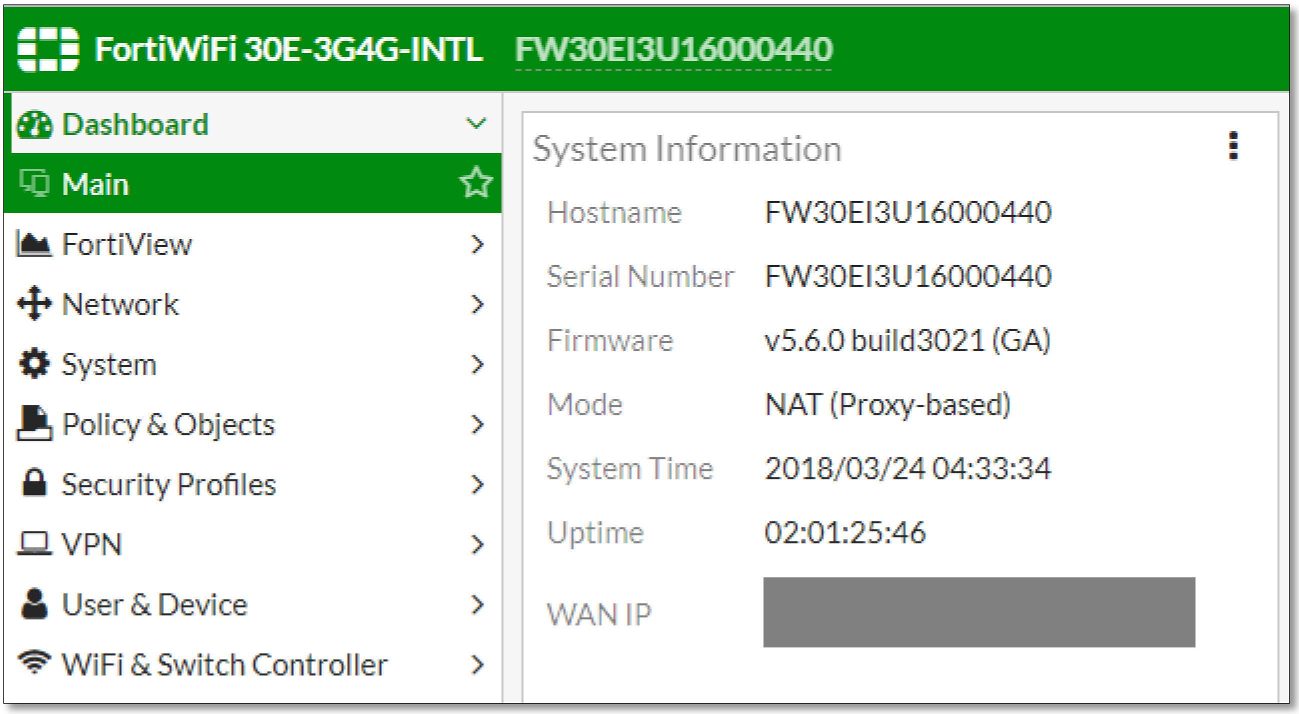
Setting up IPSec RUT9 with Fortigate

Setup was made with a following Fortigate build:



System Information

Hostname FW30EI3U16000440

Serial Number FW30EI3U16000440

Firmware v5.6.0 build3021 (GA)

Mode NAT (Proxy-based)

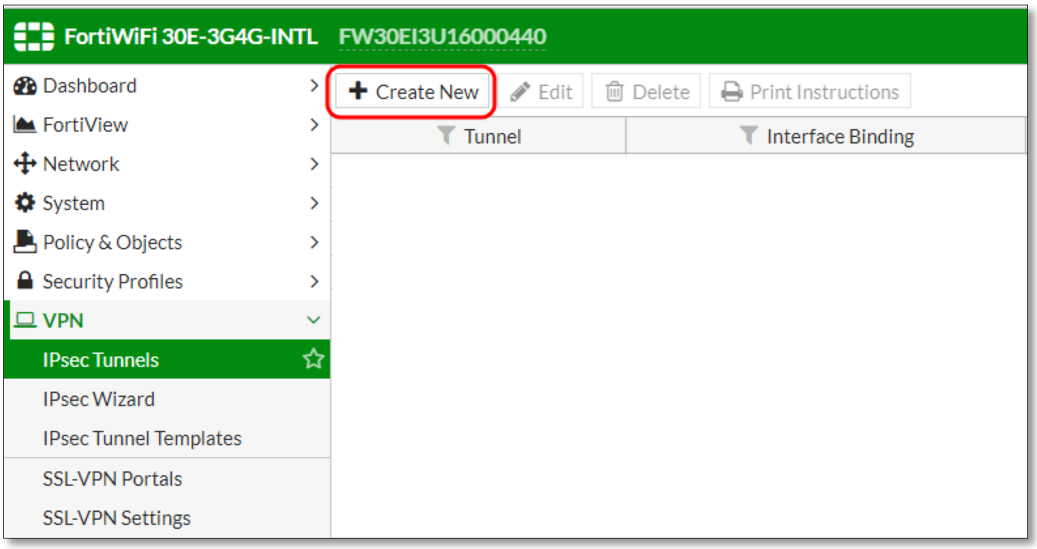
System Time 2018/03/24 04:33:34

Uptime 02:01:25:46

WAN IP [redacted]

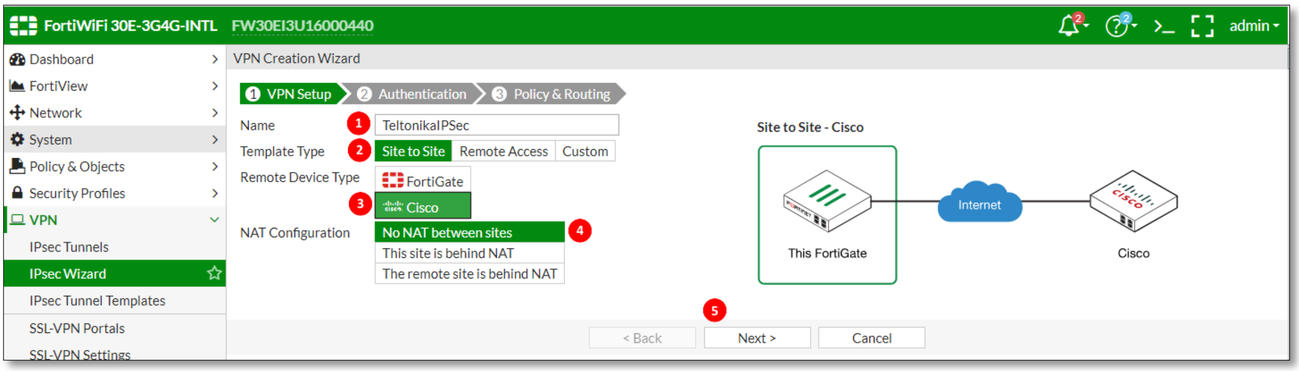
Fortigate VPN Wizard setup

Create a new IPSec tunnel via **VPN -> IPSec Tunnels -> (+)Create New**



IPsec Wizard will open, **STEP 1**, select:

1. give this tunnel a **Name** (*it will be important in configuration*);
2. Site to Site type;
3. Remote device as “Cisco”;
4. No NAT between sites (this was the testing setup);
5. hit Next >



1 Name: TeltonikaIPSec

2 Template Type: Site to Site | Remote Access | Custom

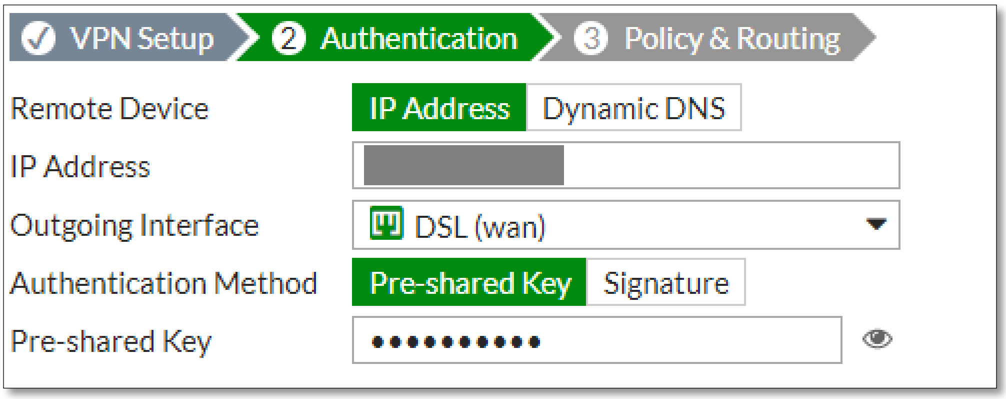
Remote Device Type: FortiGate | 3 Cisco

NAT Configuration: 4 No NAT between sites | This site is behind NAT | The remote site is behind NAT

5 Next >

On **STEP 2** configure:

1. IP address of a Remote Device – in this case – Teltonika RUT950;
2. select Outgoing Interface to the one that Fortigate will be using to communicate with Remote Device; In this case it is Wired WAN (DSL wan);
3. enter a pre-shared key (**same key will be used on RUT950**);
4. hit Next >



Remote Device: [✓ IP Address] Dynamic DNS

IP Address: [redacted]

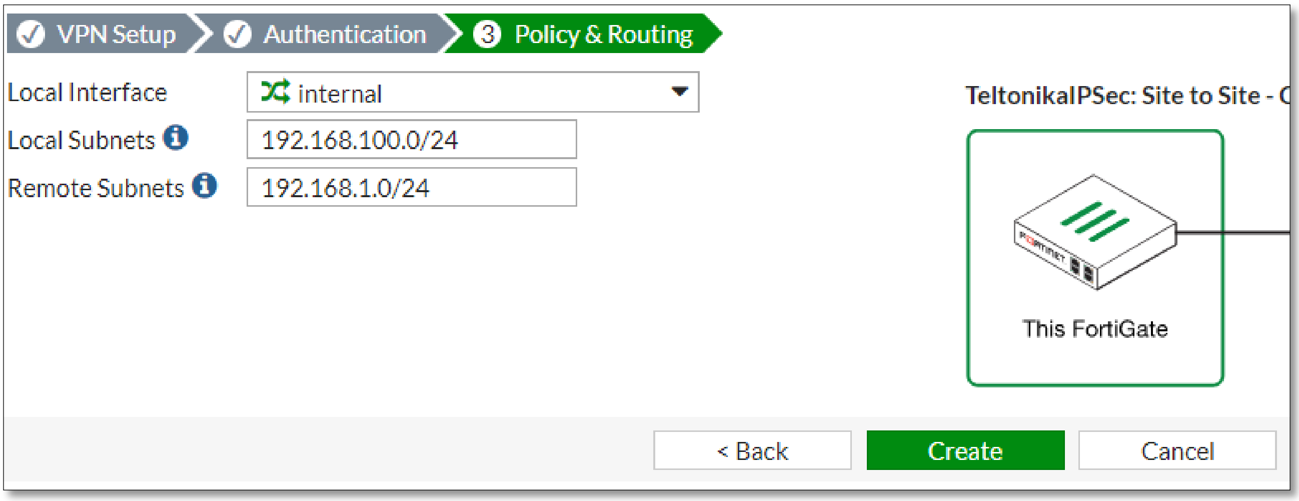
Outgoing Interface: DSL (wan)

Authentication Method: [✓ Pre-shared Key] Signature

Pre-shared Key: ●●●●●●●●●●

On **STEP 3** configure:

1. select **Internal** (Fortigate's Eth LAN) interface;
2. **Local Subnets** field will populate automatically; if not – simply enter Fortigate's LAN subnet;
3. enter RUT950's LAN subnet to **Remote Subnets** field;
4. hit **Create**.

