
                    24:d8:13:fd:88:f9:97:8d:32:b9:8f:f9:61:89:ea:
```

If everything seems to be right, sign the CSR with the CA key:

```
openssl ca -config usr.cnf -extensions usr_crt -days 365 -keyfile ca.key
-cert ca.pem -in www.csr -out www.pem
```

CA [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
-rw-r--r--. 1 root root    0 Jan 19 13:17 www.pem
[root@localhost ~]# rm usr.cnf.1
rm: remove regular file 'usr.cnf.1'? Y
[root@localhost ~]# openssl ca -config usr.cnf -extensions usr_cert -days 365 -k
eyfile ca.key -cert ca.pem -in www.csr -out www.pem
Using configuration from usr.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jan 19 11:37:52 2017 GMT
            Not After : Jan 19 11:37:52 2018 GMT
        Subject:
            countryName               = FI
            stateOrProvinceName       = JKL
            localityName              = JKL
            organizationName          = RommiOY
            organizationalUnitName    = Tupakka
            commonName                = www.k1521.com
            emailAddress              = dddd@dddd.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

Before answering yes, take time to check that the certificate info is correct. Especially check that Basic Constraints has CA:FALSE as we do not want our webserver to be a CA. Also X509v3 Key Usage should have Digital Signature, Non Repudiation and Key Encipherment.

Examine the contents of the new CRT file:

```
openssl x509 -nout -text -in www.pem
```

```
[root@localhost ~]# openssl x509 -noout -text -in www.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FI, L=JKL, O=RommiOy, OU=Tupakki, CN=K1521/emailAddress=aaaa@a
aaa
        Validity
            Not Before: Jan 19 11:37:52 2017 GMT
            Not After : Jan 19 11:37:52 2018 GMT
        Subject: C=FI, ST=JKL, L=JKL, O=RommiOY, OU=Tupakka, CN=www.k1521.com/em
ailAddress=dddd@dddd.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9a:81:5a:70:a1:12:33:e9:55:e6:14:4d:c2:97:
                    5f:e1:e8:61:89:69:ec:02:4d:4b:6c:c4:f7:3a:2a:
                    20:08:1f:1c:cf:14:9b:70:3c:d9:89:dd:1e:a9:a6:
```

And finally, copy it back to the Webserver VM:

```
scp www.pem root@10.10.10.10:www.pem
```

```
[root@localhost ~]# scp www.pem root@10.10.10.10:www.pem
root@10.10.10.10's password: _
```

- **Configure SSL (1p)**

In the Webserver, you have to do two things. First, install mod_ssl to Apache:

```
yum install mod_ssl
```

```
[root@localhost ~]# yum install mod_ssl -y_
```

Then copy the key and certificate to the correct paths:

```
cp www.key /etc/pki/tls/private/
cp www.pem /etc/pki/tls/certs/
```

```
[root@localhost ~]# cp www.key /etc/pki/tls/private/
[root@localhost ~]# cp www.pem /etc/pki/tls/certs/
```

In those folders should exist also a default self-signed certificate (localhost.key and localhost.crt). Check their permissions and set the same permissions to the www.key and www.pem.

```
[root@localhost private]# ls -lah
total 8.0K
drwxr-xr-x. 2 root root   40 Jan 19 13:43 .
drwxr-xr-x. 5 root root   76 Oct  5  2015 ..
-rw-------. 1 root root 1.7K Jan 19 13:42 localhost.key
-rw-r--r--. 1 root root 1.7K Jan 19 13:43 www.key
[root@localhost private]# chmod 600 www.key
```

```
[root@localhost certs]# ls -lah
total 28K
drwxr-xr-x. 2 root root 4.0K Jan 19 13:44 .
drwxr-xr-x. 5 root root   76 Oct  5  2015 ..
lrwxrwxrwx. 1 root root   49 Oct  5  2015 ca-bundle.crt -> /
racted/pem/tls-ca-bundle.pem
lrwxrwxrwx. 1 root root   55 Oct  5  2015 ca-bundle.trust.cr
st/extracted/openssl/ca-bundle.trust.crt
-rw-------. 1 root root 1.5K Jan 19 13:42 localhost.crt
-rwxr-xr-x. 1 root root  610 Mar  6  2015 make-dummy-cert
-rw-r--r--. 1 root root 2.4K Mar  6  2015 Makefile
-rwxr-xr-x. 1 root root  829 Mar  6  2015 renew-dummy-cert
-rw-r--r--. 1 root root 5.8K Jan 19 13:44 www.pem
[root@localhost certs]# chmod 600 www.pem
```

Last thing you need to do is edit /etc/httpd/conf.d/ssl.conf and change Apache to use your certificates. Find the following lines:

