

***DrayTek***

*IKEv2 Site-to-Site*  
***DrayTek naar Fortigate***



## Inhoudsopgave

IKEv2 .....	3
Configuratie DrayTek .....	4
IPsec service inschakelen .....	4
VPN profiel aanmaken .....	4
Algemene instellingen.....	4
IKE-Authenticatie .....	5
TCP/IP Netwerk instellingen .....	6
Configuratie Fortigate .....	7
IPsec VPN tunnel aanmaken .....	7
Netwerkinstellingen configureren .....	7
IKE Phase 1 configureren.....	8
IKE Phase 2 configureren.....	9
Address Object aanmaken .....	10
Firewall policies configureren .....	10
Static Route toevoegen .....	11
VPN status controleren.....	12
Veelvoorkomende problemen en oplossingen .....	12

## **IKEv2**

Deze handleiding beschrijft stap voor stap hoe een IKEv2 IPsec Site-to-Site VPN-tunnel wordt opgezet tussen een FortiGate firewall en een DrayTek Vigor Router. Na voltooiing kunnen apparaten op beide lokale netwerken veilig met elkaar communiceren via een versleutelde verbinding over internet.

Voor deze handleiding is gebruikgemaakt van een DrayTek Vigor2928. De Vigor2928 maakt gebruik van DrayOS5.

### **Voorwaarden:**

- Een werkende internetverbinding op beide locaties.
- Beheerrechten op zowel de DrayTek als de Fortigate.
- Bekende LAN-subnetten van beide locaties.
- Een vooraf afgesproken Pre-Shared Key (PSK).
- Openbaar IP-adres of FQDN van de FortiGate.
- FortiOS 7.0 of nieuwer.

### **Netwerkvoorbeeld:**

Locatie A (FortiGate)

LAN: 192.168.1.0/24

Locatie B (DrayTek Vigor)

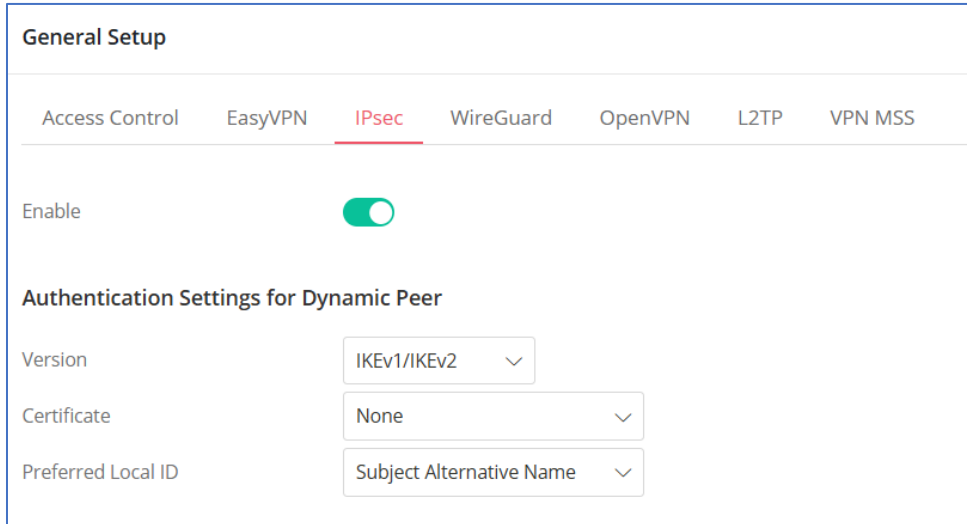
LAN: 192.168.10.0/24

Deze waarden zijn voorbeelden en moeten worden vervangen door de daadwerkelijke netwerken.

## Configuratie DrayTek

### IPsec service inschakelen

Ga naar VPN and Remote Access > General Setup > IPsec. Activeer de optie IPsec Service en sla de wijziging op met Apply.