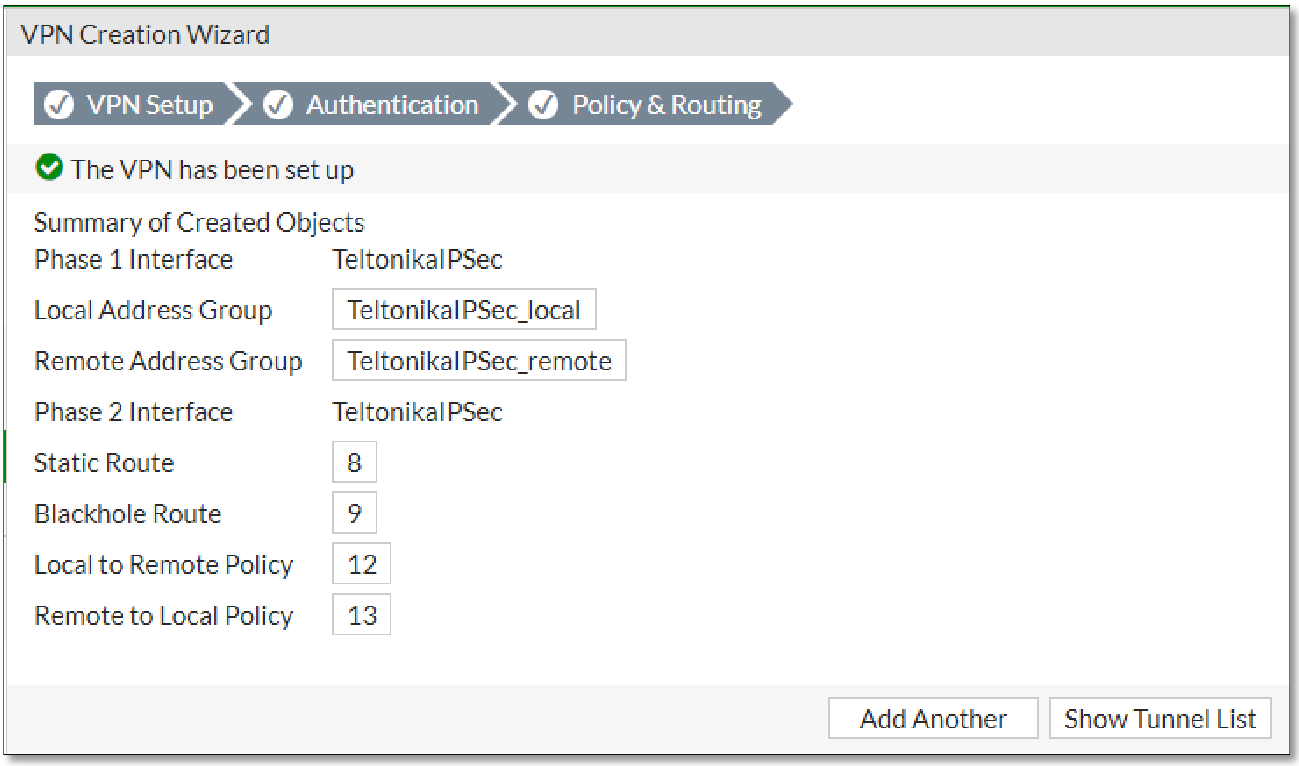


Local Interface: internal

Local Subnets: 192.168.100.0/24

Remote Subnets: 192.168.1.0/24

Review/Change config settings right after tunnel creation by selecting each created parameter individually, or go to **Show Tunnel List**:



VPN Creation Wizard

✓ The VPN has been set up

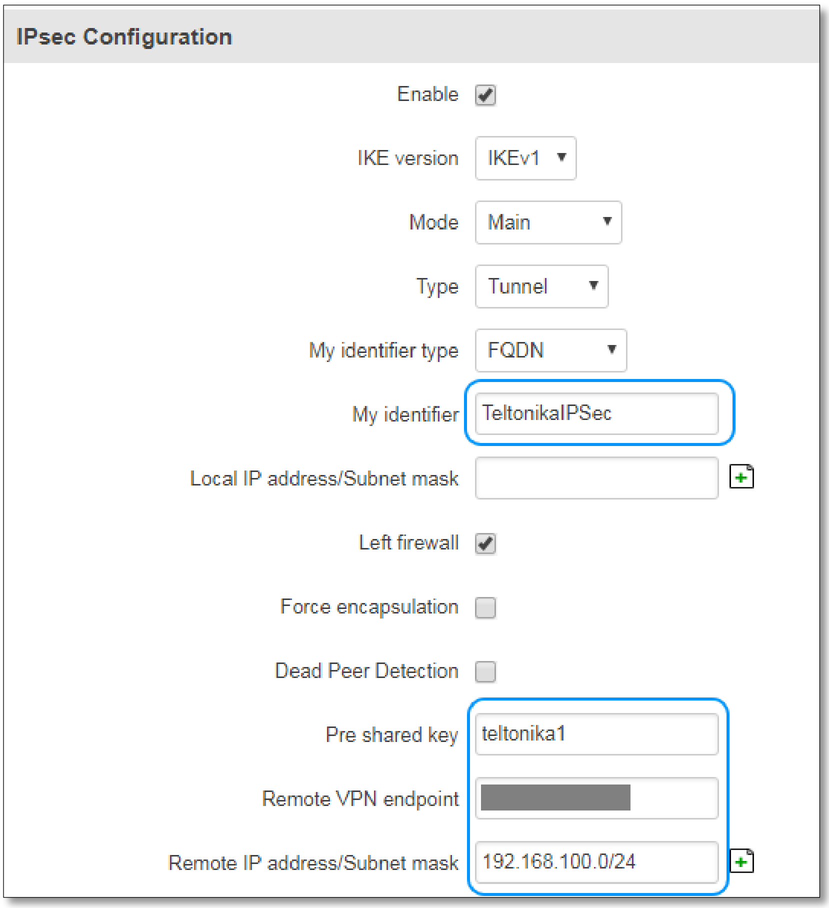
Summary of Created Objects

Phase 1 Interface	TeltonikaIPSec
Local Address Group	TeltonikaIPSec_local
Remote Address Group	TeltonikaIPSec_remote
Phase 2 Interface	TeltonikaIPSec
Static Route	8
Blackhole Route	9
Local to Remote Policy	12
Remote to Local Policy	13

Configuring RUT950

Setup main settings (everything not mentioned in items below can be left as Default):

1. **My identifier** ought to be set to **TeltonikaIPSec** (***VPN tunnel Name on Fortigate side***);
2. **Pre-sared key** set to the same as on Fortigate (**STEP 2** of tunnel wizard);
3. **Remote VPN endpoint** – Fortigate's WAN IP;
4. **Remote IP/Subnet mask** – Fortigate's LAN (internal interface);

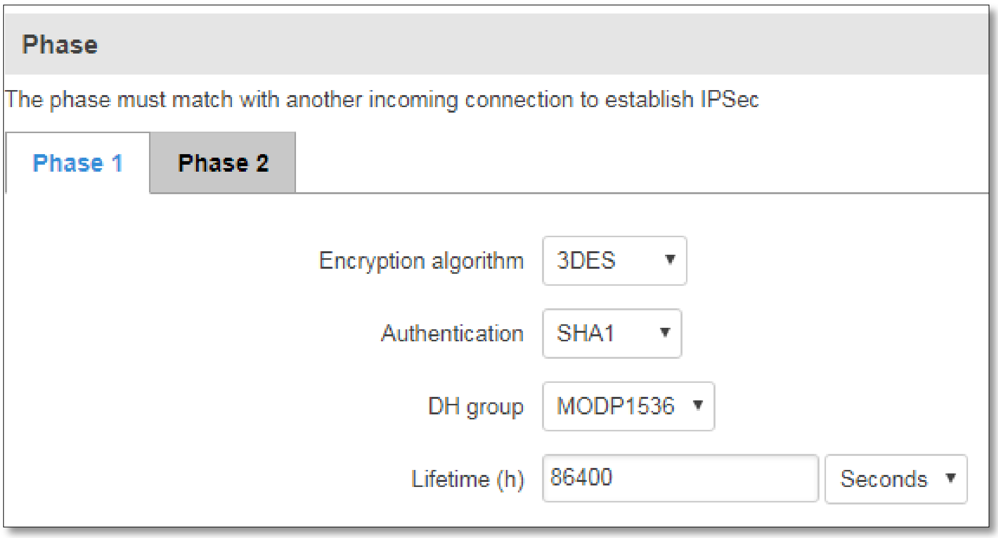


IPsec Configuration

Enable	☑
IKE version	IKEv1 ▾
Mode	Main ▾
Type	Tunnel ▾
My identifier type	FQDN ▾
My identifier	TeltonikaIPSec
Local IP address/Subnet mask	
Left firewall	☑
Force encapsulation	☐
Dead Peer Detection	☐
Pre shared key	teltonika1
Remote VPN endpoint	[redacted]
Remote IP address/Subnet mask	192.168.100.0/24

