SSL VPN - Certificate Based Authentication

Below are the steps to configure CA, Server and Client certificate for SSL VPN certificate based authentication.

On linux:

Create Certificate Authority(CA)

Create a working directory and openssl.cnf file specifically for this purpose.

```
# mkdir -p /opt/edoceo/etc/ssl
# cd /opt/edoceo/etc/ssl
# cp /etc/ssl/openssl.cnf ./
```

Edit openssl.cnf accordingly, adjusting paths and defaults in req_distingushed_name section.

Create a key, request and then self-sign.

```
# openssl genrsa -out labca.key 1024
# openssl req -config ./openssl.cnf -new -key labca.key -out labca.csr
# openssl x509 -req -days 3660 -in labca.csr -out labca.crt -signkey labca.key
```

Create Server Certificates

Request and sign the web-server certificate, remember the passwords when prompted!

```
# openssl genrsa -des3 -out sslserver.key 1024
# openssl req -config openssl.cnf -new -key sslserver.key -out sslserver.csr
# openssl ca -config openssl.cnf -in sslserver.csr -cert labca.crt -keyfile labca.key -out sslserver.crt
```

Create Client Certificates

Create Client Certifictes in PEM (openssl), PKCS#12 (firefox) and DER (internet explorer) formats. Enter a reasonable username (eg: "first.last") and organizational unit as these will be used for the authentication.

```
# openssl genrsa -des3 -out ssluser1.key 1024
# openssl req -config openssl.cnf -new -key ssluser1.key -out ssluser1.csr
# openssl ca -config openssl.cnf -in ssluser1.csr -cert labca.crt -keyfile labca.key -out ssluser1.crt

# openssl pkcs12 -export -clcerts -in ssluser1.crt -inkey ssluser1.key -out ssluser1.p12
# openssl x509 -inform PEM -in ssluser1.crt -outform DER -out ssluser1.der
# openssl x509 -inform PEM -in labca.crt -outform DER -out labca.der
```

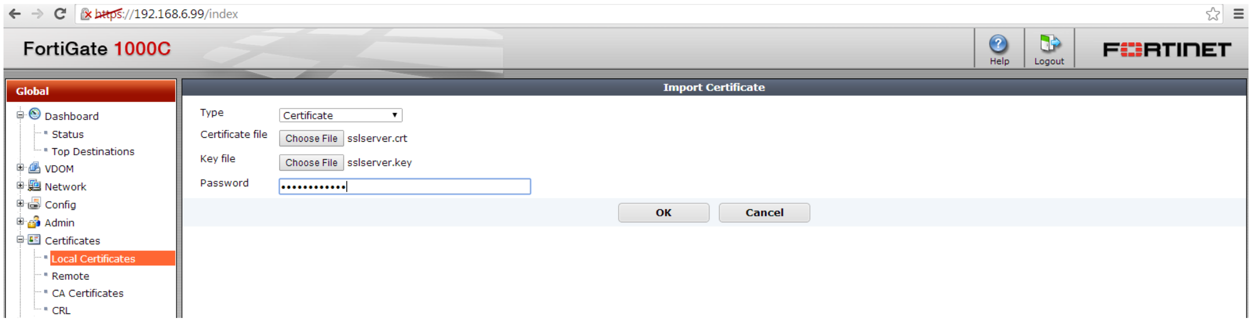
Import the pkcs12 to Firefox and both DER files to Internet Explorer.

How to add the Certificates on Fortigate:

To enable certificate authentication for an SSL VPN user group

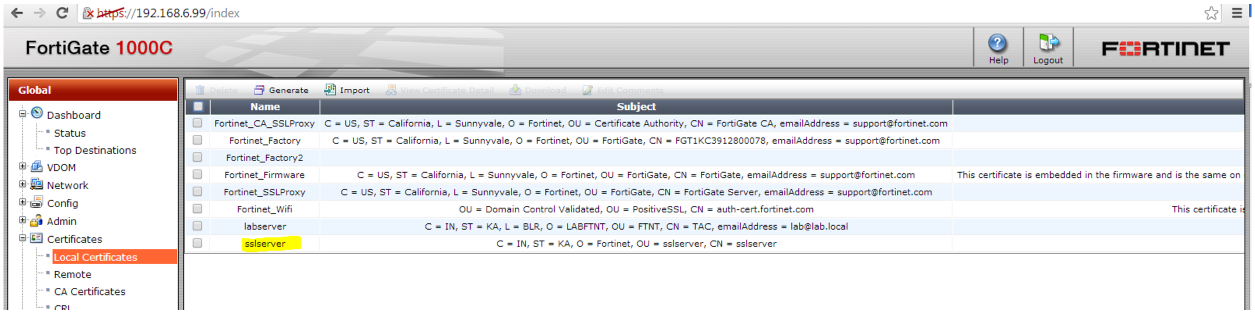
1. Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
2. Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.
3. Install the root certificate and the CRL from the issuing CA on the FortiGate
4. Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
5. Add the PKI users to the SSL VPN usergroup
6. Select the Server Certificate and enable Require Client Certificate on SSL VPN settings and apply the usergroup.

1. Add the SSL server Certificate on Fortigate (Under System >> Certificates >> Local Certificates).



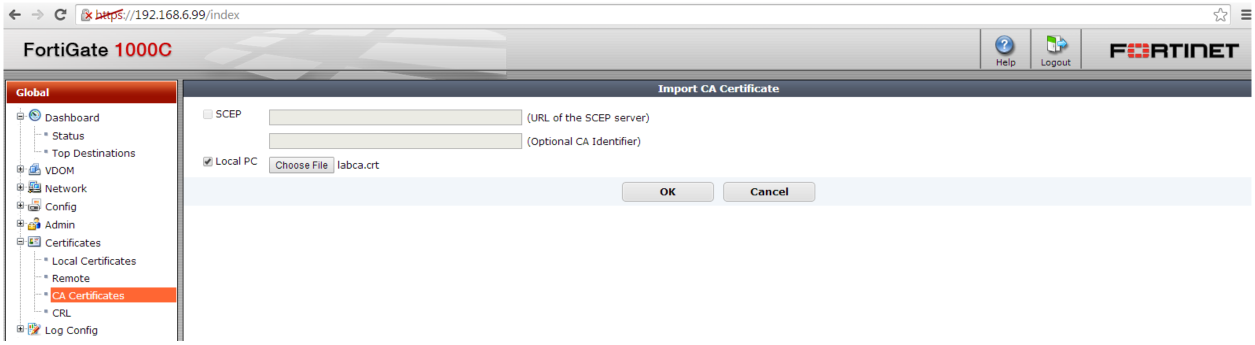
Import Certificate

Type: Certificate
Certificate file: Choose File sslserver.crt
Key file: Choose File sslserver.key
Password: ••••••••••••



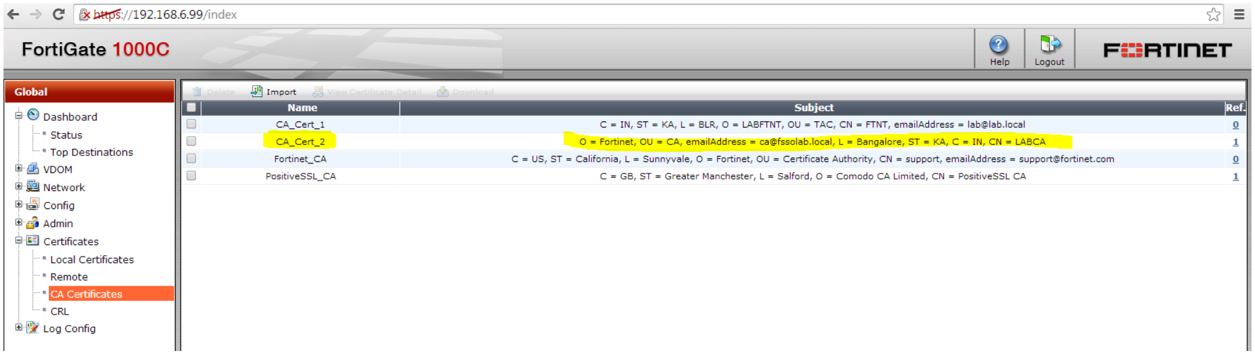
☐	Name	Subject	
☐	Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	
☐	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT1KC3912800078, emailAddress = support@fortinet.com	
☐	Fortinet_Factory2		
☐	Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FortiGate, emailAddress = support@fortinet.com	This certificate is embedded in the firmware and is the same on
☐	Fortinet_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FortiGate Server, emailAddress = support@fortinet.com	
☐	Fortinet_Wifi	OU = Domain Control Validated, OU = PositiveSSL, CN = auth-cert.fortinet.com	This certificate i
☐	labserver	C = IN, ST = KA, L = BLR, O = LABFTNT, OU = FTNT, CN = TAC, emailAddress = lab@lab.local	
☐	sslserver	C = IN, ST = KA, O = Fortinet, OU = sslserver, CN = sslserver	