**General Setup**

Access Control   EasyVPN   **IPsec**   WireGuard   OpenVPN   L2TP   VPN MSS

Enable

**Authentication Settings for Dynamic Peer**

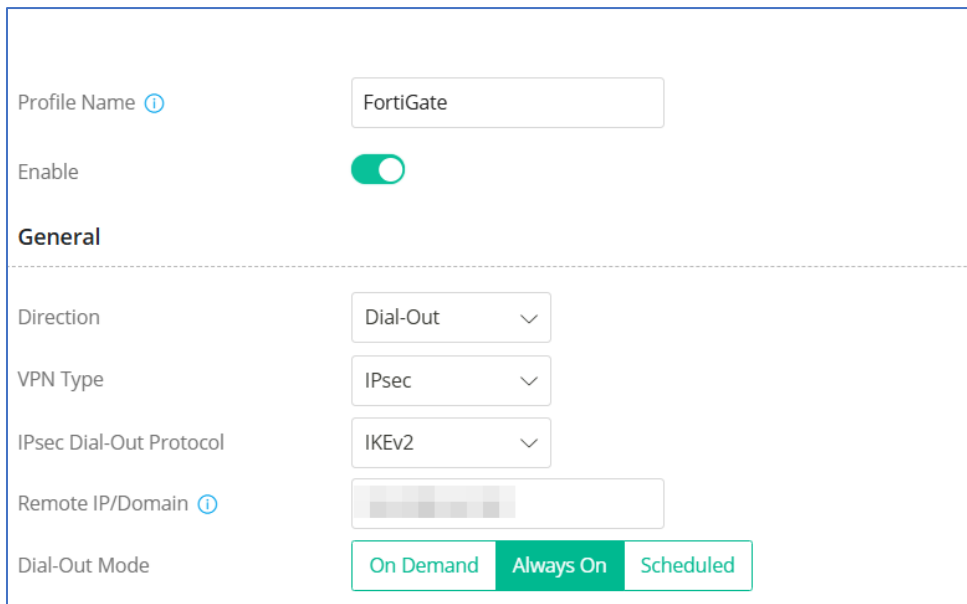
Version: IKEv1/IKEv2

Certificate: None

Preferred Local ID: Subject Alternative Name

### VPN profiel aanmaken.

Open VPN / Site-to-Site VPN en kies Add. Geef het profiel een duidelijke naam en schakel het profiel in.



Profile Name ⓘ: FortiGate

Enable

**General**

Direction: Dial-Out

VPN Type: IPsec

IPsec Dial-Out Protocol: IKEv2

Remote IP/Domain ⓘ: [Empty]

Dial-Out Mode:  On Demand  Always On  Scheduled

### Algemene instellingen

Direction: Dial-Out

VPN Type: IPsec Tunnel

IPsec Dial-Out Protocol: IKEv2

Server IP/Host Name: Publiek IP-adres of FQDN van de FortiGate

Dial-Out Mode: Always On

## IKE-Authenticatie

Selecteer Pre-Shared Key als authenticatiemethode en voer dezelfde sleutel in als op de FortiGate. Vul vervolgens de IKEv2 Local ID in. Deze waarde moet exact overeenkomen met de Peer ID die op de FortiGate is geconfigureerd.

### IKE Authentication

---

#### Dial-Out Settings

Authentication Pre-Shared Key Certificate

Pre-Shared Key ⓘ

#### IKE Identifier

Local ID (IP Address/FQDN/Email) ⓘ

Peer ID (IP Address/FQDN/Email) ⓘ

**Note:** IKE Identifier is optional in Main Mode negotiations.

Via More Settings kunnen aanvullende opties zoals Force Reauthentication en Perfect Forward Secrecy (PFS) worden geactiveerd. Zorg ervoor dat encryptie- en authenticatie-instellingen overeenkomen met de FortiGate-configuratie.

### IKE Phase1

Encryption ⓘ	Group ⓘ	Authentication ⓘ	Lifetime ⓘ
AES256-CBC ▾	14 ▾	SHA256 ▾	28800

Force UDP Encapsulation

Force Reauthentication ⓘ

### IKE Phase 2

Security Protocol	Encryption ⓘ	Authentication ⓘ	Lifetime ⓘ	Perfect Forward Secret
<span>ESP (High)</span>	AES256-CBC ▾	SHA256 ▾	3600	<input checked="" type="checkbox"/>

## TCP/IP Netwerk instellingen

Voer bij Local Network het lokale subnet van de DrayTek in. Bij Remote Network voert u het subnet van de FortiGate in. Sla vervolgens het profiel op.

