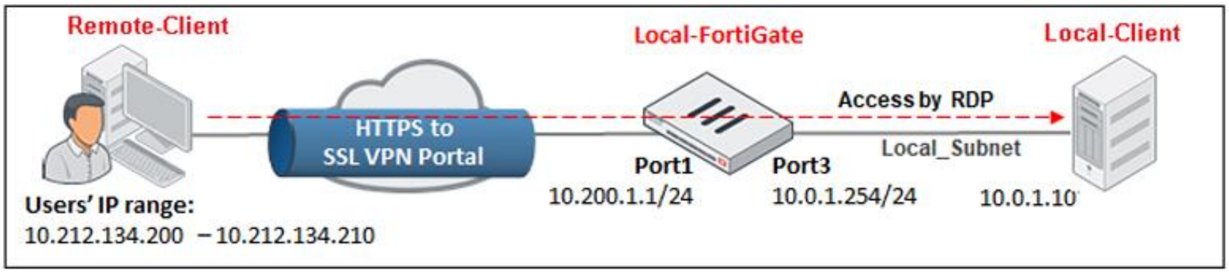
# SSL VPN Configuration

## Objectives:

In this lab, you will examine how to configure an SSL VPN connection in tunnel and web modes. You will also manage user groups and portals for SSL VPN.

- Configure and connect to an SSL VPN.
- Enable authentication security.
- Configure a firewall policy for SSL VPN users to access private network resources.
- Customize the SSL VPN portal for web mode.
- Configure FortiClient for the SSL VPN connection in tunnel mode.

## Topology:



## Components which used:

1-Fortigate Device

2-Local Windows Machine

3-Remote Windows Machine

## Steps of the Lap:

- 1. Configuring Web Mode SSL VPN:
  1. Connect to the Local-FortiGate GUI
  2. Click User & Authentication>User Definition
  3. Click Create New.
  4. Click Local User, and then click Next.
  5. Type the following credentials for the remote user (Username & Password), and then click Next.
  6. Leave the contact information empty and click Next.

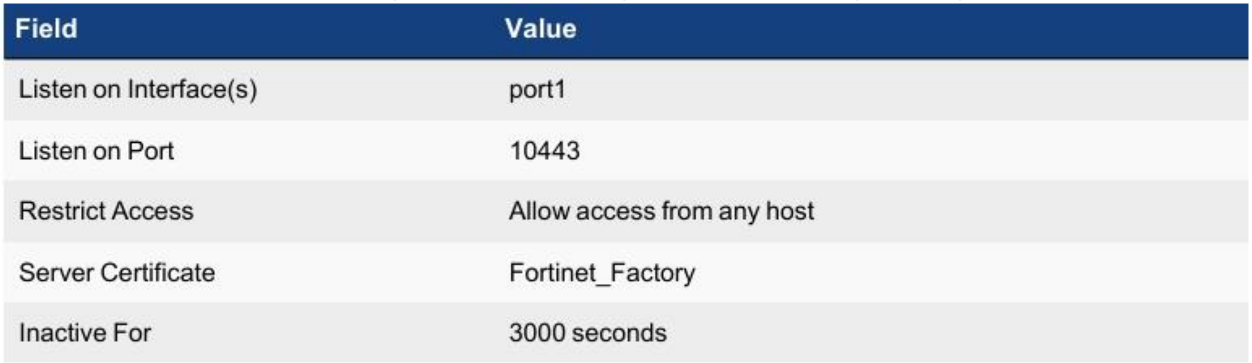
  7. For User Account Status, verify that Enabled is selected.

8. Enable User Group, click the + that appears, and then in the right pane, select SSL_VPN_USERS.

9. Click Submit

- To configure the SSL VPN settings for web access:

1. click VPN > SSL-VPN Settings.
2. In the Connection Settings section, configure the following settings.



| Field | Value |
|---|---|
| Listen on Interface(s) | port1 |
| Listen on Port | 10443 |
| Restrict Access | Allow access from any host |
| Server Certificate | Fortinet_Factory |
| Inactive For | 3000 seconds |

3. In the Tunnel Mode Client Settings section, verify the following setting:
Address Range -----→ Automatically assign addresses
4. In the Authentication/Portal Mapping section, select All Other Users/Groups, and then click Edit.
5. In the Portal drop-down list, select web-access, and then click OK.
6. Click Apply to save the changes.
7. create a firewall policy that allows traffic to the local subnet (10.0.1.0/24) from remote users connected to the SSL VPN portal
8. After finish the policy save the Configuration and logout from FortiGate.