2. To add CA certificate on Fortigate (Under System >> Certificates >> CA certificate).



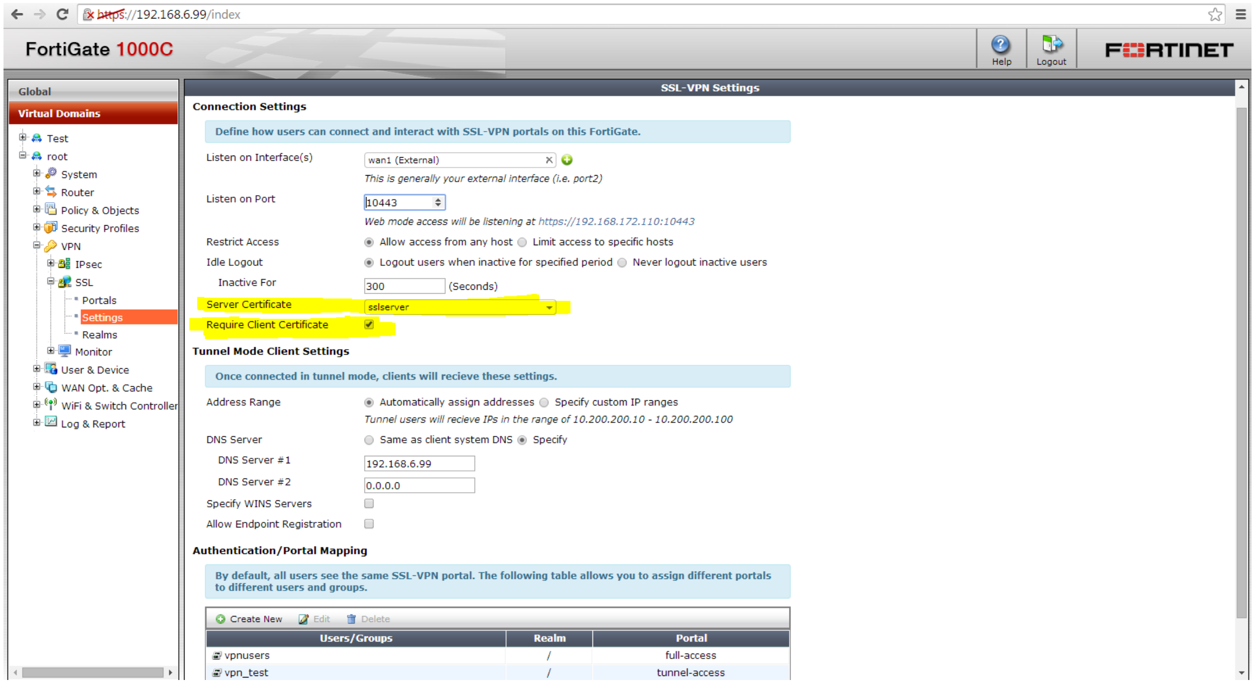
Import CA Certificate

☐ SCEP (URL of the SCEP server)
(Optional CA Identifier)
☑ Local PC Choose File labca.crt