**Network**

---

Network

	Local Network	Subnet Mask	Remote Network	Subnet Mask
	<input type="text" value="192.168.228.0"/>	<input type="text" value="255.255.255.0/24"/> ▾	<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0/24"/> ▾

Routing/NAT Mode  Routing  NAT

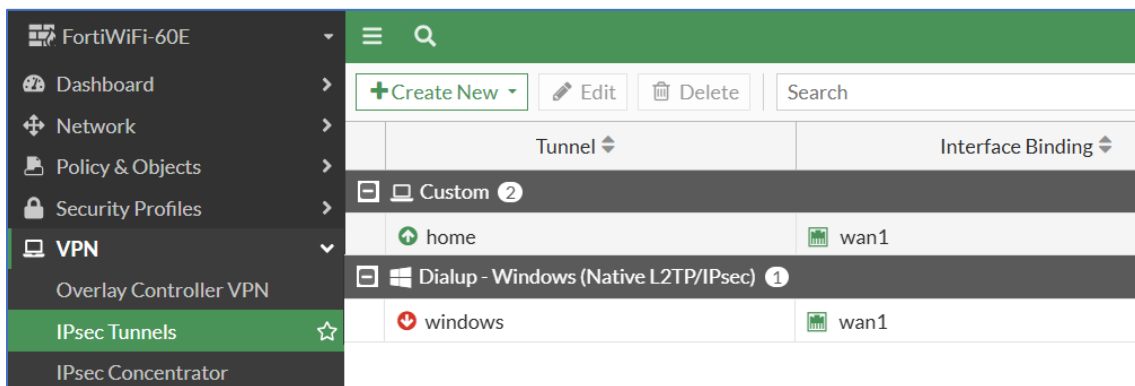
Translate Local Network

More Remote Subnets  ▾

## Configuratie Fortigate

### IPsec VPN tunnel aanmaken

Log eerst in op uw Fortigate. Navigeer naar VPN > IPsec Tunnels en kies Create New. Geef de tunnel een herkenbare naam, bijvoorbeeld 'VPN-DrayTek'. Selecteer Custom als template en klik op Next.



### Netwerkinstellingen configureren

Selecteer de juiste IP-versie. Wanneer de DrayTek-router een dynamisch WAN-adres gebruikt, kiest u bij Remote Gateway voor Dialup User. Selecteer vervolgens de WAN-interface waarop de VPN actief moet worden.

New VPN Tunnel

Name

Comments  0/255

Enable IPsec Interface Mode

**Network**

IP Version

Remote Gateway

Interface

Local Gateway

Mode Config

NAT Traversal

Dead Peer Detection

DPD retry count

DPD retry interval  s

Forward Error Correction Egress  Ingress

## IKE Phase 1 configureren

Selecteer IKEv2 als protocolversie. Kies Pre-Shared Key als authenticatiemethode en voer de afgesproken sleutel in. Configureer de Peer ID zodat deze overeenkomt met de Local ID op de DrayTek. Stel de Key Lifetime in op 28800 seconden.

<b>Authentication</b>	
Method	Pre-shared Key
Pre-shared Key	••••••••
<b>IKE</b>	
Version	1 2
<b>Peer Options</b>	
Accept Types	Specific peer ID
Peer ID	vigor2928
<b>Phase 1 Proposal</b>	<input type="button" value="Add"/>
Encryption	AES128
Authentication	SHA256 <input type="checkbox"/>
Encryption	AES256
Authentication	SHA256 <input type="checkbox"/>
Encryption	AES128GCM
PRF	PRFSHA256 <input type="checkbox"/>
Encryption	AES256GCM
PRF	PRFSHA384 <input type="checkbox"/>
Encryption	CHACHA20P
PRF	PRFSHA256 <input type="checkbox"/>
Diffie-Hellman Groups	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1
Key Lifetime (seconds)	28800
Local ID	

## IKE Phase 2 configureren

Voer het lokale subnet van de FortiGate in als Local Address en het subnet van de DrayTek als Remote Address. Open de Advanced-instellingen en configureer de gewenste encryptie- en authenticatiealgoritmen. Stel de Key Lifetime in op 3600 seconden.