By default, "Cisco template" uses following **Phase1** and **Phase2** settings, configure RUT9XX accordingly:

1. **Phase 1**

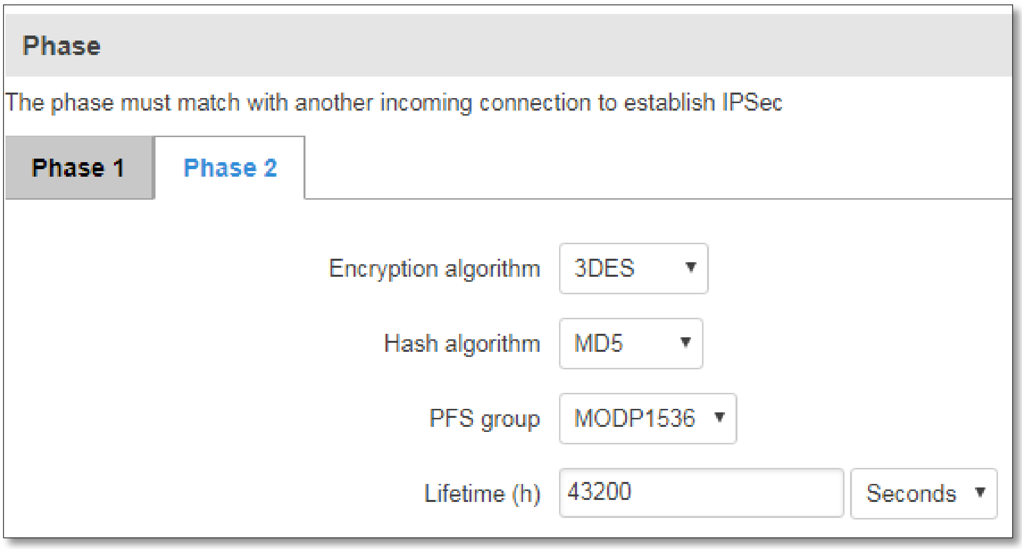


Phase

The phase must match with another incoming connection to establish IPSec

Encryption algorithm	3DES ▾
Authentication	SHA1 ▾
DH group	MODP1536 ▾
Lifetime (h)	86400 Seconds ▾

2. **Phase 2**



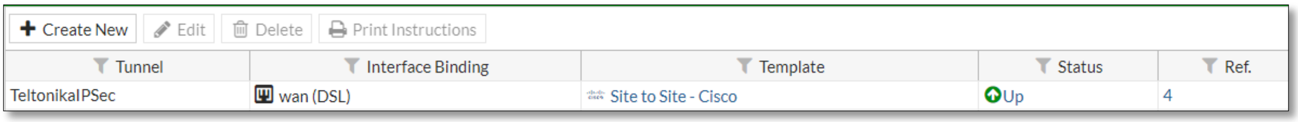
Phase

The phase must match with another incoming connection to establish IPSec

Phase 1	Phase 2

Encryption algorithm	3DES
Hash algorithm	MD5
PFS group	MODP1536
Lifetime (h)	43200 Seconds

Once everything is set up – check tunnel status on Fortigate under **VPN -> IPSec Tunnels**:



Tunnel	Interface Binding	Template	Status	Ref.
TeltonikaIPSec	wan (DSL)	Site to Site - Cisco	Up	4

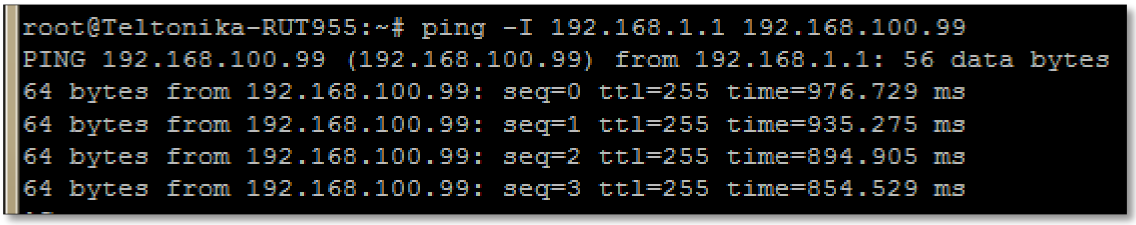
Test the tunnel

Login to Teltonika's SSH:

User: root

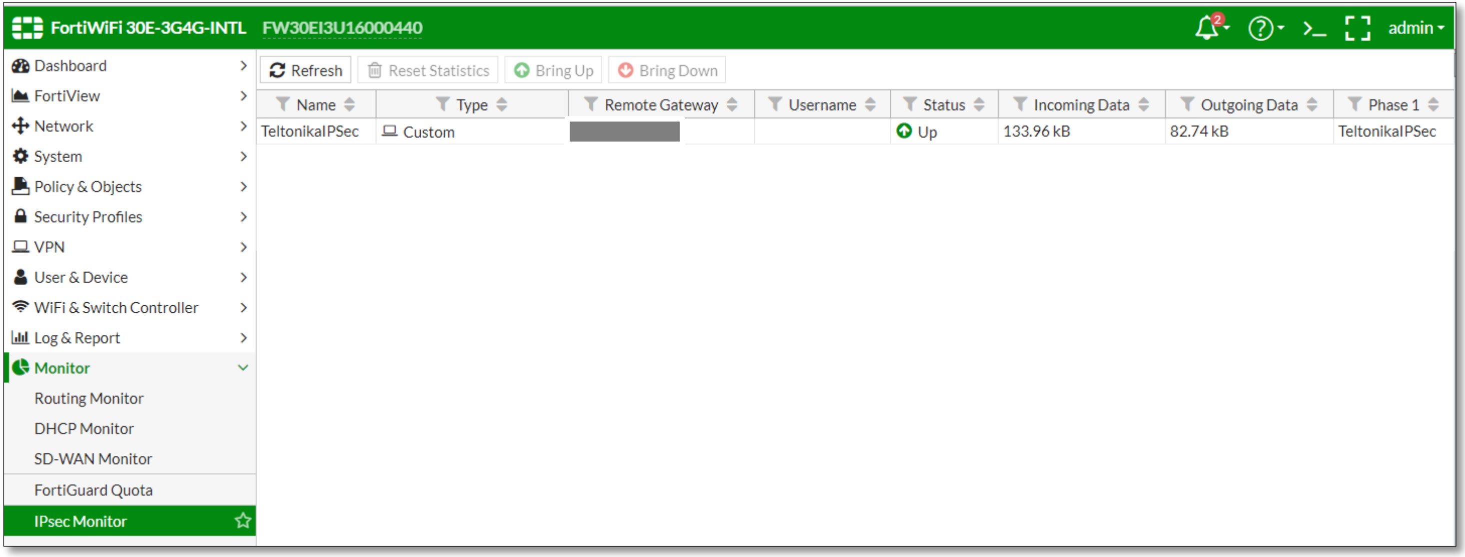
Pass: admin01 (or new WebUI password)

