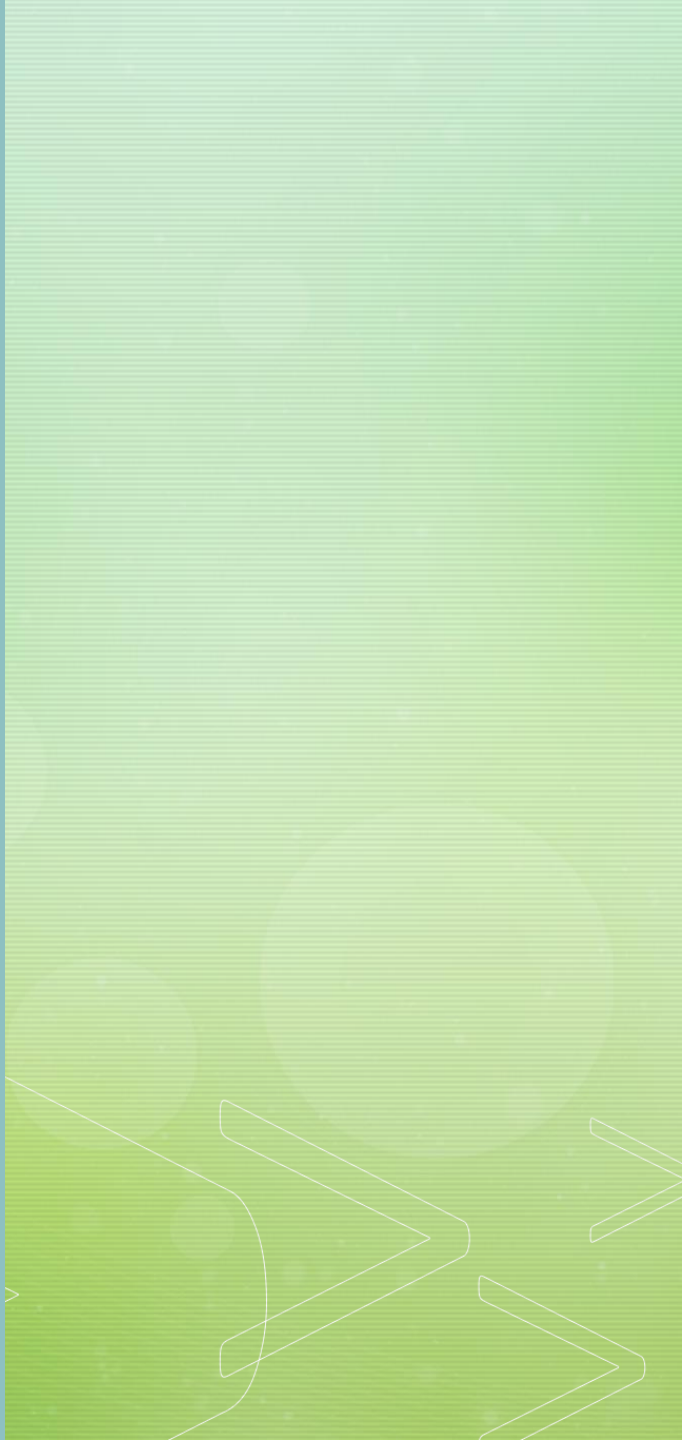




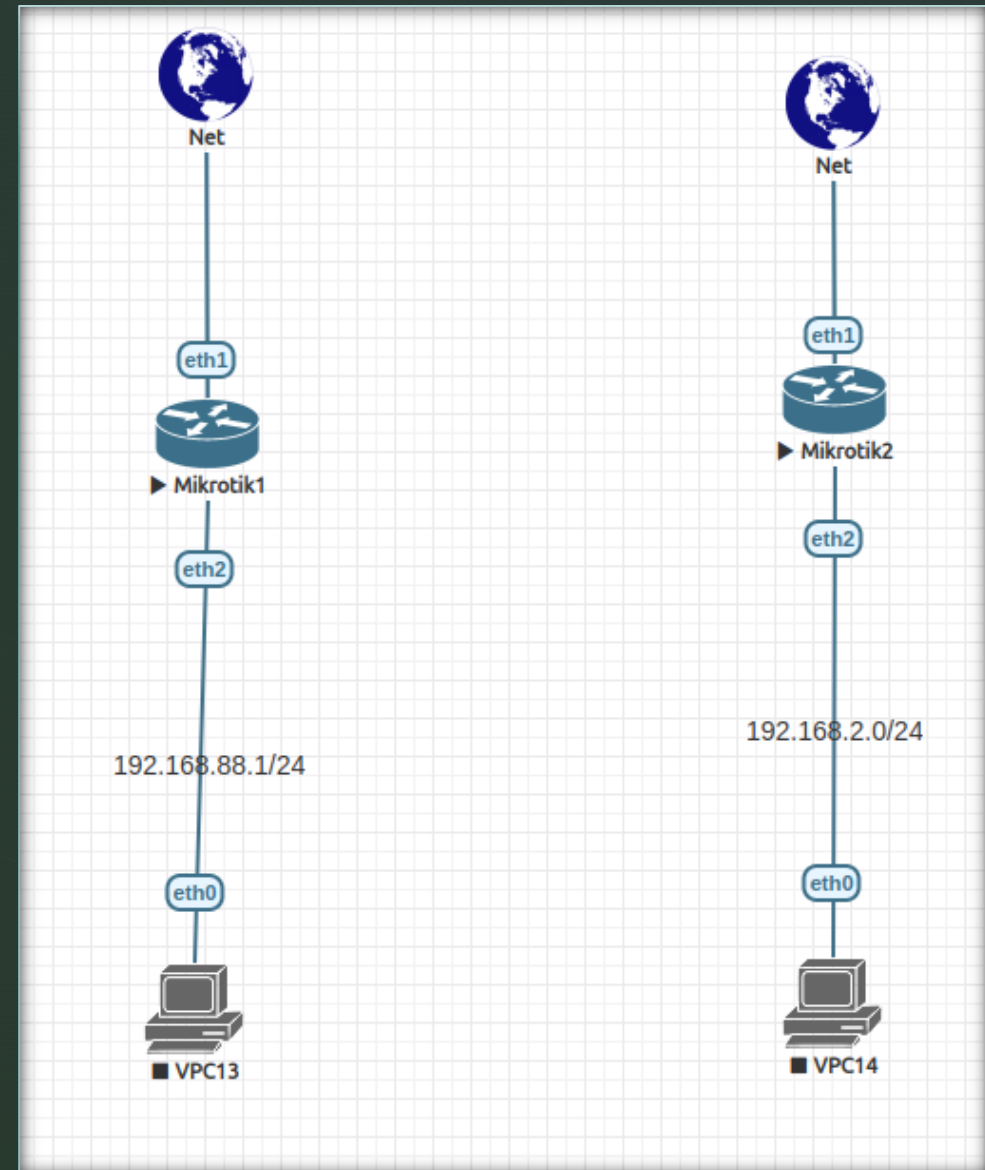
Laboratoare Retelistica

Configurarea protocolului SSTP



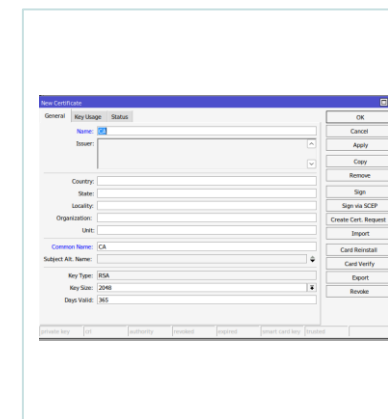
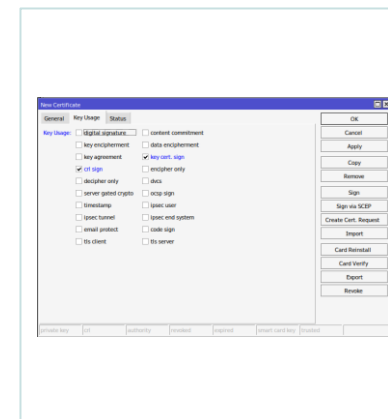
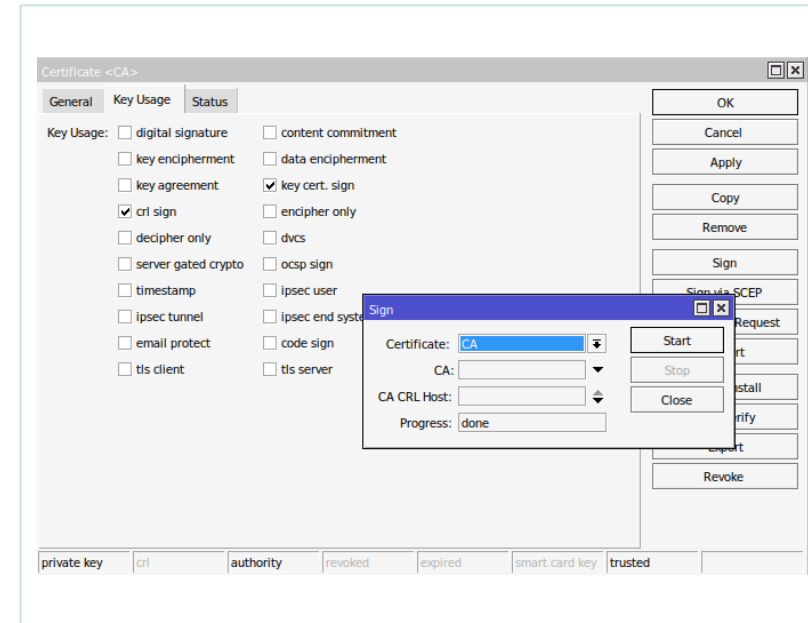
Topologie

- Incepem de la o topologie cu doua zone.
- Pentru a putea autentifica mai facil clientii in acest protocol am decis sa implementez si un server de SCEP (Simple Certificate Enrollment Protocol) care sa semneze certificatele clientilor remote.