```
SSLCertificateFile=…
SSLCertificateKeyFile=…
```

```
  GNU nano 2.3.1        File: /etc/httpd/conf.d/ssl.conf                Modified

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/www.pem

#   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.)
SSLCertificateKeyFile /etc/pki/tls/private/www.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
```

And set them to point to your files. Reload apache (systemctl restart httpd).

```
[root@localhost certs]# firewall-cmd --add-service=https --permanent
success
[root@localhost certs]# firewall-cmd --reload
success
```

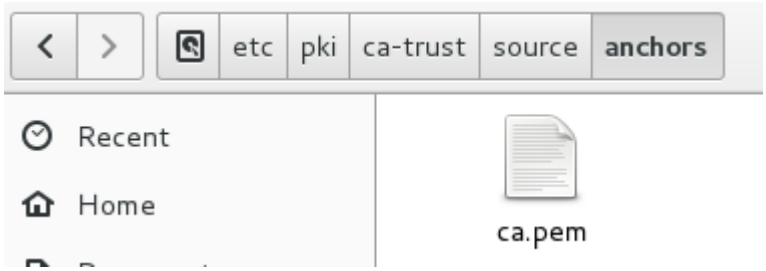
- **Trusted root (1p)**

Your Workstation VM needs to trust to your CA certificate or it will alert you about the server. Fetch the ca.pem from the CA VM to your Workstation VM using SSH (scp root@a.b.c.d:ca.pem ca.pem). There are several places where the ca.pem needs to be put

~~In a Windows-based PC, you can add the certificate to trusted roots in MMC console.~~ We don't currently use Windows in this lab.

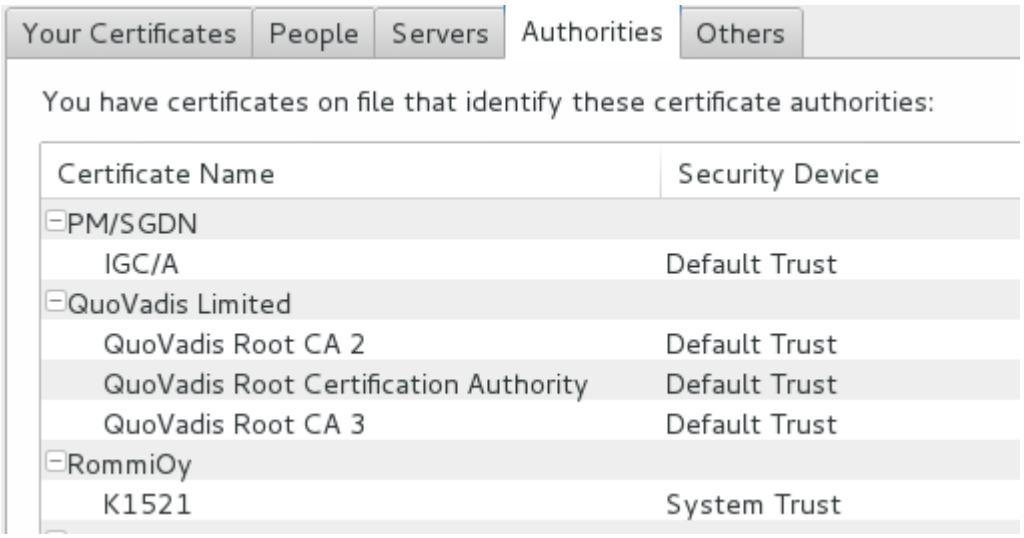
```
[root@localhost ~]# scp root@192.168.1.102:ca.pem ca.pem
The authenticity of host '192.168.1.102 (192.168.1.102)' can't be established.
ECDSA key fingerprint is 0a:fd:37:4a:64:07:48:ee:e2:23:0c:25:57:0d:e1:cc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.102' (ECDSA) to the list of known hosts.
root@192.168.1.102's password:
ca.pem                                        100% 2021     2.0KB/s   00:00
[root@localhost ~]#
```

In Centos7, put the certificate file in /etc/pki/ca-trust/source/anchors/ and run sudo update-ca trust. This will add the certificate as a trusted root.