Issue **PING** from router's LAN interface to Fortigate's LAN interface with **ping -I 192.168.1.1 192.168.100.99**



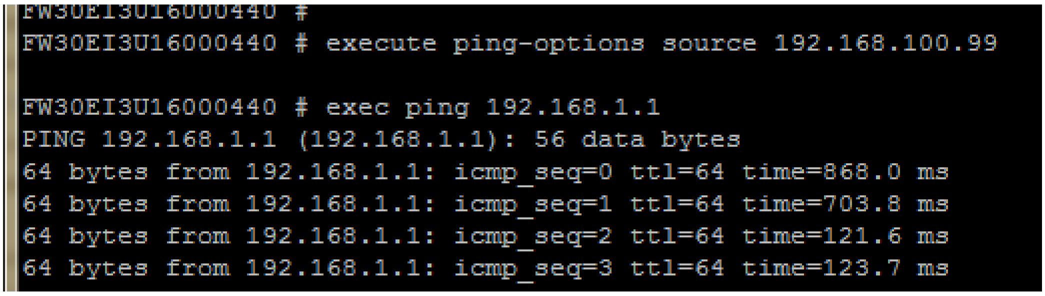
```
root@Teltonika-RUT955:~# ping -I 192.168.1.1 192.168.100.99
PING 192.168.100.99 (192.168.100.99) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.100.99: seq=0 ttl=255 time=976.729 ms
64 bytes from 192.168.100.99: seq=1 ttl=255 time=935.275 ms
64 bytes from 192.168.100.99: seq=2 ttl=255 time=894.905 ms
64 bytes from 192.168.100.99: seq=3 ttl=255 time=854.529 ms
```

From Fortigate – use **Monitor -> IPsec Monitor** menu (or via CLI):



Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 1
TeltonikaIPSec	Custom	[redacted]		Up	133.96 kB	82.74 kB	TeltonikaIPSec

Via CLI:

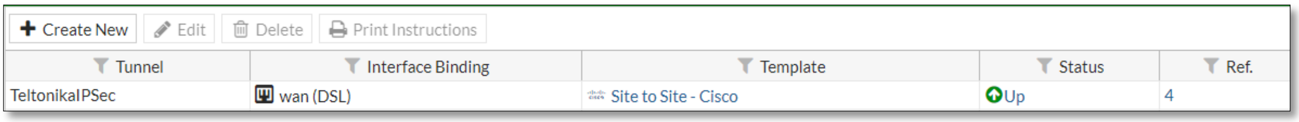


```
FW30EI3U16000440 #
FW30EI3U16000440 # execute ping-options source 192.168.100.99

FW30EI3U16000440 # exec ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=868.0 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=703.8 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=121.6 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=123.7 ms
```

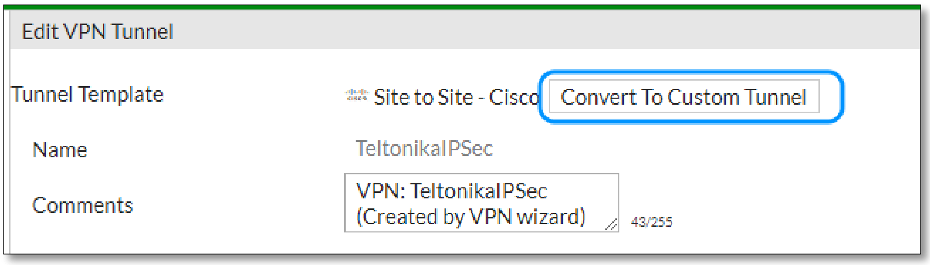
OPTIONAL: Configuring created Tunnel (Phase1 and Phase1)

Go to **VPN -> IPsec Tunnels** and double click on created tunnel:



Tunnel	Interface Binding	Template	Status	Ref.
TeltonikaIPSec	wan (DSL)	Site to Site - Cisco	Up	4

Hit **Convert To Custom Tunnel**:



Edit VPN Tunnel

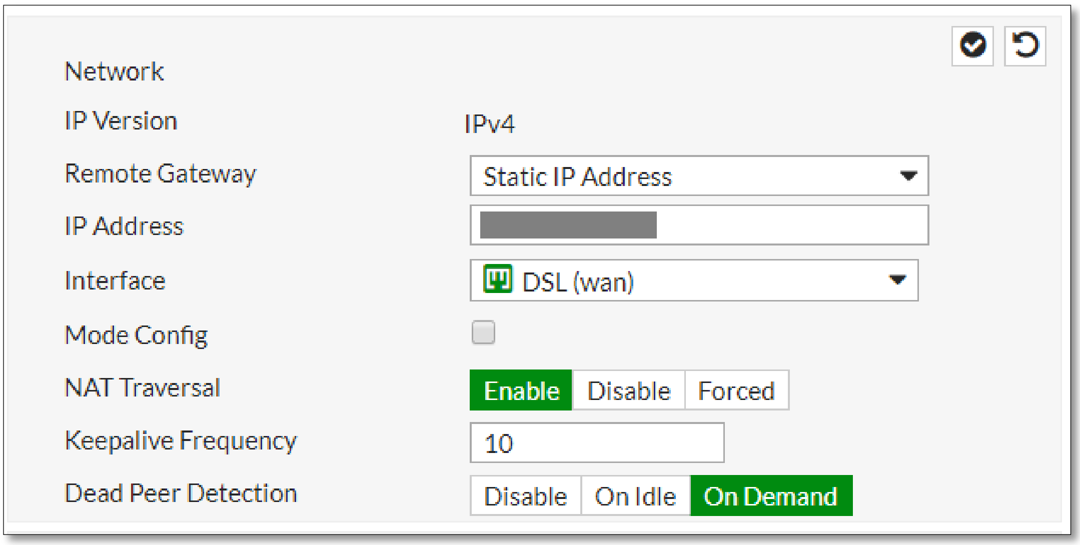
Tunnel Template: Site to Site - Cisco

Name: TeltonikaIPSec

Comments: VPN: TeltonikaIPSec (Created by VPN wizard) 43/255

You will now have full control of IPSec tunnel settings:

1. **Network** settings:



Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: [redacted]

Interface: DSL (wan)

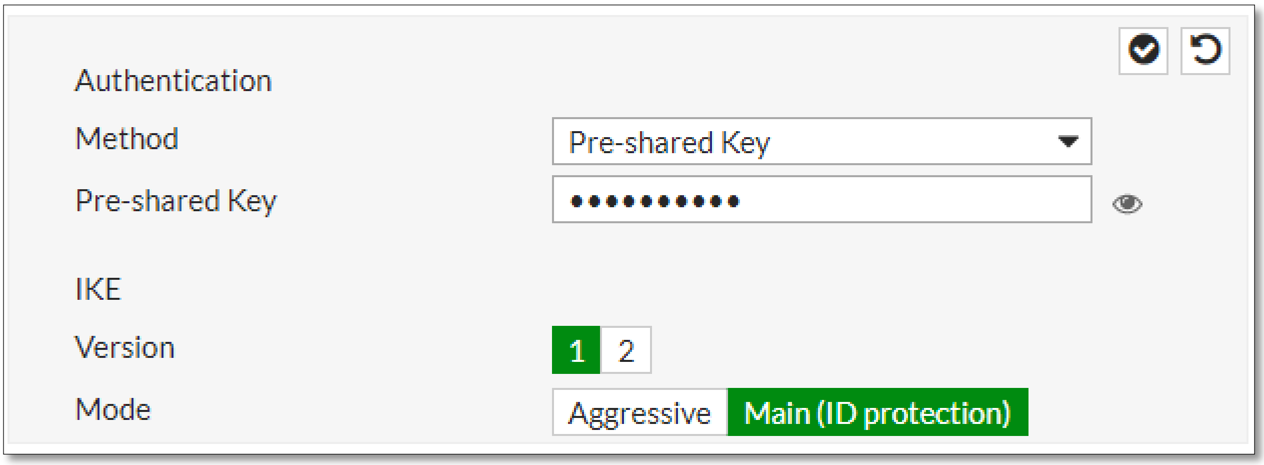
Mode Config: □

NAT Traversal: [✓ Enable] Disable Forced

Keepalive Frequency: 10

Dead Peer Detection: Disable On Idle [✓ On Demand]

2. **Authentication** settings:



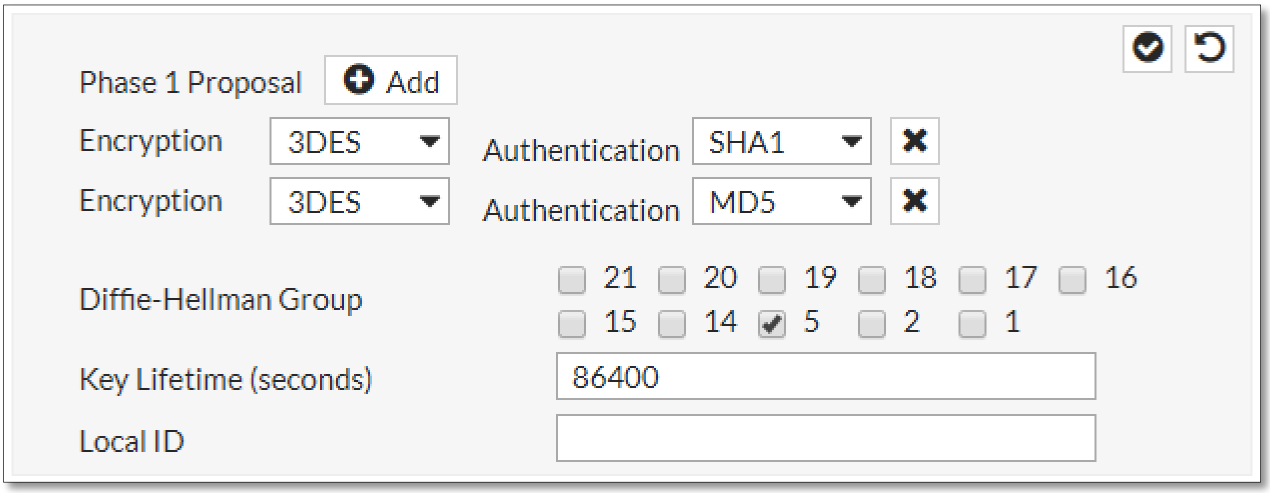
Authentication

Method	Pre-shared Key
Pre-shared Key	●●●●●●●●●●

IKE

Version	[✓ 1] 2
Mode	Aggressive [✓ Main (ID protection)]

3. **Phase 1** settings:



Phase 1 Proposal

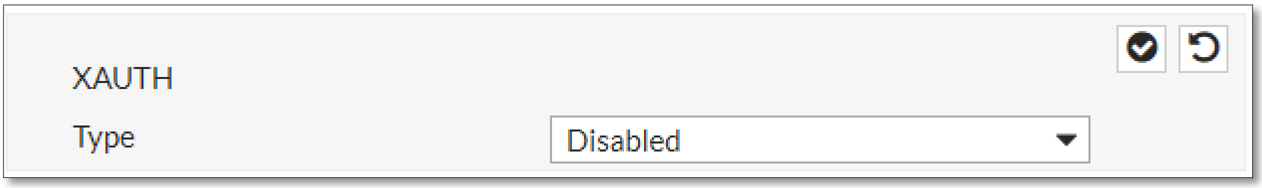
Encryption	3DES	Authentication	SHA1
Encryption	3DES	Authentication	MD5

Diffie-Hellman Group: □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1

Key Lifetime (seconds): 86400

Local ID:

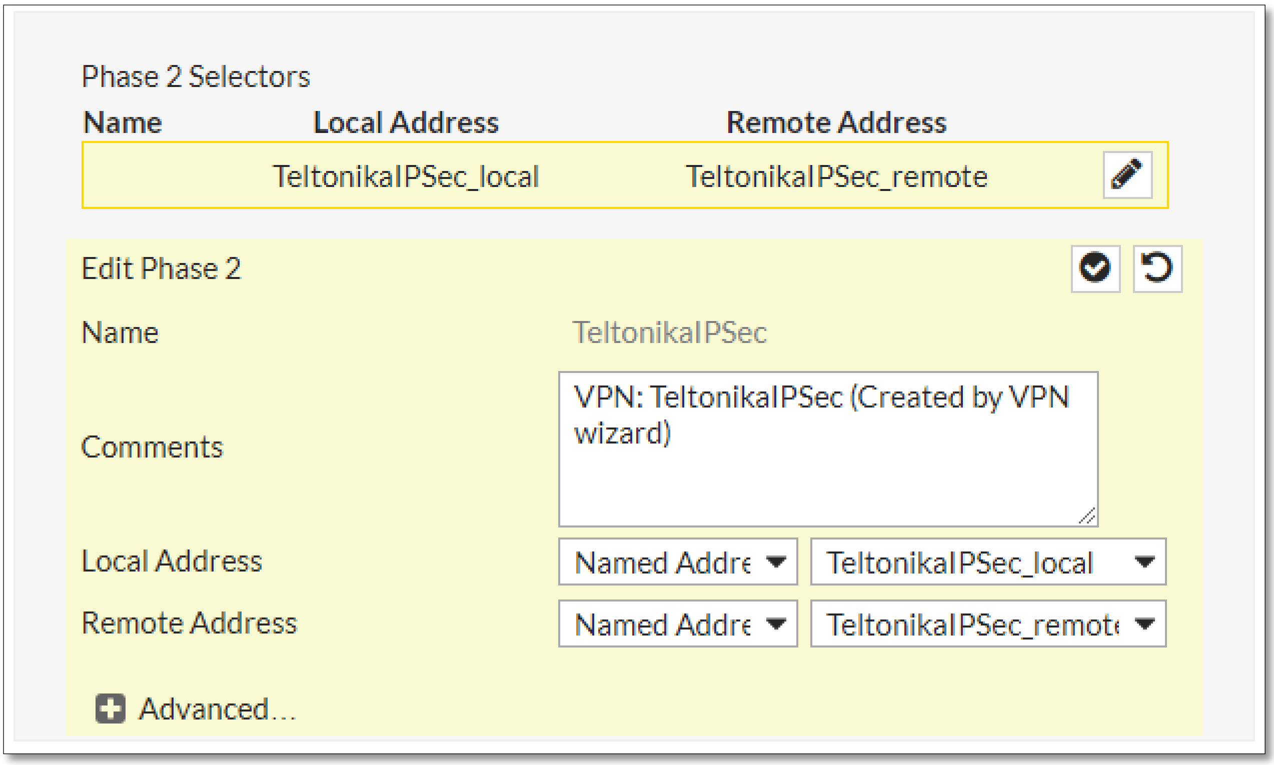
4. **XAUTH** settings (note: not supported by Teltonika):



XAUTH

Type: Disabled

5. **Phase 2** settings:



Phase 2 Selectors

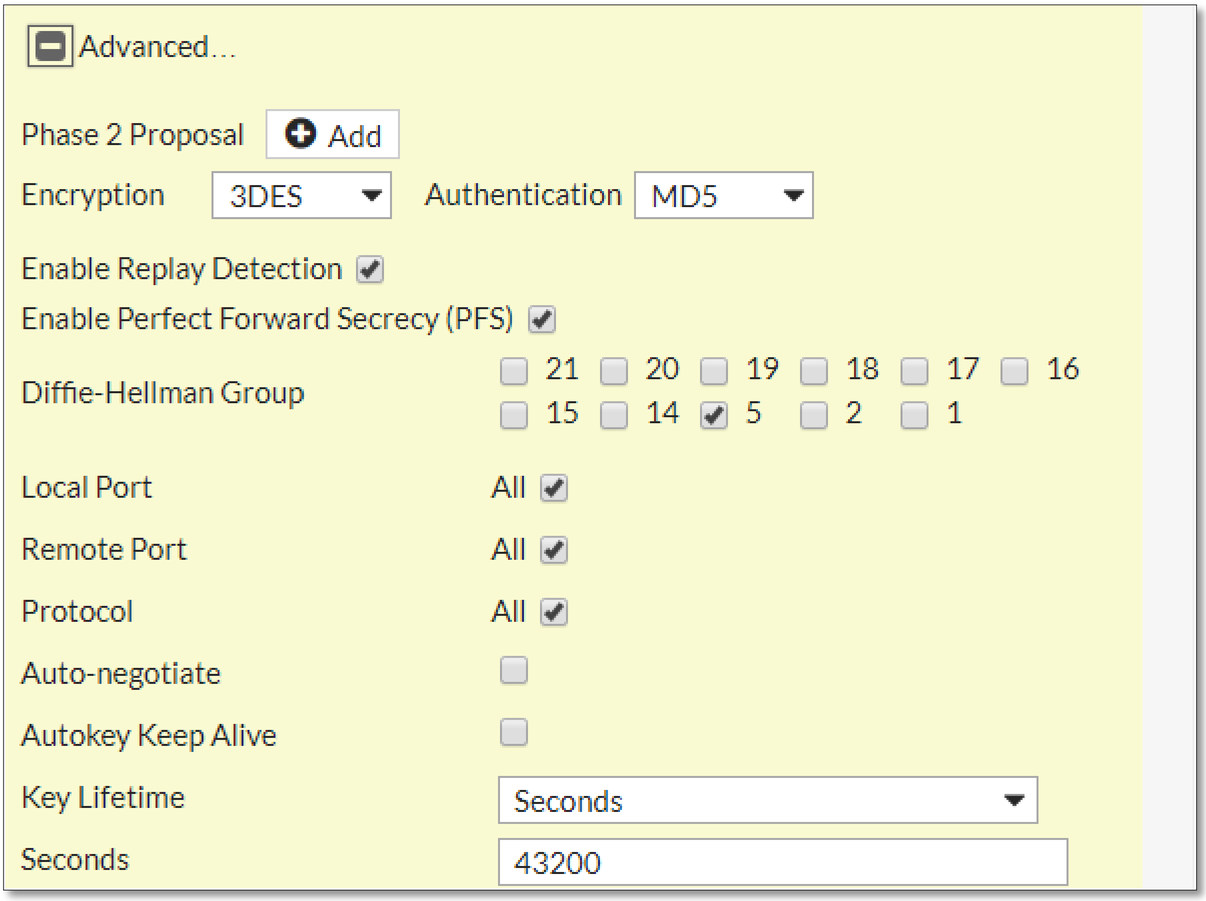
Name	Local Address	Remote Address
	TeltonikaIPSec_local	TeltonikaIPSec_remote

Edit Phase 2

Name	TeltonikaIPSec	
Comments	VPN: TeltonikaIPSec (Created by VPN wizard)	
Local Address	Named Addre	TeltonikaIPSec_local
Remote Address	Named Addre	TeltonikaIPSec_remot

Advanced...

6. And **Advanced Phase 2** settings (Proposal settings) under **[+]Advanced**:



Advanced...