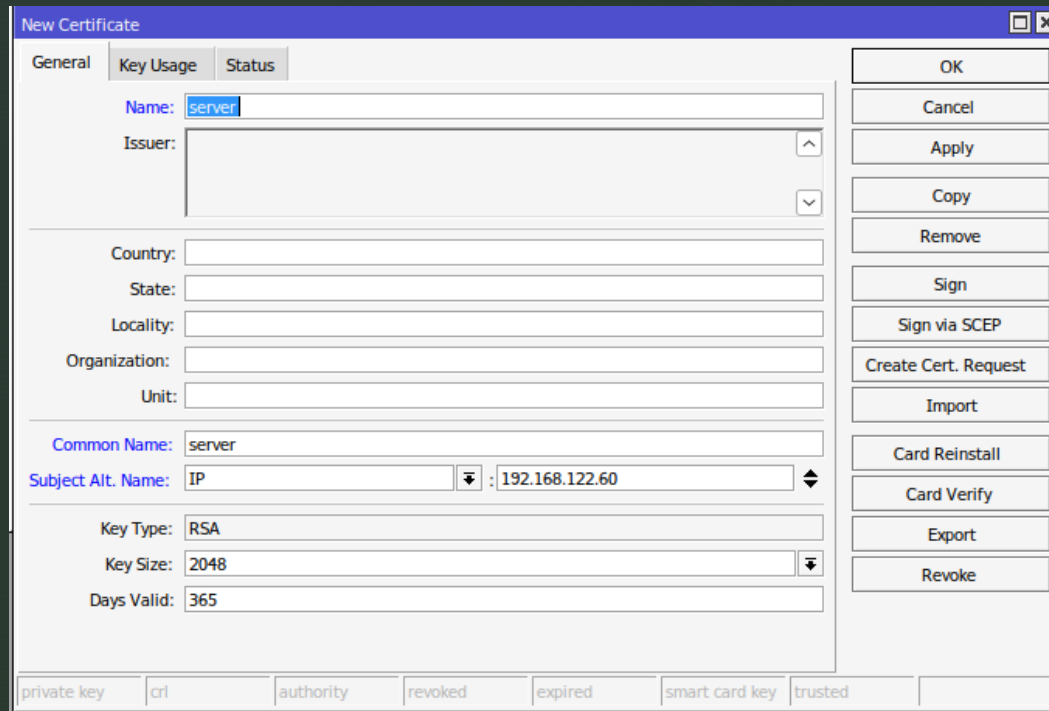
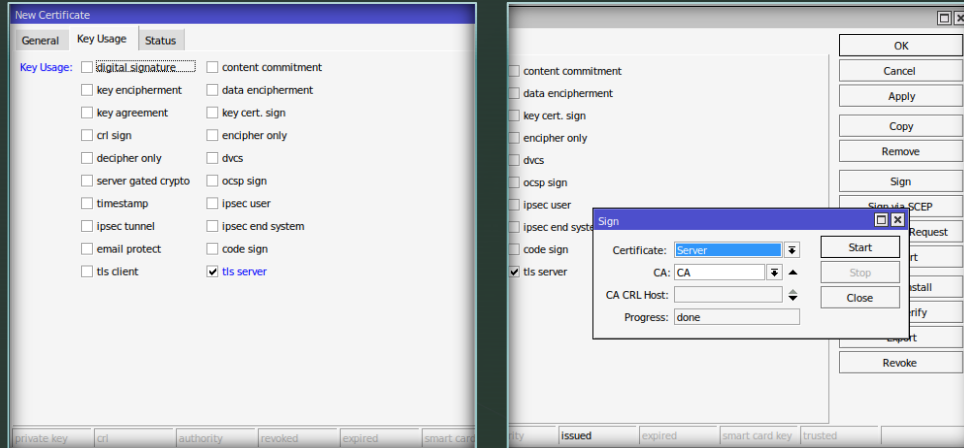


Setarea CA-ului si certificatului pentru server

- Incepem sa facem
certificatul CA mergand in
System->Certificates si
adaugam un certificat nou cu
optiunile de "ctl sign" si "key
cert. Sing".
- Dupa ce il salvam il semnam
si la status o sa vedem ca
apare ca authority si trusted.



