1. Скопировать содержимое файла openssl.cnf, сохранить под таким же именем на ПК.

https://jamielinux.com/docs/openssl-certificate-authority/appendix/intermediate-configuration-file.html

Intermediate CA configuration file

View this file as plain text.

```
# OpenSSL intermediate CA configuration file.
# Copy to `/root/ca/intermediate/openssl.cnf`.

[ ca ]
# `man ca`
default_ca = CA_default

[ CA_default ]
# Directory and file locations.
dir               = /root/ca/intermediate
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand

# The root key and root certificate.
private_key       = $dir/private/intermediate.key.pem
certificate       = $dir/certs/intermediate.cert.pem

# For certificate revocation lists.
crlnumber         = $dir/crlnumber
crl               = $dir/crl/intermediate.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30

# SHA-1 is deprecated, so use SHA-2 instead.
default_md        = sha256
```

2. Добавить следующие строки в раздел [v3_intermediate_ca]:

subjectAltName = @alt_names

[alt_names]
DNS.1 = iwtm.demo.lab

3. Передать файл на IWTM

```
C:\Users\Администратор\Desktop>cd C:\

C:\>scp openssl.cnf root@172.16.6.3:/root/
root@172.16.6.3's password:
openssl.cnf                                   100%   12KB 264.3KB/s   00:00

C:\>
```

4. Подготовить каталог для сертификатов

```
[root@iwtm ~]# mkdir /ca
[root@iwtm ~]# mv openssl.cnf /ca/
[root@iwtm ~]# cd /ca/
[root@iwtm ca]# ls
openssl.cnf
[root@iwtm ca]# _
```

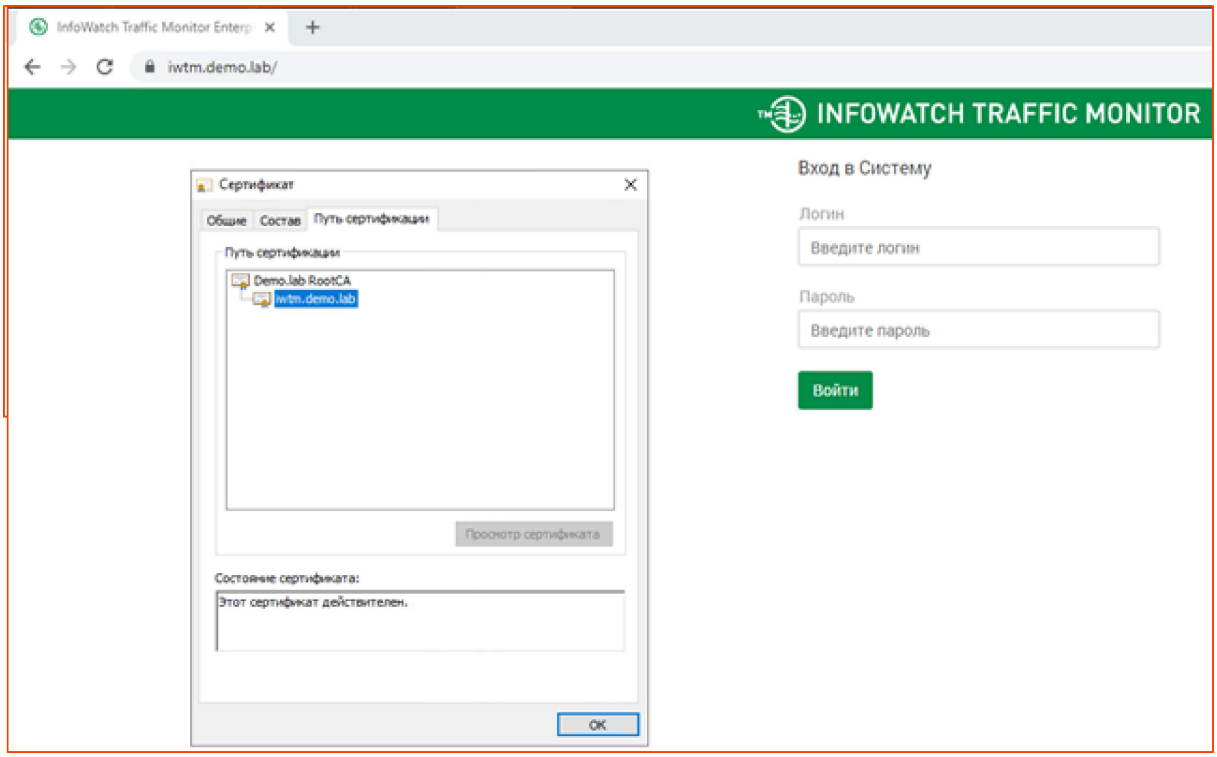
5.Написать скрипт следующего содержания:

```
#!/bin/bash
openssl req -x509 -newkey rsa:4096 -passout pass:"QWEasd123" -days 3650 -subj
"/C=RU/ST=Tomsk/L=Tomsk/O=Demo.lab/CN=Demo.lab RootCA" -config openssl.cnf -
extensions v3_ca -keyout rootca.key -out rootca.crt
openssl req -newkey rsa:4096 -passout pass:"QWEasd123" -subj
"/C=RU/ST=Tomsk/L=Tomsk/O=Demo.lab/CN=iwtm.demo.lab" -config openssl.cnf -keyout
server.key -out server.csr
openssl x509 -req -passin pass:"QWEasd123" -in server.csr -CA rootca.crt -CAkey rootca.key -
CAcreateserial -days 365 -extfile openssl.cnf -extensions v3_intermediate_ca -out server.crt
openssl req -newkey rsa:4096 -passout pass:"QWEasd123" -subj
"/C=RU/ST=Tomsk/L=Tomsk/O=Demo.lab/CN=demolab" -config openssl.cnf -keyout client.key -
out client.csr
openssl x509 -req -passin pass:"QWEasd123" -in client.csr -CA server.crt -CAkey server.key -
CAcreateserial -days 365 -extfile openssl.cnf -extensions usr_cert -out client.crt

cat client.crt server.crt rootca.crt > certs.crt

openssl pkcs12 -export -passin pass:"QWEasd123" -passout pass:"QWEasd123" -in certs.crt -inkey
```

6. Выполнить скрипт:
7. Изменить строчки в конфиге /etc/nginx/conf.d/iwtm.conf:

```
ssl_certificate     /ca/server.crt;
ssl_certificate_key /ca/server.key;
ssl_verify_client on;
ssl_verify_depth 2;
ssl_password_file /ca/cert.pass;
ssl_client_certificate /ca/rootca.crt;
```

8. Создать файл «cert.pass» с паролем.
9. Перезапустить nginx.
10. Передать bundle.p12 на домен demo.lab и импортировать сертификаты в хранилище.
11. Запустить Google Chrome и проверить работоспособность:


InfoWatch Traffic Monitor Enterp
iwtm.demo.lab/
INFOWATCH TRAFFIC MONITOR
Сертификат
Общие
Состав
Путь сертификации
Путь сертификации
Demo.lab RootCA
wtm.demo.lab
Просмотр сертификата
Состояние сертификата:
Этот сертификат действителен.
OK
Вход в Систему
Логин
Введите логин
Пароль
Введите пароль
Войти