### Edit Phase 2

Name: vigor2928

Comments:

Local Address: Subnet 192.168.1.0/255.255.25

Remote Address: Subnet 192.168.228.0/255.255.

**Advanced...**

Phase 2 Proposal

Encryption	AES128	Authentication	SHA1	<input type="button" value="X"/>
Encryption	AES256	Authentication	SHA1	<input type="button" value="X"/>
Encryption	AES128	Authentication	SHA256	<input type="button" value="X"/>
Encryption	AES256	Authentication	SHA256	<input type="button" value="X"/>

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

<input type="checkbox"/>	32	<input type="checkbox"/>	31	<input type="checkbox"/>	30	<input type="checkbox"/>	29	<input type="checkbox"/>	28	<input type="checkbox"/>	27
<input type="checkbox"/>	21	<input type="checkbox"/>	20	<input type="checkbox"/>	19	<input type="checkbox"/>	18	<input type="checkbox"/>	17	<input type="checkbox"/>	16
<input type="checkbox"/>	15	<input checked="" type="checkbox"/>	14	<input checked="" type="checkbox"/>	5	<input type="checkbox"/>	2	<input type="checkbox"/>	1		

Local Port: All

Remote Port: All

Protocol: All

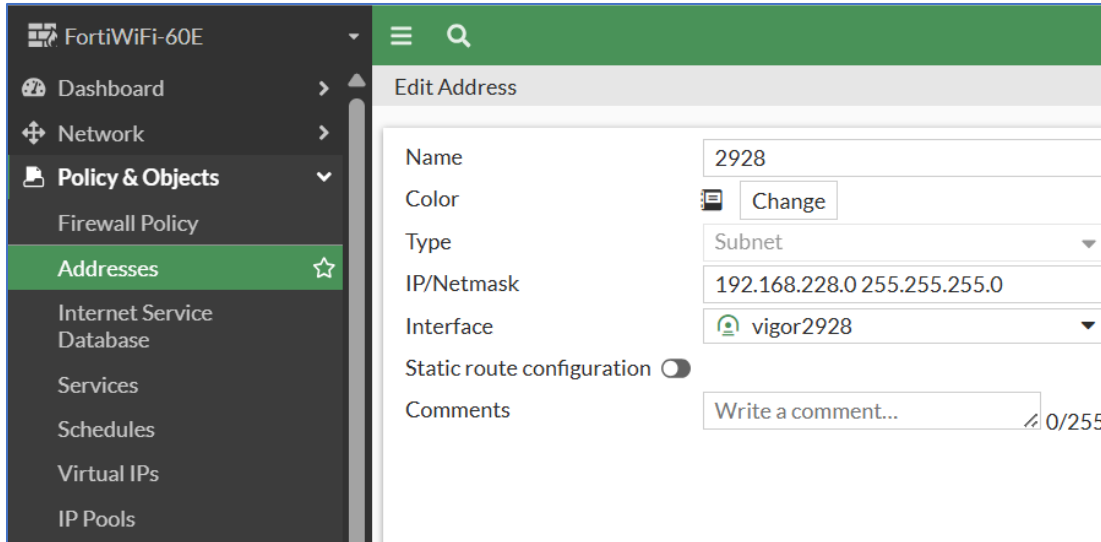
Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 3600

## Address Object aanmaken

Ga naar Policy & Objects > Addresses en maak een nieuw object aan voor het LAN-subnet van de DrayTek. Koppel dit object aan de eerder aangemaakte IPsec-tunnel.