Phase 2 Proposal [Add]

Encryption: 3DES Authentication: MD5

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group: □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1

Local Port: All ☑

Remote Port: All ☑

Protocol: All ☑

Auto-negotiate □

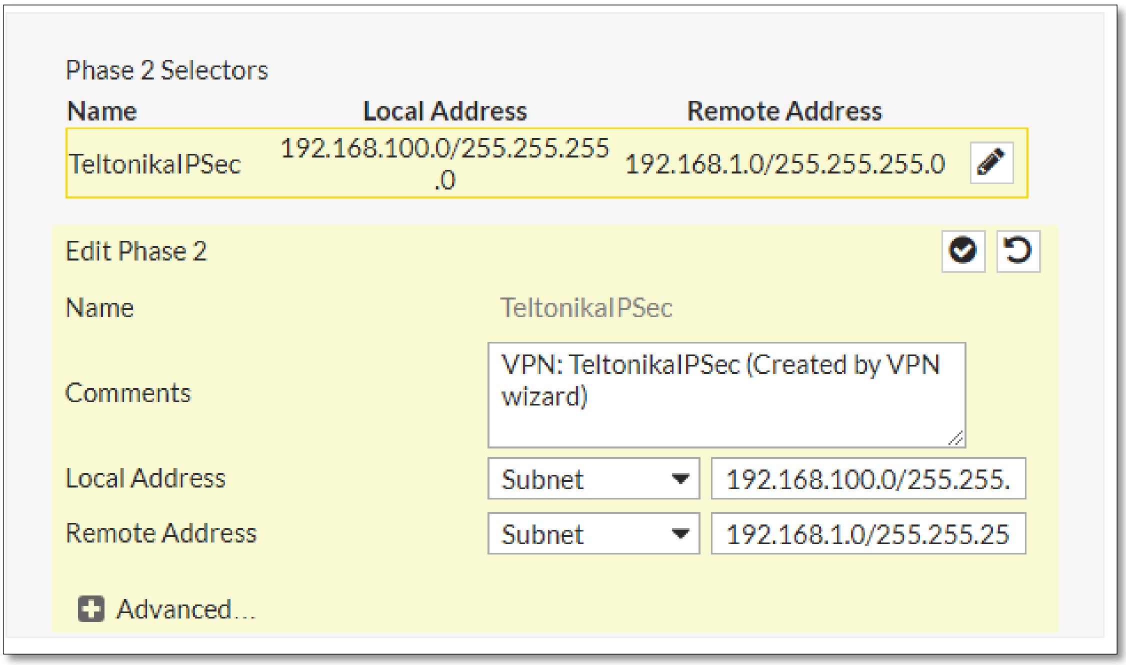
Autokey Keep Alive □

Key Lifetime: Seconds

Seconds: 43200

Note about Phase 2, Policies and Routes on Fortigate

Local and Remote addresses can be selected as **Subnet** if so desired:



Phase 2 Selectors

Name	Local Address	Remote Address
TeltonikaIPSec	192.168.100.0/255.255.255.0	192.168.1.0/255.255.255.0

Edit Phase 2

Name: TeltonikaIPSec

Comments: VPN: TeltonikaIPSec (Created by VPN wizard)

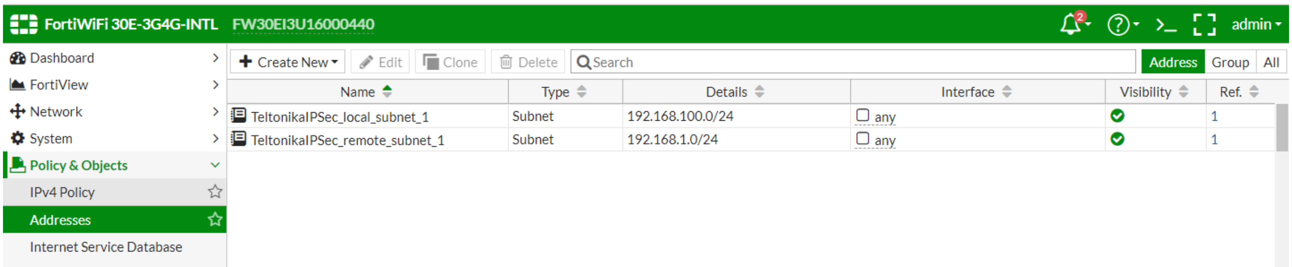
Local Address: Subnet 192.168.100.0/255.255.

Remote Address: Subnet 192.168.1.0/255.255.25

Advanced...

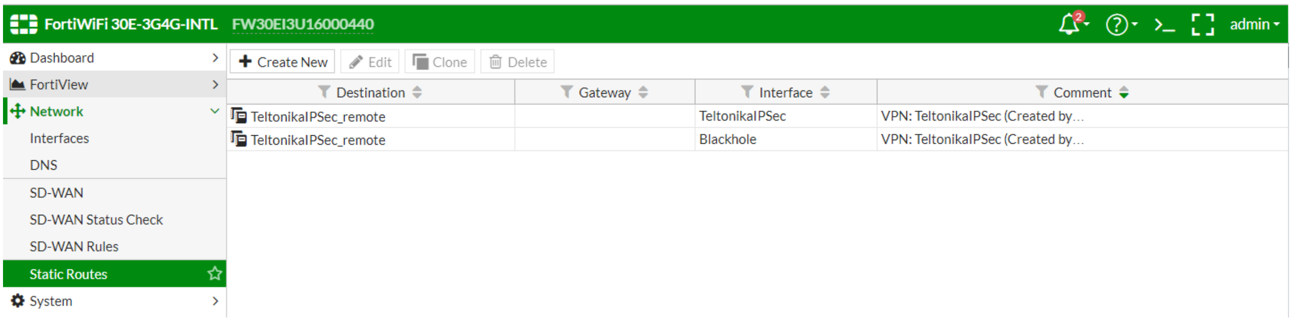
When creating tunnel with Cisco template, **Named Addresses**: **TeltonikaIPSec_local** and **TeltonikaIPSec_remote** are created automatically. Their respective policies can be found under:

Policy & Objects -> Addresses menu:



Name	Type	Details	Interface	Visibility	Ref.
TeltonikaIPSec_local_subnet_1	Subnet	192.168.100.0/24	□ any	✓	1
TeltonikaIPSec_remote_subnet_1	Subnet	192.168.1.0/24	□ any	✓	1

And respectively created routes found at **Network -> Static Routes** menu:



Destination	Gateway	Interface	Comment
TeltonikaIPSec_remote		TeltonikaIPSec	VPN: TeltonikaIPSec (Created by...
TeltonikaIPSec_remote		Blackhole	VPN: TeltonikaIPSec (Created by...