# Test the SSL VPN Access:

1.From remote Client Open Firefox, and then connect to: https://10.200.1.1:10443/

2. Click Advanced, and then click Accept the Risk and Continue. The remote login page opens.

3. Log in with the username and password. The SSL VPN web portal opens. The portal is using default settings.

4. Continuing the SSL VPN portal where you are logged in, click Quick Connection. Notice all the available options the SSL VPN portal allows for connections.

5. Click RDP, and then configure the following setting:

Host -------------------→ 10.0.1.10

6.Keep the default values for the remaining settings, and then click Launch.

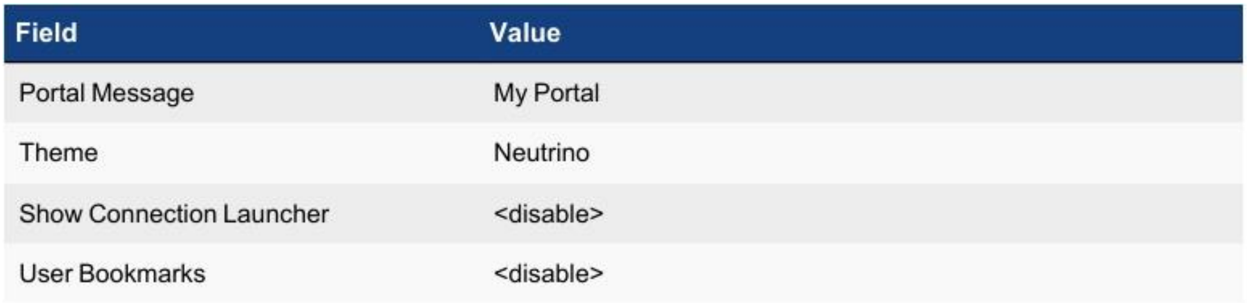
7. Log in with the username Administrator and password password.

8. Click OK.

You are now remotely connected to the Local-Client VM

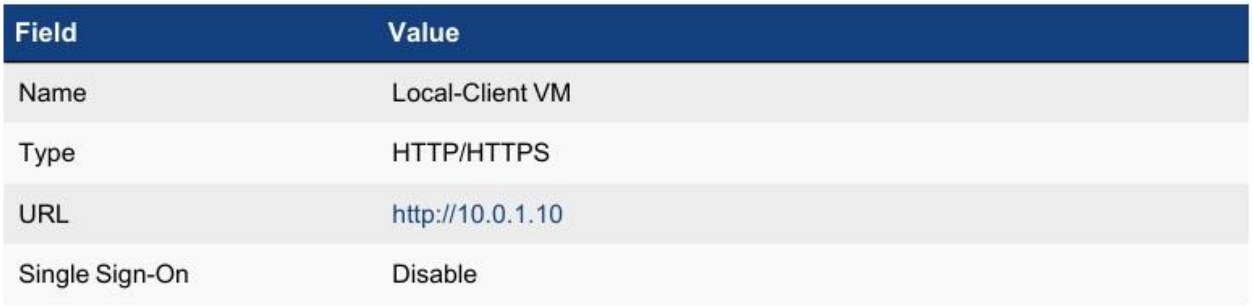
- Add an Administrator-Based Bookmark to the SSL VPN Portal:

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.
2. Click VPN>SSL-VPN Portals.
3. Select web-access, and then click Edit.
4. Configure the following settings



| Field | Value |
|---|---|
| Portal Message | My Portal |
| Theme | Neutrino |
| Show Connection Launcher | <disable> |
| User Bookmarks | <disable> |

5. In the Predefined Bookmarks section, click Create New, and then configure the following settings



| Field | Value |
|---|---|
| Name | Local-Client VM |
| Type | HTTP/HTTPS |
| URL | http://10.0.1.10 |
| Single Sign-On | Disable |

6. Click OK.
7. Click OK again to save the portal settings.

## Test SSL VPN Access Using the Predefined Bookmark:

To test the bookmark

1. Return to the Remote-Client VM.

2. Open Firefox, and then reconnect to the SSL VPN portal at: https://10.200.1.1:10443/
3. Login with the username and password. Notice that the SSL VPN portal no longer allows quick connections or allows you to add bookmarks.