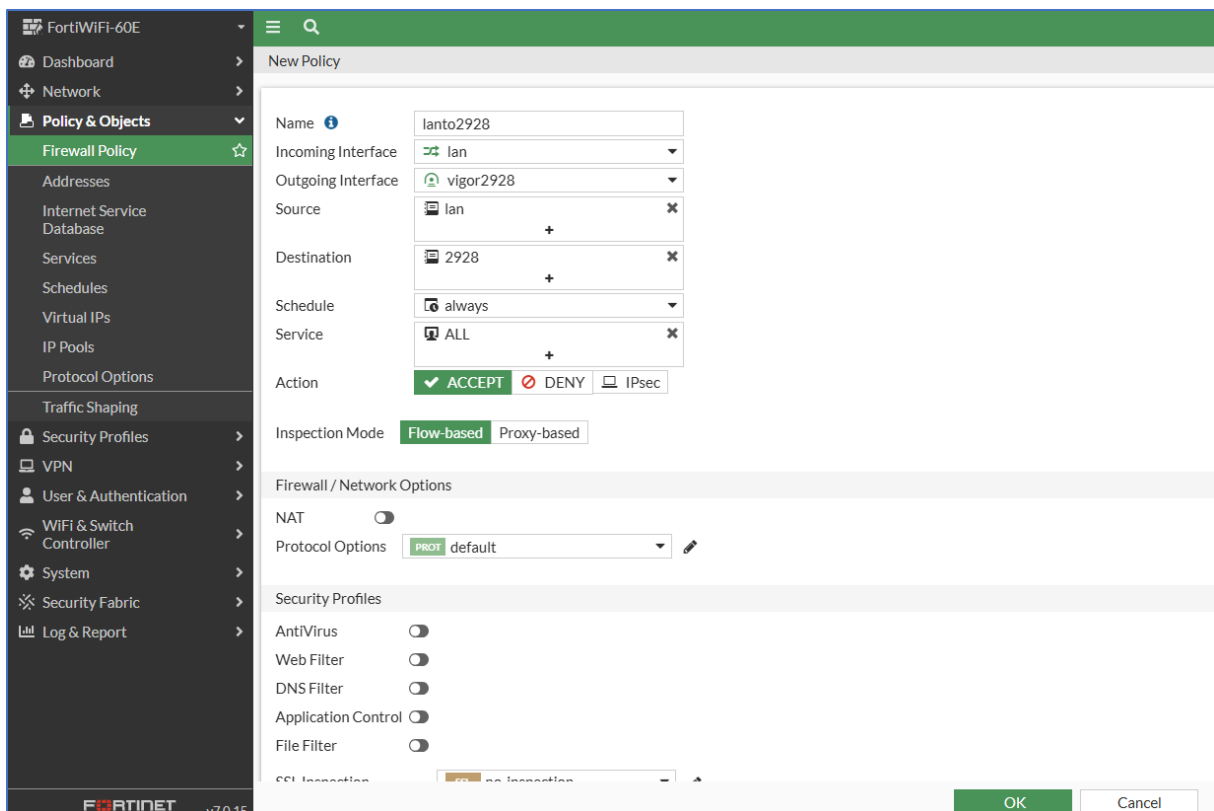


The screenshot shows the 'Edit Address' configuration page in the FortiWiFi-60E web interface. The left sidebar is expanded to 'Policy & Objects' > 'Addresses'. The main content area shows the following configuration:

- Name: 2928
- Color: Change
- Type: Subnet
- IP/Netmask: 192.168.228.0 255.255.255.0
- Interface: vigor2928
- Static route configuration:
- Comments: Write a comment... (0/255)