☐	Name	Subject	Ref.
☐	CA_Cert_1	C = IN, ST = KA, L = BLR, O = LABFTNT, OU = TAC, CN = FTNT, emailAddress = lab@lab.local	0
☐	CA_Cert_2	O = Fortinet, OU = CA, emailAddress = ca@fssolab.local, L = Bangalore, ST = KA, C = IN, CN = LABCA	1
☐	Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com	0
☐	PositiveSSL_CA	C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = PositiveSSL CA	1

3. Goto Vpn >> SSL >> Settings >> Select the Server Certificate created above.



SSL-VPN Settings

Connection Settings

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s): wan1 (External)

This is generally your external interface (i.e. port2)

Listen on Port: 10443

Web mode access will be listening at https://192.168.172.110:10443

Restrict Access: ● Allow access from any host ○ Limit access to specific hosts

Idle Logout: ● Logout users when inactive for specified period ○ Never logout inactive users

Inactive For: 300 (Seconds)

Server Certificate: sslserver

Require Client Certificate: ☑

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will recieve these settings.

Address Range: ● Automatically assign addresses ○ Specify custom IP ranges

Tunnel users will recieve IPs in the range of 10.200.200.10 - 10.200.200.100

DNS Server: ○ Same as client system DNS ● Specify

DNS Server #1: 192.168.6.99

DNS Server #2: 0.0.0.0

Specify WINS Servers: ☐

Allow Endpoint Registration: ☐

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Create New Edit Delete

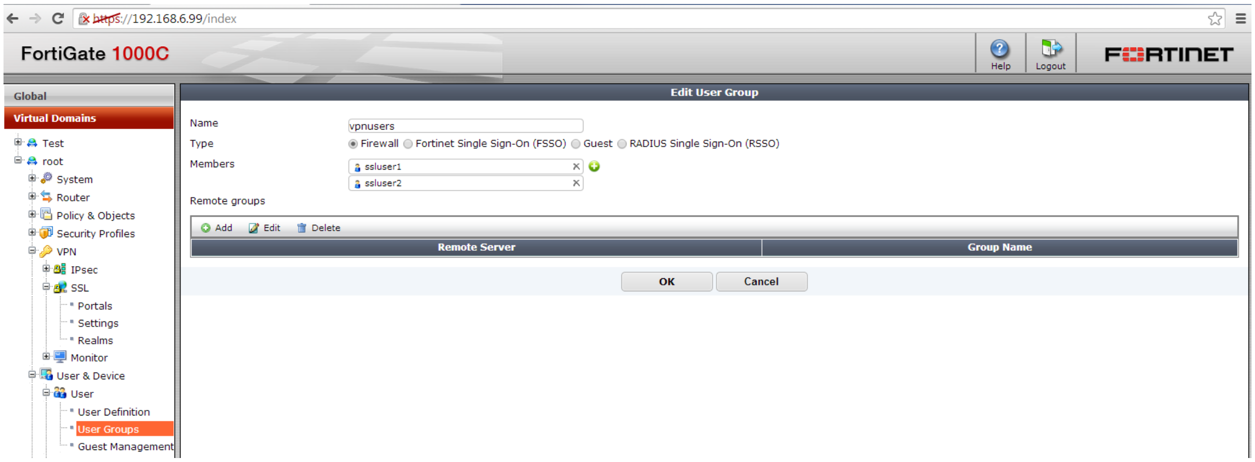
Users/Groups	Realm	Portal
vpnusers	/	full-access
vpn_test	/	tunnel-access

4. Create PKI userusing CLI

```
config user peer
   edit "ssluser1"
      set ca "CA_Cert_2"
      set subject "ssluser1"
   next
   edit "ssluser2"
      set ca "CA_Cert_2"
      set subject "ssluser2"
   next
end
```

The subject should match the client certificate.