Setarea CA-ului si certificatului pentru server



- Dupa care putem face certificatul de Server pe care il semnam cu CA-ul facut mai devreme.

Setarea de baza a serverului SSTP

- In meniul IP->Pools facem un nou pool pentru clientii de vpn.
- Mergem in PPP->Profiles si facem un nou profil.
- Dupa care facem un cont pentru primul client mergand in PPP->Secrets

Pool <sstp-pool>

Name: sstp-pool

Addresses: 0.10.1-10.10.10.254

Next Pool: none

OK

Cancel

Apply

Comment

Copy

Remove

New PPP Profile

General

Name: sstp-profile

Local Address: 10.10.10.1

Remote Address: sstp-pool

Remote IPv6 Prefix Pool:

DHCPv6 PD Pool:

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Bridge Learning: default

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

Change TCP MSS:

no yes default

Use UPnP:

no yes default

OK

Cancel

Apply

Comment

Copy

Remove

New PPP Secret

Name: sstp

Password: test123

Service: sstp

Caller ID:

Profile: sstp-profile

Local Address:

Remote Address:

Remote IPv6 Prefix:

Routes:

IPv6 Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

Last Caller ID:

Last Disconnect Reason:

enabled

OK

Cancel

Apply

Disable

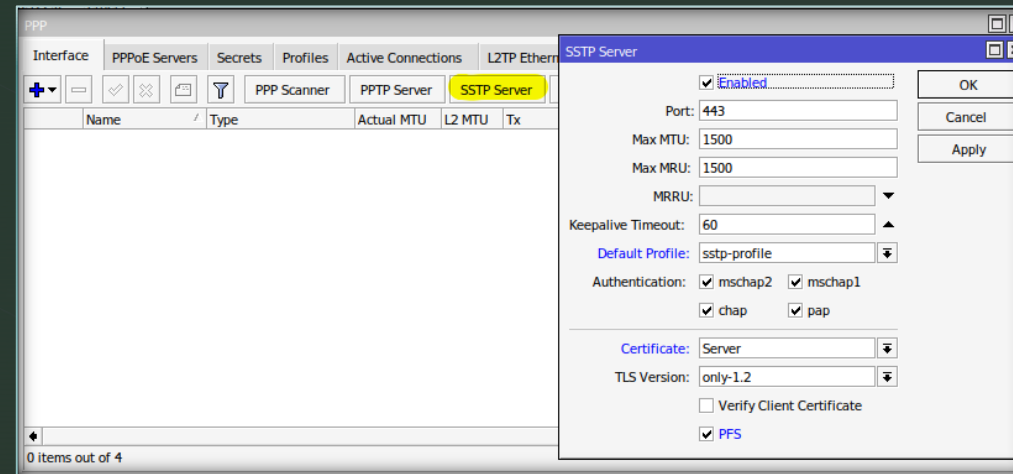
Comment

Copy

Remove

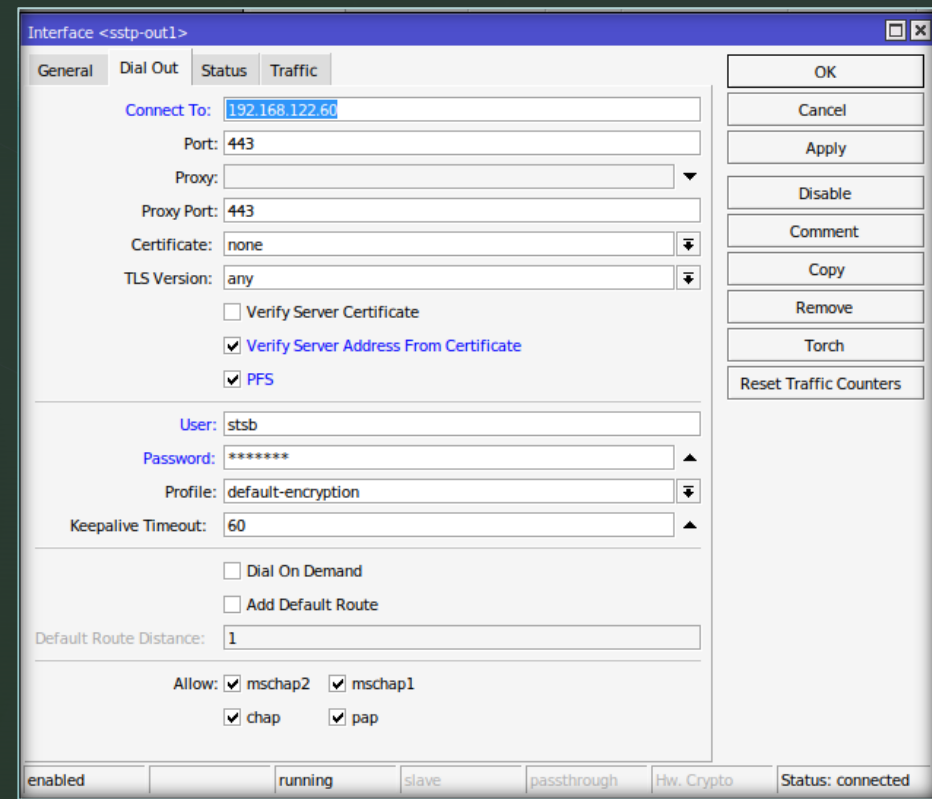
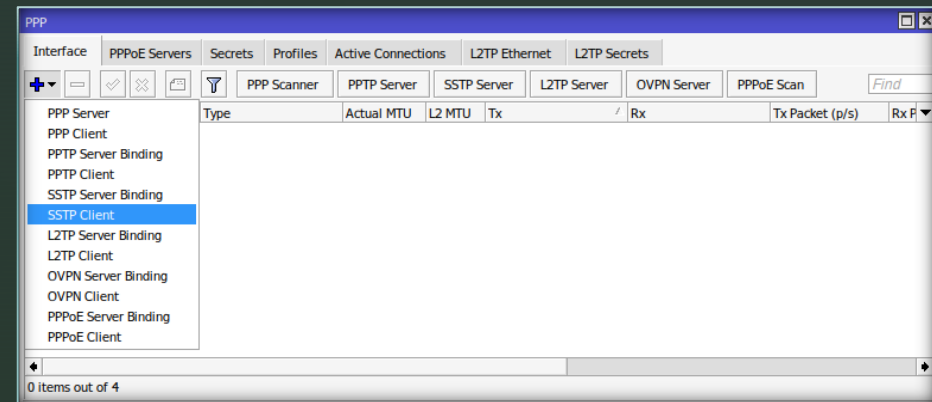
Setarea de baza a serverului SSTP

- Dupa ce am facut aceasta configuratie de baza putem activa si configura serverul mergand in PPP->Interface->SSTP Server



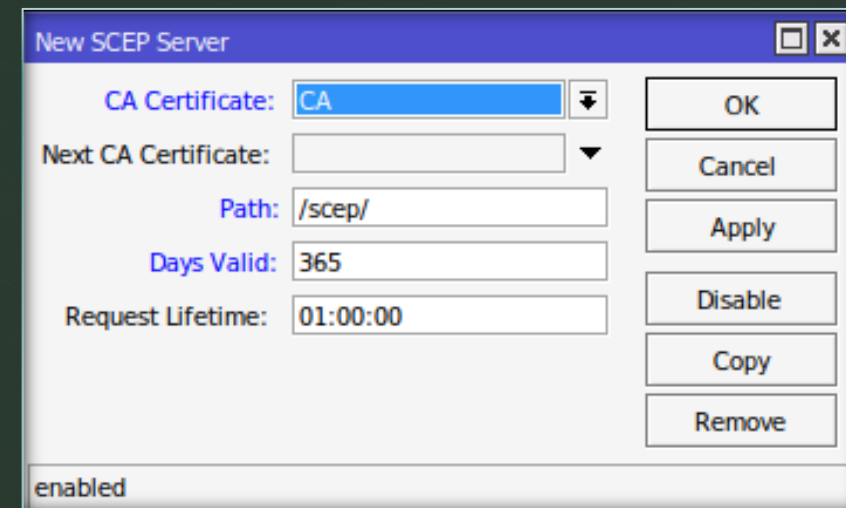
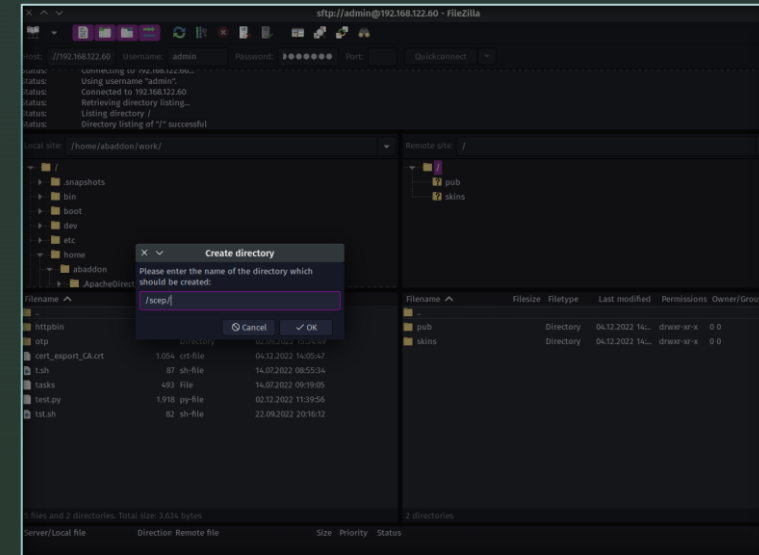
Setarea Clientului MikroTik

- Pe al doilea router intram in PPP->Interface->"+"-> SSTP Client.
- Putem vedea ca este conectat si running.
- Si acesti pasi ar fi suficienti pentru o conexiune de baza intre doua routere mikrotik. Dar nu putem verifica certificatul de server si nici pe cel de client.



