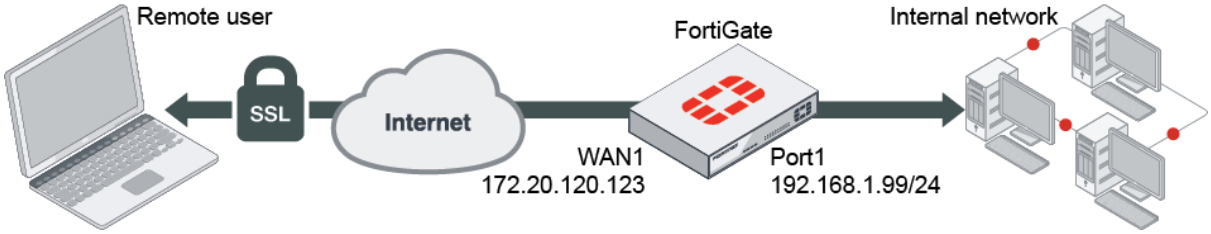
SSL VPN FULL TUNNEL FOR REMOTE USER

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

To configure SSL VPN using the GUI:

1. Configure the interface and firewall address:
    1. Go to *Network* > *Interfaces* and edit the *wan1* interface.
    2. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
    3. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
    4. Click *OK*.
2. Configure user and user group:
    1. Go to *User & Authentication* > *User Definition* to create a local user *sslvpnuser1*.
    2. Go to *User & Authentication* > *User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal:
    1. Go to *VPN* > *SSL-VPN Portals* to create a tunnel mode only portal *my-full-tunnel-portal*.
    2. Disable *Split Tunneling*.
4. Configure SSL VPN settings:
    1. Go to *VPN* > *SSL-VPN Settings*.
    2. For *Listen on Interface(s)*, select *wan1*.
    3. Set *Listen on Port* to *10443*.

4. Choose a certificate for *Server Certificate*. The default is *Fortinet_Factory*.
5. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.
6. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-full-tunnel-portal*.

5. Configure SSL VPN firewall policies to allow remote user to access the internal network:
    1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
    2. Set *Name* to *sslvpn tunnel mode access*.
    3. Set *Incoming Interface* to *SSL-VPN tunnel interface(ssl.root)*.
    4. Set *Outgoing Interface* to *port1*.
    5. Set the *Source* Address to *all* and User to *sslvpngroup*.
    6. Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
    7. Click *OK*.
    8. Click *Create New*.
    9. Set *Name* to *sslvpn tunnel mode outgoing*.
    10. Configure the same settings as the previous policy, except set *Outgoing Interface* to *wan1*.
    11. Click *OK*.

To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.
2. config system interface
3. edit "wan1"
4. set vdom "root"
5. set ip 172.20.120.123 255.255.255.0
6. next

end

2. Configure the internal interface and protected subnet, then connect the port1 interface to the internal network.
3. config system interface
4. edit "port1"
5. set vdom "root"
6. set ip 192.168.1.99 255.255.255.0

7. next

end

3. Configure user and user group.
4. config user local
5. edit "sslvpnuser1"
6. set type password
7. set passwd your-password
8. next

end

config user group

edit "sslvpngroup"

set member "sslvpnuser1"

next

end

4. Configure SSL VPN web portal and predefine RDP bookmark for windows server.
5. config vpn ssl web portal
6. edit "my-full-tunnel-portal"
7. set tunnel-mode enable
8. set split-tunneling disable
9. set ip-pools "SSLVPN_TUNNEL_ADDR1"
10. next

end

5. Configure SSL VPN settings.
6. config vpn ssl settings
7. set servercert "Fortinet_Factory"
8. set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
9. set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
10. set source-interface "wan1"
11. set source-address "all"
12. set source-address6 "all"
13. set default-portal "full-access"

```
    config authentication-rule
        edit 1
            set groups "sslvpngroup"
            set portal "my-full-tunnel-portal"
        next
    end
end
```

6. Configure SSL VPN firewall policies to allow remote user to access the internal network. Traffic is dropped from internal to remote client.

```
    config firewall policy
        edit 1
            set name "sslvpn tunnel mode access"
            set srcintf "ssl.root"
            set dstintf "port1"
            set srcaddr "all"
            set dstaddr "all"
            set groups "sslvpngroup"
            set action accept
            set schedule "always"
            set service "ALL"
        next
        edit 2
            set name "sslvpn tunnel mode outgoing"
            set srcintf "ssl.root"
            set dstintf "wan1"
            set srcaddr "all"
            set dstaddr "all"
            set groups "sslvpngroup"
            set action accept
            set schedule "always"
            set service "ALL"
```

29. next

end

To see the results:

1. Download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
    - Set *VPN Type* to *SSL VPN*.
    - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.
7. After connection, all traffic except the local subnet will go through the tunnel *FGT*.
8. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report > Forward Traffic* and view the details for the SSL entry.