

# 01 | IPsec Dial Up VPN (Vervanger voor SSL-VPN)

SSL-VPN is voortaan niet meer beschikbaar op de entry level modellen van Fortinet. Tevens is het gebruik van SSL-VPN ook niet altijd even veilig gebleken in het verleden. Hieronder staan een aantal stappen om de IPsec Dial Up VPN te configureren op basis van lokale gebruikers.

## Stap 1 - Phase 1 interface aanmaken

```
config vpn ipsec phase1-interface
edit "DU-VPN"
    set type dynamic          ## Dynamic allows multiple clients to connect
    set interface "wan1"     ## Bind to the incoming interface
    set ike-version 2        ## use IKEv2 for negotiation
    set peertype one         ## Only allow one specific peer ID
    set net-device disable
    set mode-cfg enable      ## Mode cfg, allow clients to dynamically get an IP and DNS settings
    set proposal aes256-sha256 ## Encryption/authentication proposal
    set localid <redacted>>  ## Local ID (remote ID on client)
    set dhgrp 16             ## Diffie-Hellman group
    set eap enable           ## Enable EAP (Username / Password authentication)
    set eap-identity send-request ## how to handle EAP identity requests from the client
    set fec-egress enable    ## Forward Error Correction (FEC), for noisy links such as 4G/5G
    set fec-codec rs
    set fec-ingress enable
    set peerid <redacted>    ## Peer ID (local ID on client)
    set ipv4-start-ip 10.32.250.10
    set ipv4-end-ip 10.32.250.30
    set ipv4-netmask 255.255.255.224 ## Subnet mask for mode cfg
    set dns-mode auto        ## Add DNS to mode cfg
    set save-password enable ## Allow user to store password on client
    set client-auto-negotiate enable ## Allow client to auto-negotiate the tunnel at startup
    set client-keep-alive enable ## Keepalive to maintain idle tunnel
```

```
set psksecret <redacted>      ## Pre-shared key
set dpd-retryinterval 60     ## Dead Peer Detection

next

end
```

## Stap 2 - Phase 2 configureren

```
config vpn ipsec phase2-interface
edit "DU-VPN-IPv4"
    set phase1name "DU-VPN"      ## link back to the phase1 interface defined earlier
    set proposal aes256-sha256   ## ESP proposal for the IPsec tunnel (AES-256 + SHA-256)
    set dhgrp 16                 ## DH group for PFS (set to match policy requirements)
    set replay disable
    set keepalive enable        ## keepalive will try to maintain the tunnel association

next

end
```

## Stap 3 - Phase 1 interface configureren

```
config system interface
edit "DU-VPN"
    set vdom "root"              ## VDOM the interface belongs to (single VDOM named root here)
    set ip 10.32.250.1 255.255.255.255 ## Local IP assigned to the firewall side of the tunnel (/32
common)
    set type tunnel              ## mark as a tunnel interface
    set remote-ip 10.32.250.1 255.255.255.224 ## define the remote subnet that clients will be in
(pool/netmask)
    set interface "wan1"

next

end
```

## Stap 4 - Zone aanmaken (optioneel)

```
config system zone                ## Zone to group the VPN interface for easier firewall policy management
edit "Z-VPN-DU"
    set interface "DU-VPN"        ## add the virtual DU-VPN interface to this zone
```

```
next
end
```

## Stap 5 - Lokale gebruiker aanmaken

```
config user local
  edit "firstname.lastname"
    set type password
    set email-to "firstname.lastname@example.com"
    set passwd <redacted>
  next
end
```

## Stap 6 - Firewall groep aanmaken

```
config user group
  edit "DU-VPN-USERS"
    set member "firstname.lastname"
  next
end
```

## Stap 7 - Policy aanmaken

```
config firewall policy
  edit 48
    set name "Dial-up VPN user -> INET"
    set srcintf "Z-VPN-DU"
    set dstintf "wan1"
    set action accept
    set srcaddr "N-10.32.250.0/27"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set nat enable
    set groups "DU-VPN-USERS"
  next
```

---

Revision #2

Created 8 February 2026 13:57:53 by Joshua Bergman | Lighted Networks

Updated 8 February 2026 14:30:20 by Joshua Bergman | Lighted Networks