5. Add the PKI to SSL VPN usergroup.



Edit User Group

Name: vpnusers

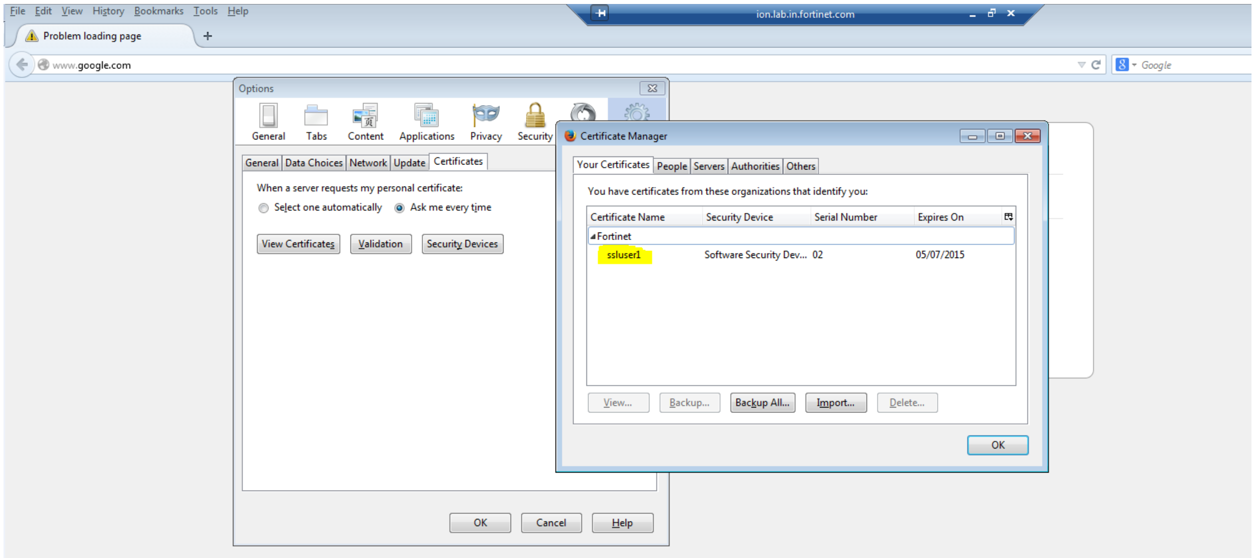
Type: ● Firewall ○ Fortinet Single Sign-On (FSSO) ○ Guest ○ RADIUS Single Sign-On (RSSO)

Members: ssluser1, ssluser2

Remote groups

Remote Server	Group Name

6. Add Client and CA Certificate on Browser.
To add the client certificate on Mozilla browser, goto Tools >> Options >> Advanced >> Certificates >> Add the certificates



When a server requests my personal certificate:

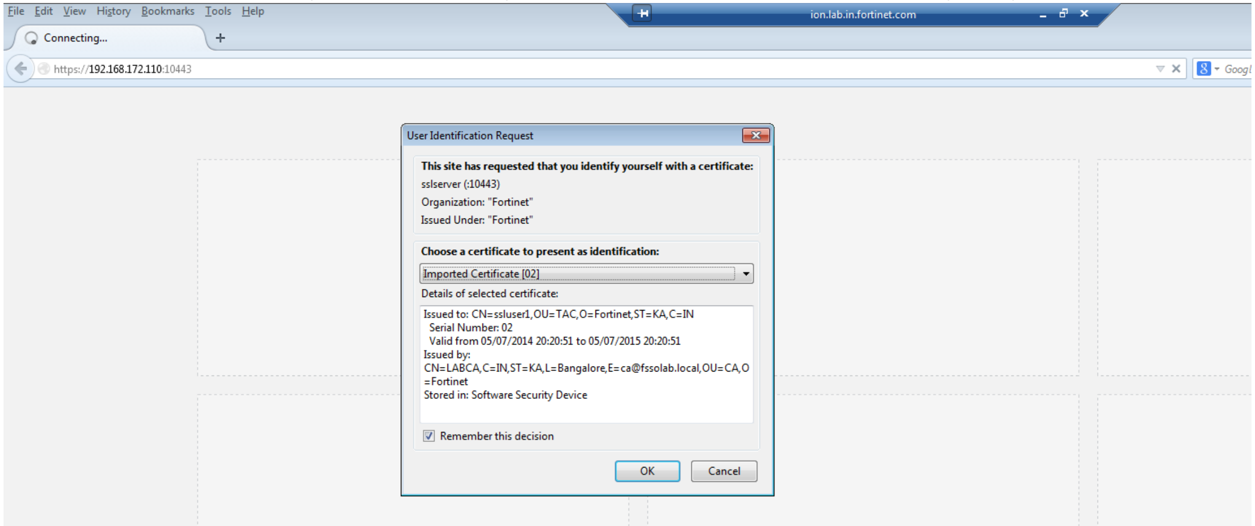
○ Select one automatically ● Ask me every time