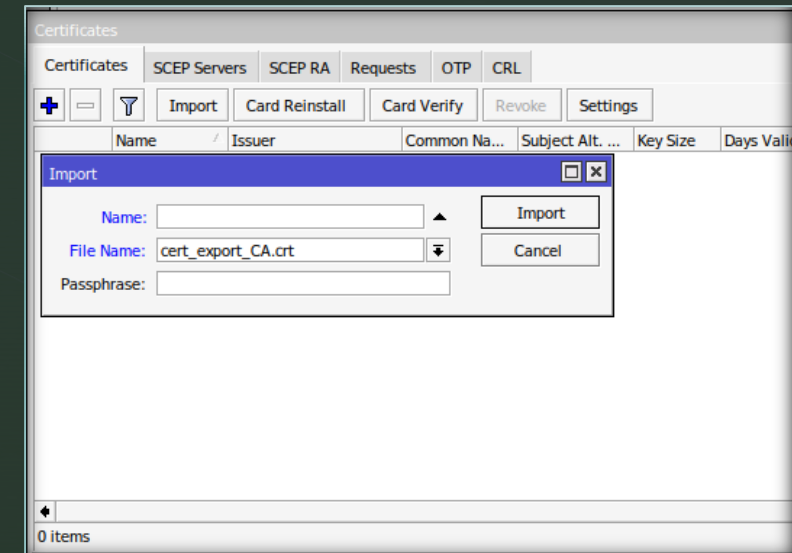
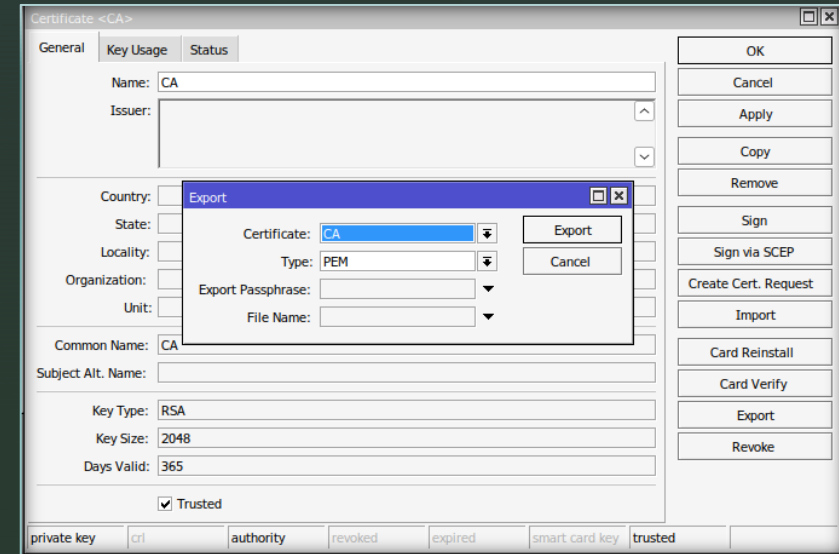
Configurarea serverului SCEP

- Inainte de a incepe configurarea trebuie sa ne conectam la router prin ftp sau sftp si sa facem un folder `"/scep/"`
- Dupa care in System->Certificates->SCEP Servers adaugam un nou server.



Exportarea CA-ului din routerul 1 in routerul 2

- Mergand in System->Certificates, deschidem CA-ul si ii dam export.
- Dupa care il copiem pe calculator apoi pe routerul 2 si il importam.
- In System->Certificates-> Import.



Activarea verificarii certificatului pe routerul 2

- Acum vom merge unde am configurat clientul si bifam "Verify Server Certificate"
- Resetam conexiunea si verificam reautentificarea.