3.Click the Local-Client VM bookmark. You will connect to the web server running on the Local-Client VM at 10.0.1.10

## The Result:

We Can Monitor to see the Result

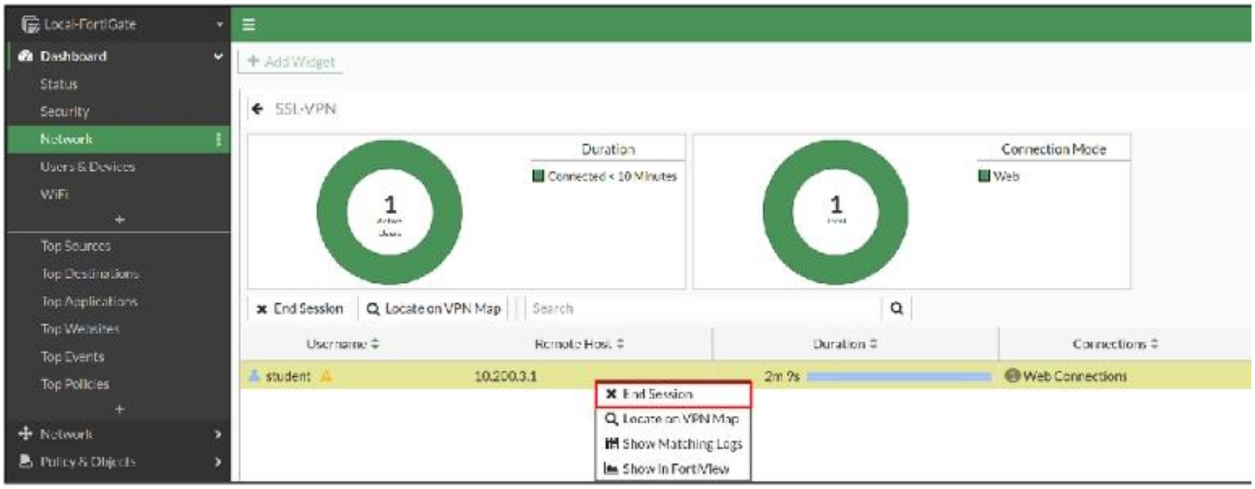
Monitor an SSL VPN User

1. Return to the Local-FortiGate GUI.

2. Click Dashboard>Network, and then view the SSL-VPN widget. You can see that the student user is connecting from the remote host 10.200.3.1

3. Right-click student, and then select End Session.

4. Click OK. The student user no longer appears in the SSL VPN monitor.



| Username | Remote Host | Duration | Connections |
|---|---|---|---|
| student | 10.200.3.1 | 2m 9s | Web Connections |

## 2. Configuring SSL VPN Tunnel Mode:

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password.

2. Click VPN>SSL-VPN Settings.

3. In the Authentication/Portal Mapping section, select All Other Users/Groups, and then click Edit

4. In the Portal drop-down list, select tunnel access, and then click OK.

5. Click Apply.

**Configure the Routing for Tunnel Mode:**

You will establish the routing address to use in tunnel mode.

