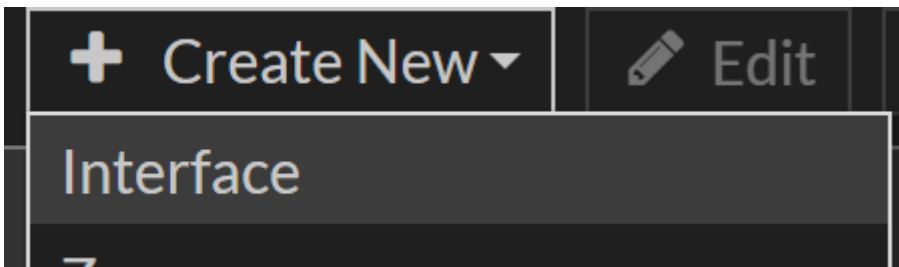
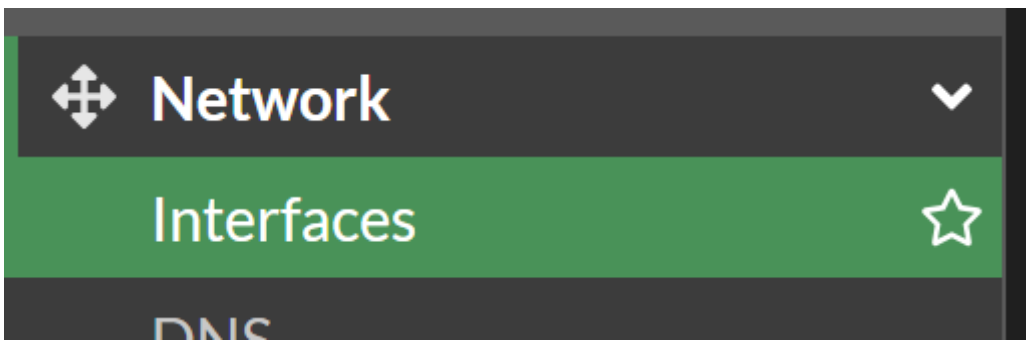


# SSL-VPN on custom Interface

This explains how to setup the SSL-VPN on a FortiGate (E-Series) on a Custom Interface for better Controls.

This is done because per default, SSL-VPN Listens on the WAN Interface directly, therefor can not be controlled by any Policy.