Interface <ssstp-out1>

General Dial Out Status Traffic

Connect To: 192.168.122.60

Port: 443

Proxy:

Proxy Port: 443

Certificate: none

TLS Version: any

☒ Verify Server Certificate

☒ Verify Server Address From Certificate

☒ PFS

User: stsb

Password: *****

Profile: default-encryption

Keepalive Timeout: 60

☐ Dial On Demand

☐ Add Default Route

Default Route Distance: 1

Allow: ☒ mschap2 ☒ mschap1

☒ chap ☒ pap

OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters

enabled running slave passthrough No Crypto Status: connected

Interface <ssstp-out1>

General Dial Out Status Traffic

Last Link Down Time: Dec/04/2022 13:36:00

Last Link Up Time: Dec/04/2022 13:36:18

Link Downs: 3

Uptime: 00:03:48

Encoding: AES256-CBC

MTU: 1500

MRU: 1500

Local Address: 10.10.10.254

Remote Address: 10.10.10.1

Local IPv6 Address: fe80::6

Remote IPv6 Address: fe80::f0:3

OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters

enabled running slave passthrough No Crypto Status: connected

Crearea certificatului de client si semnarea lui remote.

- Pe routerul 1 intram la System->Certificates->Requests si trebuie sa vedem o cerere de semnare a certificatului.

The screenshot displays a web-based interface for managing certificates. The 'Requests' tab is active, showing a table with one entry: a pending request from authority 'CA' created on Dec/04/2022 13:44:10. The request fingerprint is 'cce9f146876c20e9e6927d70d24d999347f25a84422dc96bd32735e83159afef' and the common name is 'cert-site-b'. A modal window is open for this request, showing fields for Authority (CA), Created (Dec/04/2022 13:44:10), Transaction ID, Req. Fingerprint, Country, State, Locality, Organization, Unit, Common Name (cert-site-b), Serial Number, and Email. 'OK' and 'Grant' buttons are visible on the right.

Authority	Status	Created	Req. Fingerprint	Common Name
CA	pending	Dec/04/2022 13:44:10	cce9f146876c20e9e...	cert-site-b

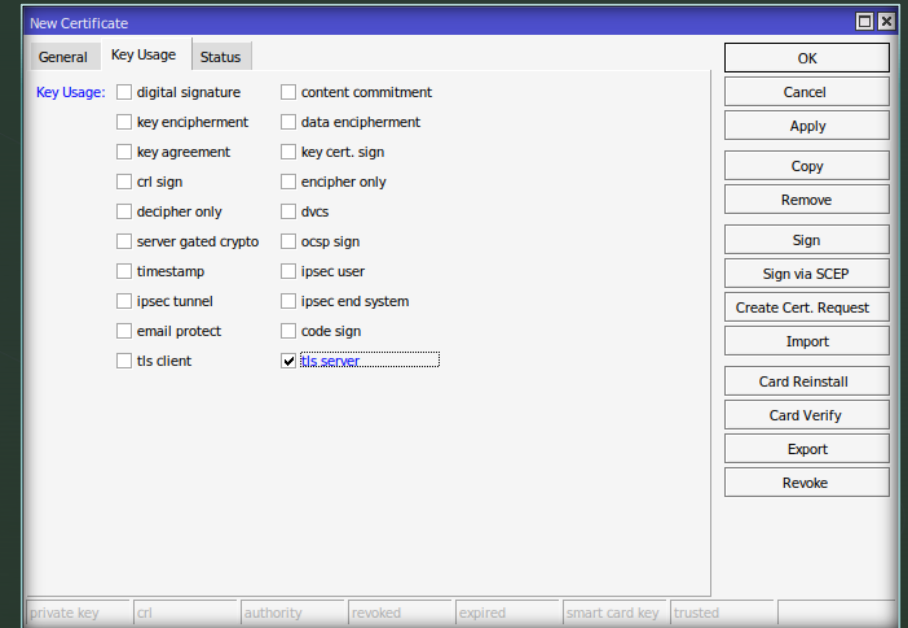
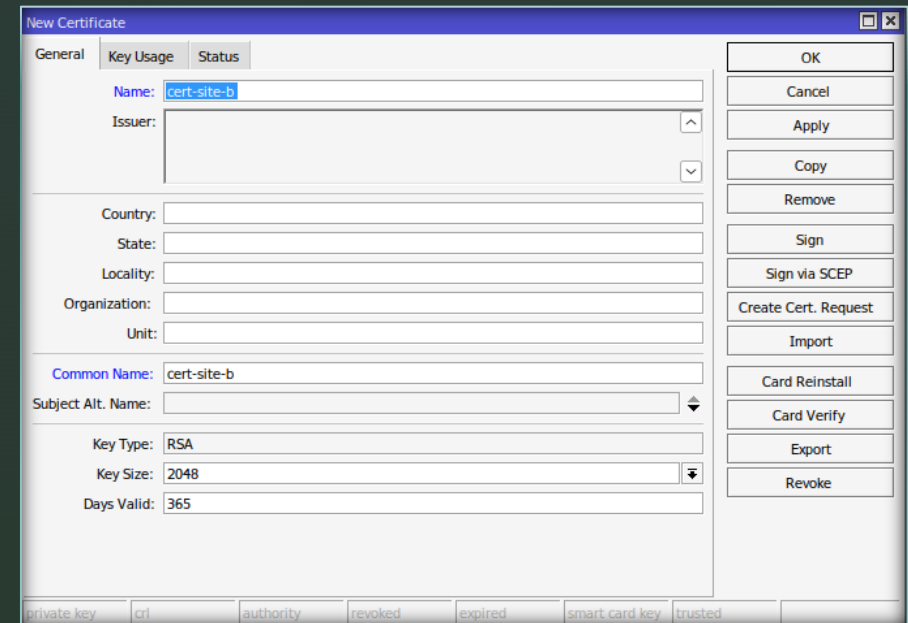
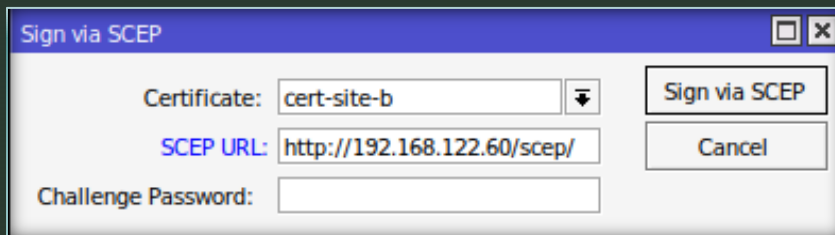
SCEP Request <cce9f146876c20e9e6927d70d24d999347f25a84422dc96bd32735e83159afef>