You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
Fortinet			
ssluser1	Software Security Dev...	02	05/07/2015

7. Login to SSL VPN

When user enter the url/ip address of sslvpn, the user/client Certificate will be prompted.


File Edit View History Bookmarks Tools Help
ion.lab.in.fortinet.com
Connecting...
https://192.168.172.110:10443
Googl
OK
Cancel

User Identification Request

This site has requested that you identify yourself with a certificate:
sslserver (:10443)
Organization: "Fortinet"
Issued Under: "Fortinet"

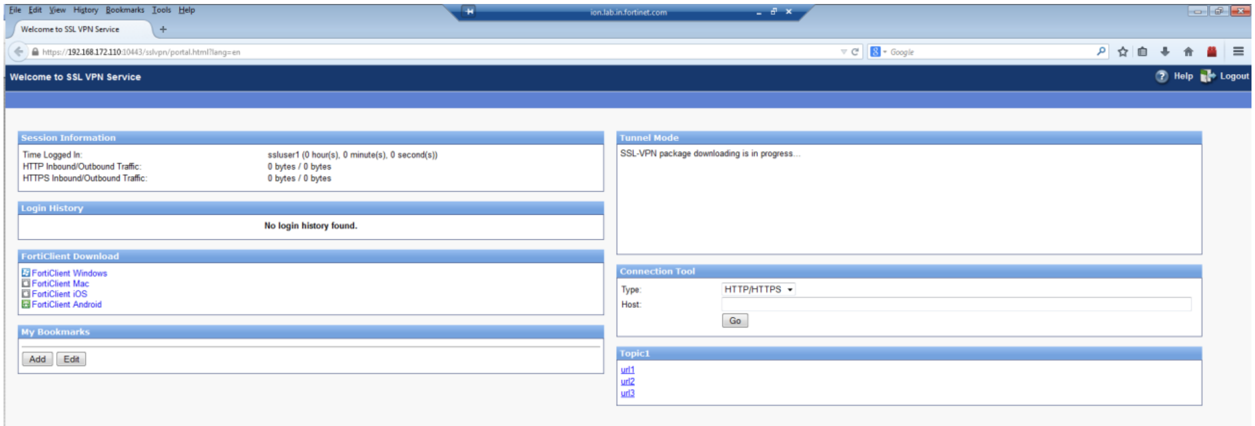
Choose a certificate to present as identification:
Imported Certificate [02]

Details of selected certificate:

Issued to: CN=ssluser1,OU=TAC,O=Fortinet,ST=KA,C=IN
Serial Number: 02
Valid from 05/07/2014 20:20:51 to 05/07/2015 20:20:51
Issued by:
CN=LABCA,C=IN,ST=KA,L=Bangalore,E=ca@fssolab.local,OU=CA,O=Fortinet
Stored in: Software Security Device

☑ Remember this decision

Once you select the Certificate, Fortigate verifies the certificate and if it matches, the user will be login to SSL VPN.


File Edit View History Bookmarks Tools Help
ion.lab.in.fortinet.com
Welcome to SSL VPN Service
https://192.168.172.110:10443/sslvpn/portal.html?lang=en
Google
Help
Logout
Add
Edit
Go

Welcome to SSL VPN Service

Session Information

Time Logged In: ssluser1 (0 hour(s), 0 minute(s), 0 second(s))
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Login History

No login history found.

FortiClient Download

FortiClient Windows
FortiClient Mac
FortiClient iOS
FortiClient Android

My Bookmarks

Tunnel Mode

SSL-VPN package downloading is in progress...

Connection Tool

Type: HTTP/HTTPS
Host:

Topic1

url1
url2
url3