## Create Loopback Interface



Name

Alias

Type  ▼

Role ⓘ  ▼

---

Address

IP/Netmask

Create address object matching subnet

Name ⓘ

Destination

Secondary IP address

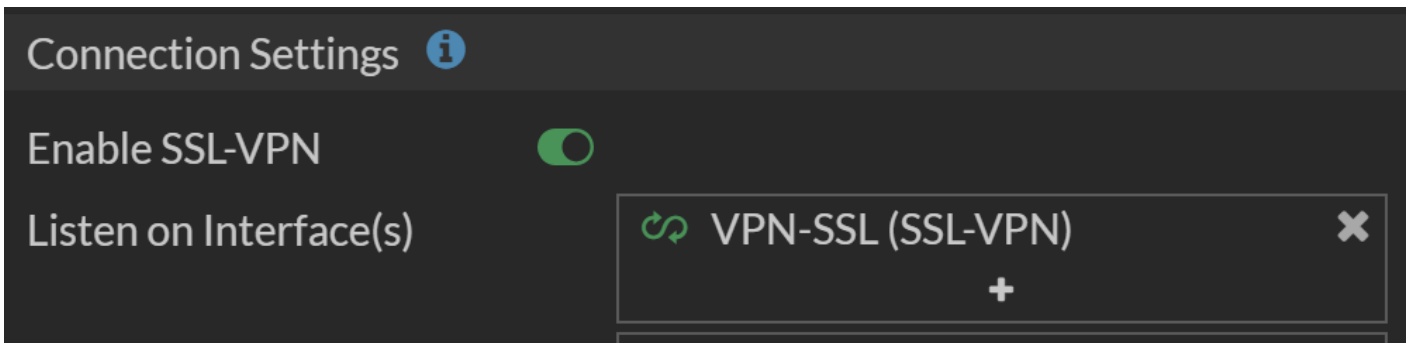
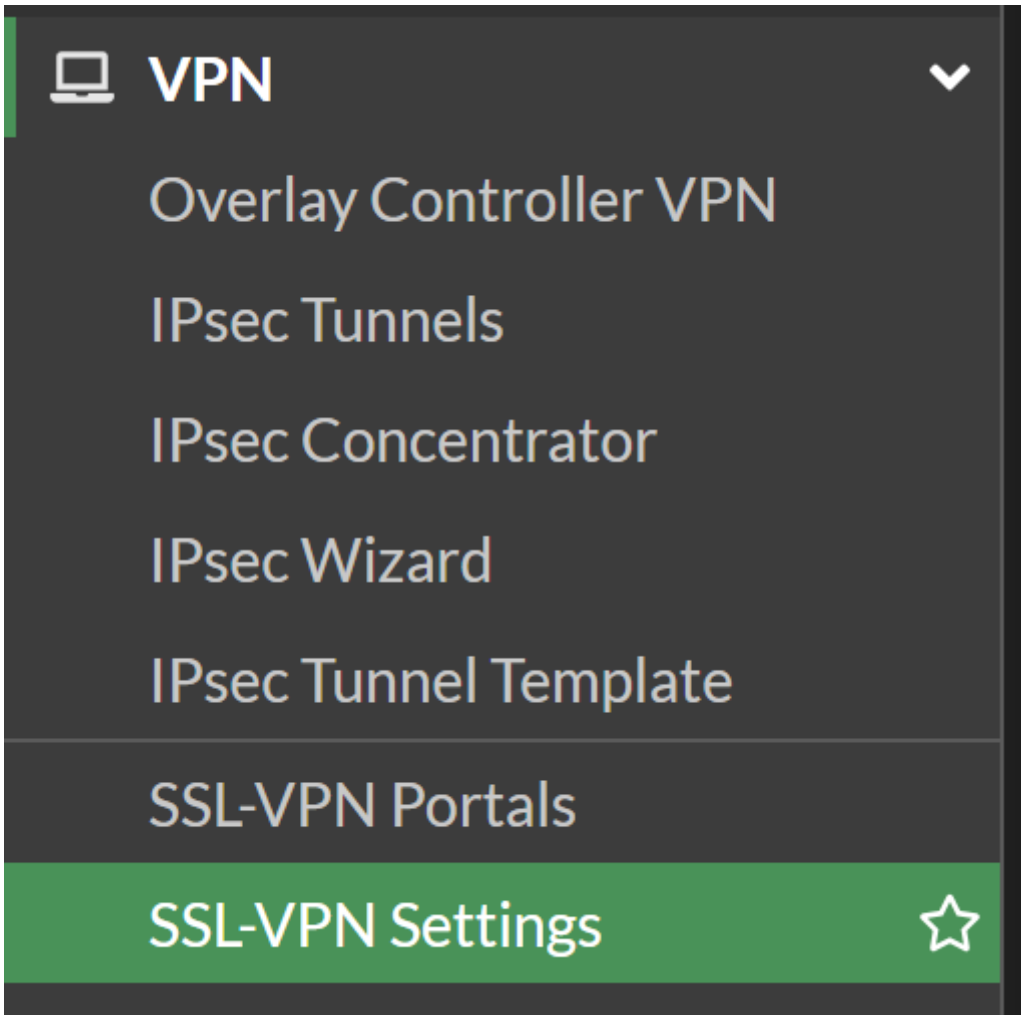
---

Administrative Access

IPv4

|                                     |  |   |
|-------------------------------------|--|---|
| <input type="checkbox"/> HTTPS      | <input type="checkbox"/> HTTP ⓘ            | <input type="checkbox"/> PING                         |
| <input type="checkbox"/> FMG-Access | <input type="checkbox"/> SSH               | <input type="checkbox"/> SNMP                         |
| <input type="checkbox"/> FTM        | <input type="checkbox"/> RADIUS Accounting | <input type="checkbox"/> Security Fabric Connection ⓘ |
| <input type="checkbox"/> Speed Test |  |   |

## Bind SSL-VPN to new Loopback Interface



## Redirect SSL-VPN Traffic

We now need to make sure the SSL-VPN Traffic actually reaches the new SSL-VPN Interface. We will use a Virtual IP with Port Forwarding for that.



## Policy & Objects



Firewall Policy

Local In Policy

IPv4 DoS Policy

Proxy Policy

Authentication Rules

Addresses

Internet Service Database

Services

Schedules

Virtual IPs




+ Create new

VIP type IPv4

Name


Comments  0/255

Color 

### Network

Interface

Type Static NAT

External IP address/range 

Map to

IPv4 address/range


Optional Filters

Source address

Services

Port Forwarding

Port Mapping Type

Map to IPv4 port 

Allow Traffic to new Interface



## Policy & Objects





Firewall Policy





+ Create New

ID 19



Name ⓘ Allow-WAN-to-SSLVPN

Incoming Interface  FB WAN (wan1) 

+



Outgoing Interface  VPN-SSL (SSL-VPN) 

+

Source  all 



+



Negate Source

Destination  VIP-SSLVPN-TCP 

+

Negate Destination

Schedule  always 

Service  SSL-VPN 

+

Action  ACCEPT  DENY  IPsec

Inspection Mode  Flow-based  Proxy-based

Firewall/Network Options

NAT

Revision #1

Created 3 October 2025 22:00:30 by Oliver Karger

Updated 3 October 2025 22:05:49 by Oliver Karger