Authority: CA
Created: Dec/04/2022 13:44:10
Transaction ID:
Req. Fingerprint: cce9f146876c20e9e6927d70d24d999347f25a84422dc96bd32735e83159afef
Country:
State:
Locality:
Organization:
Unit:
Common Name: cert-site-b
Serial Number:
Email:

1 item (1 selected) Status: pending

Crearea certificatului de client si semnarea lui remote.

- Facem un nou certificat pe routerul 2
- Dupa ce il salvam apasam buntoul Sign via SCEP.



Verificarea certificatului de client de catre server.

- Intram pe routerul 1 unde este serverul si activam "Verify Client Certificate"
- Iar pe client selectam in client ul de SSTP certificaul facut.
- Dupa care resetam conexiunea si verificam conectivitatea.

The screenshot shows the 'SSTP Server' configuration window. The 'Enabled' checkbox is checked. The 'Port' is set to 443, 'Max MTU' is 1500, and 'Max MRU' is 1500. The 'MRRU' is set to a default value. The 'Keepalive Timeout' is 60. The 'Default Profile' is 'sstp-profile'. Under 'Authentication', 'mschap2', 'mschap1', 'chap', and 'pap' are all checked. The 'Certificate' is set to 'server2' and 'TLS Version' is 'only-1.2'. The 'Verify Client Certificate' checkbox is checked, and the 'PFS' checkbox is also checked. Buttons for 'OK', 'Cancel', and 'Apply' are on the right.

The screenshot shows the 'Interface <sstp-out1>' configuration window. The 'General' tab is selected. 'Connect To' is '192.168.122.60', 'Port' is 443, and 'Proxy Port' is 443. The 'Certificate' is 'cert-site-b' and 'TLS Version' is 'any'. The 'Verify Server Certificate', 'Verify Server Address From Certificate', and 'PFS' checkboxes are checked. The 'User' is 'stsb' and the 'Profile' is 'default-encryption'. The 'Keepalive Timeout' is 60. There are checkboxes for 'Dial On Demand' and 'Add Default Route'. The 'Default Route Distance' is 1. Under 'Allow', 'mschap2', 'mschap1', 'chap', and 'pap' are all checked. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Torch', and 'Reset Traffic Counters' are on the right. At the bottom, there are status indicators: 'enabled', 'running', 'slave', 'passthrough', 'Hw. Crypto', and 'Status: connected'.

Testare

```
VPC13
Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: May 7 2022 15:27:29
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

VPCS> dhcp
DORA IP 192.168.1.254/24 GW 192.168.1.1

VPCS> ping 192.168.2.254

84 bytes from 192.168.2.254 icmp_seq=1 ttl=62 time=1.935 ms
84 bytes from 192.168.2.254 icmp_seq=2 ttl=62 time=1.855 ms
^C
VPCS> █

VPC14
Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: May 7 2022 15:27:29
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

VPCS> dhcp
DORA IP 192.168.2.254/24 GW 192.168.2.1

VPCS> ping 192.168.1.254

84 bytes from 192.168.1.254 icmp_seq=1 ttl=62 time=2.611 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=62 time=2.189 ms
^C
VPCS> █
```