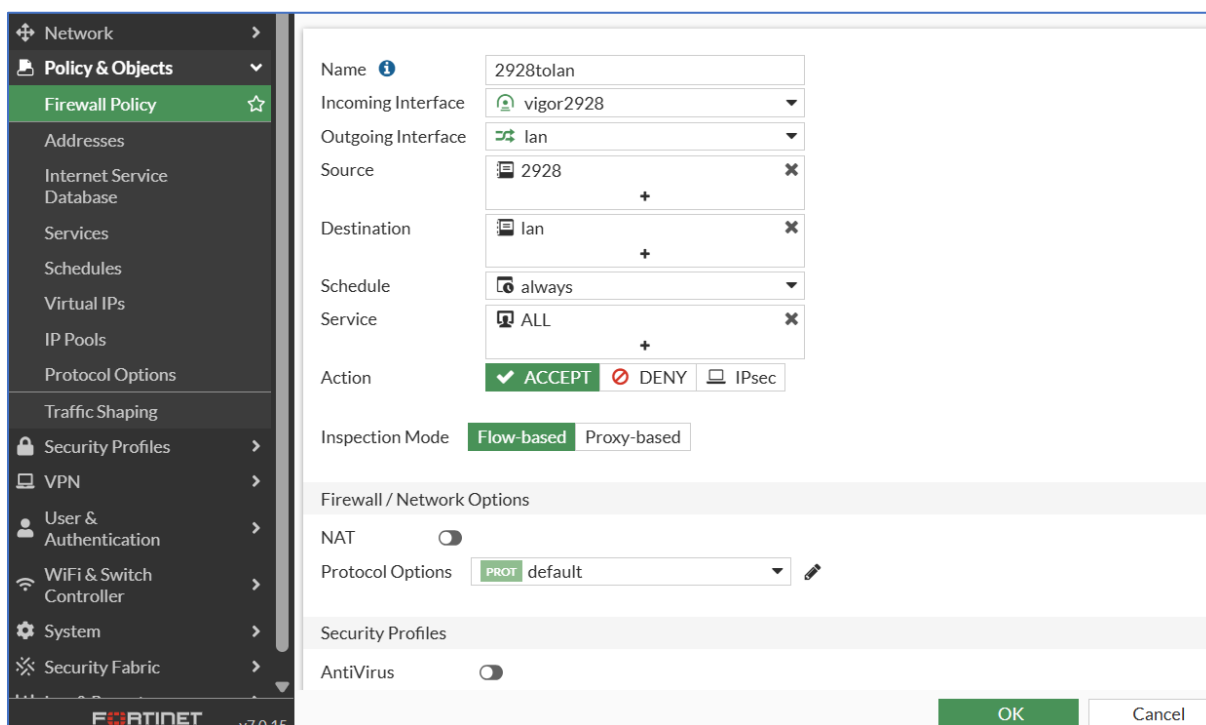
## Firewall policies configureren

Maak twee firewallregels aan: één voor verkeer van het FortiGate LAN naar het DrayTek LAN en één voor verkeer in de tegenovergestelde richting. Schakel NAT uit voor beide regels. Controleer de volgorde van de policies zodat VPN-verkeer eerder wordt verwerkt dan algemene internetregels.



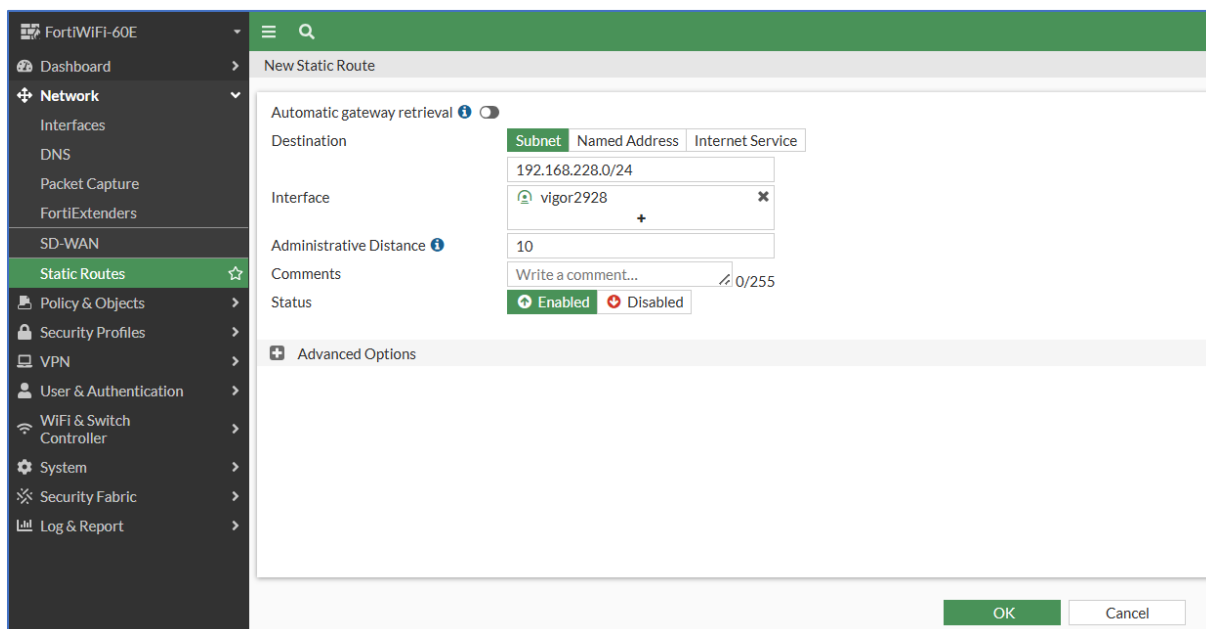
The screenshot shows the 'New Policy' configuration page in the FortiWiFi-60E web interface. The left sidebar is expanded to 'Policy & Objects' > 'Firewall Policy'. The main content area shows the following configuration:

- Name: lanto2928
- Incoming Interface: lan
- Outgoing Interface: vigor2928
- Source: lan
- Destination: 2928
- Schedule: always
- Service: ALL
- Action:  ACCEPT  DENY  IPsec
- Inspection Mode: Flow-based
- Firewall / Network Options:
  - NAT:
  - Protocol Options: PROT default
- Security Profiles:
  - AntiVirus:
  - Web Filter:
  - DNS Filter:
  - Application Control:
  - File Filter:



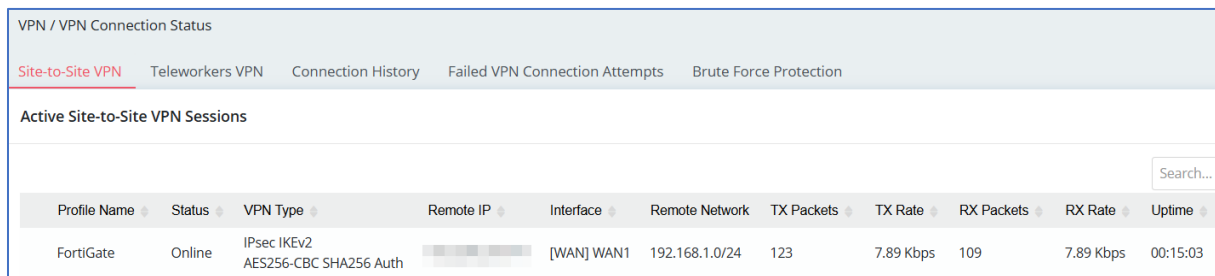
## Static Route toevoegen

Ga naar Network > Static Routes en voeg een route toe naar het subnet van de DrayTek. Selecteer hierbij de IPsec-tunnel als uitgaand interface.



## VPN status controleren

Wanneer Dial-Out Mode op Always On staat, probeert de router direct een verbinding op te bouwen. Controleer de status via VPN / VPN Connection Status. De tunnel moet zichtbaar zijn als Connected.



Profile Name	Status	VPN Type	Remote IP	Interface	Remote Network	TX Packets	TX Rate	RX Packets	RX Rate	Uptime
FortiGate	Online	IPsec IKEv2 AES256-CBC SHA256 Auth		[WAN] WAN1	192.168.1.0/24	123	7.89 Kbps	109	7.89 Kbps	00:15:03

## Veelvoorkomende problemen en oplossingen

VPN komt niet online:

- Controleer de Pre-Shared Key.
- Controleer Peer ID en Local ID.
- Controleer of IKEv2 aan beide zijden is geselecteerd.

Tunnel is actief maar verkeer werkt niet:

- Controleer firewallregels.
- Controleer de statische routes.
- Controleer de opgegeven subnetten in Phase 2.

Tunnel valt regelmatig weg:

- Controleer internetverbindingen.
- Controleer de Key Lifetime instellingen.
- Controleer of NAT-Traversal correct functioneert.

**Reservation**

We reserve the right to modify this and other documentation without the obligation to inform users. Images and screenshots may differ.

**Copyright statement**

© 2026 DrayTek

All rights reserved. Nothing from this publication may be reproduced, stored in an automated database, and/or made public in any form or manner, either electronically, mechanically, by photocopying, recording, or in any other way without the prior written permission of the publisher. Despite all the care given to the compilation of this manual, neither the manufacturer, the author, nor the distributor can accept liability for damage resulting from any errors in this publication.

**Trademarks**

All trademarks and registered trademarks are the property of their respective owners.