```
[root@localhost ~]# update-ca-trust
[root@localhost ~]#
```

Alas, Firefox does not use the system certificates and you need to add the CA there also. Open Firefox, select Options -> Advanced -> Certificates -> View Certificates. Select the Authorities tab, Click Import and select ca.pem-file.



- **DNS name and testing (1p)**

Final step is to add a DNS name for the webserver. The certificate is written only for the webserver name, not the IP address, so even if you try to access the webserver now, you will get an error.

Go to Pfsense management, and find DNS Forwarder settings. Add a Host override. Set host name as www, domain name as your-student-id.com and point the IP address to your webserver. Now you should be able to resolve host www.your-student-id.com from your Workstation. You can test this with nslookup.

Host Overrides

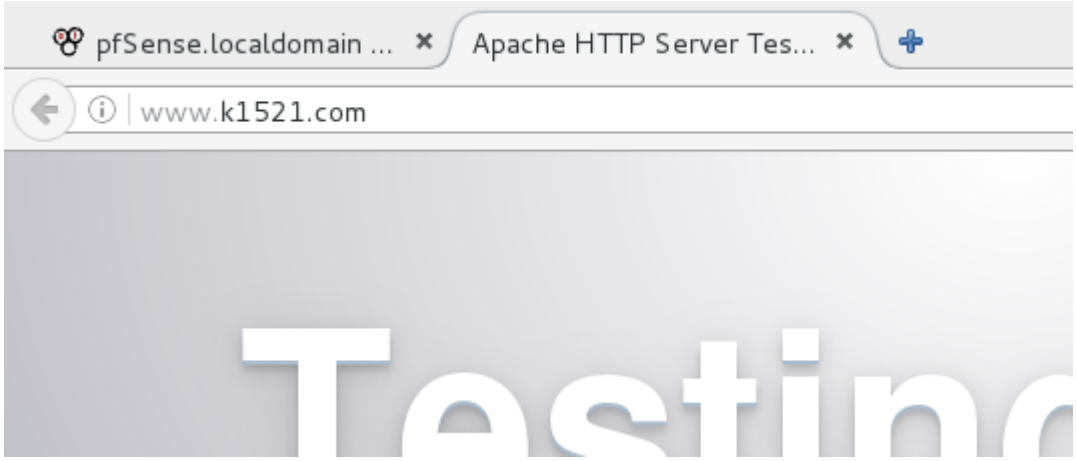
Host	Domain	IP	Description	Actions
www	k1521.com	10.10.10.10	webserver	

Add

Try to browse to your webserver with the name from the Workstation. If you get no warning, everything works. If you get warning, check configuration, Firefox certificates, etc.

```
[root@localhost ~]# nslookup www.k1521.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   www.k1521.com
Address: 10.10.10.10
```



Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	1/1.08 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✔	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			

When you are finished, take a screenshot of the Certificate Hierarchy path (shown in View Certificate - Details)

General | Details

This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate
- Email Signer Certificate
- Email Recipient Certificate
- Object Signer

Issued To

Common Name (CN)	www.k1521.com
Organization (O)	RommiOY
Organizational Unit (OU)	Tupakka
Serial Number	01

Issued By

Common Name (CN)	K1521
Organization (O)	RommiOy
Organizational Unit (OU)	Tupakki

Period of Validity

Begins On	01/19/2017
Expires On	01/19/2018

Fingerprints

SHA-256 Fingerprint	8F:47:3D:DC:4D:30:FA:5D:91:A0:F5:1A:A7:B1:45:98: C3:E3:8B:51:B7:D4:13:4A:1D:B4:AB:94:BF:2E:68:47
SHA1 Fingerprint	BB:13:51:D3:0A:C0:BF:23:46:07:95:32:8B:F2:6C:7B:95:64:EA:87

BONUS: If you have time, try to find out how to add another hostname or IP address to subjectAltNames of the certificate.