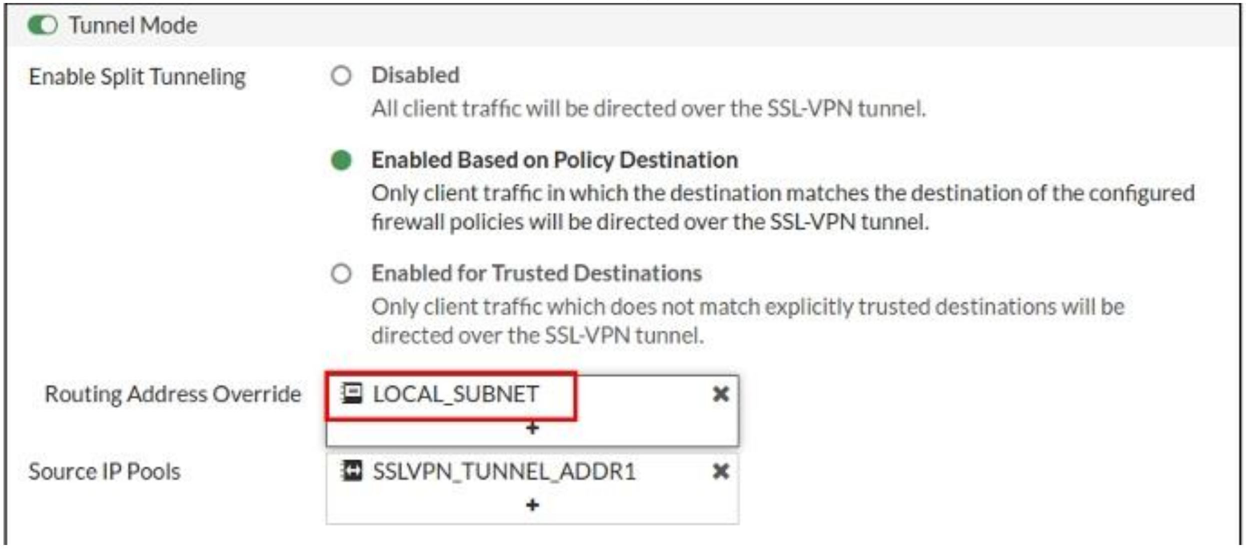
Notice that in tunnel mode, FortiClient establishes one or more routes in the SSL VPN user's host after the tunnel is connected. Traffic destined to the internal subnets is correctly routed through the tunnel.

To configure the routing for tunnel mode:

1. Continuing the Local-FortiGate GUI, click VPN > SSL-VPN Portals.

2. Select the tunnel-access portal, and then click Edit.

3. In the Tunnel Mode section, set the Routing Address Override to LOCAL_SUBNET



Tunnel Mode

Enable Split Tunneling

○ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

● Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

○ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override: LOCAL_SUBNET

Source IP Pools: SSLVPN_TUNNEL_ADDR1

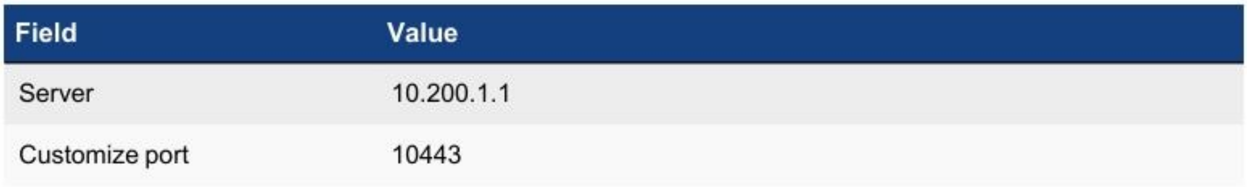
4. Click OK.

**Configure FortiClient for SSL VPN Connections:**

1. ConnecttotheRemote-Client VM.

2. Click Desktop> forticlient ssl vpn > 64bit, and then double-click forticlient ssl vpn to configure SSL VPN client settings.

3. Configure the following settings for the FortiClient SSLVPN application



| Field | Value |
|---|---|
| Server | 10.200.1.1 |
| Customize port | 10443 |

## Test SSL VPN in Tunnel Mode:

1. Continuing on the FortiClient SSLVPN application, in the User field, type Username, and in the type Password.

2. Click Connect.

3. Click Continue to accept the certificate. The tunnel is connected.

**To test the tunnel:**

1. Continuing on the Remote-Client VM, open Firefox, and then access the following URL: http://10.0.1.10 2. Look at the URL. You are connected to the webserver URL as if you were based in the local subnet (10.0.1.0/24)
2. This time, you are not using the reverse HTTP proxy as in the case of web-access mode. The IP traffic is directly encapsulated over HTTPS and sent through the tunnel.
3. Return to FortiClient, and then click Stop.

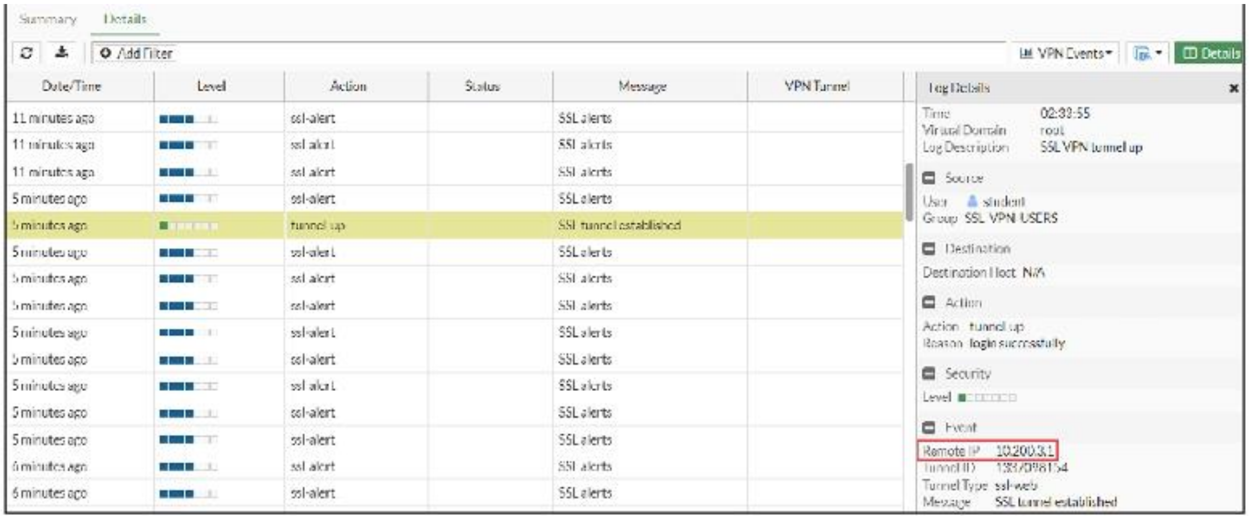
**To review VPN events for SSL VPN connections:**

1. Connect to the Local-FortiGate GUI, and then log in with the username and password. 2. Click Log & Report>System Events, and then click View Logs arrow button on the VPN Events widget.

3. Compare the log details of the tunnel-up logs you see. Hint: Use your log filters to filter on Action = tunnel-up.

## The results:

The most recent tunnel-up log shows one IP address under Remote IP. This log shows the recent connection to the SSL VPN portal. Even though the SSL VPN portal presented a warning message and did not allow remote access to the local resources, FortiGate shows that an SSL VPN connection was established, and the tunnel was up.



| Date/Time | Level | Action | Status | Message | VPN Tunnel |
|---|---|---|---|---|---|
| 11 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 11 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 11 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■□□□□□ | tunnel-up | | SSL tunnel established | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 5 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 6 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |
| 6 minutes ago | ■■■□□ | ssl-alert | | SSL alerts | |

Log Details

Time 02:33:55
Virtual Domain root
Log Description SSL VPN tunnel up

Source
User student
Group SSL VPN USERS

Destination
Destination Host N/A

Action
Action tunnel-up
Reason login successfully

Security
Level ■□□□□□

Event
Remote IP 10.200.3.1
Tunnel ID 1337098154
Tunnel Type ssl-web
Message SSL tunnel established

The second most recent tunnel-up log in the VPN event list shows the SSL VPN connection in tunnel mode through FortiClient. Notice this log presents two IP addresses**:**

**Remote IP :** IP address of the remote user's gateway(egress interface)

**Tunnel IP:** IP address FortiGate assigns to the virtual network adapter fortissl.