Setting up IPSec RUT9 with Fortigate

Fortigate VPN Wizard setup	2
Configuring RUT950	5
OPTIONAL: Configuring created Tunnel (Phase1 and Phase1)	7
Note about Phase 2, Policies and Routes on Fortigate	10

Setup was made with a following Fortigate build:

FortiWiFi 30E-3G4G-IN	πL	FW30EI3U1600	00440	
🚯 Dashboard	~	System Inform	nation	:
😳 Main	☆		FW30EI3U16000440	-
FortiView	>		FW30EI3U16000440	
Network	>			
🔅 System	>		v5.6.0 build3021 (GA)	
📕 Policy & Objects	>	Mode	NAT (Proxy-based)	
Security Profiles	>	System Time	2018/03/24 04:33:34	
U VPN	>	Uptime	02:01:25:46	
💄 User & Device	>	WAN IP		
🗢 WiFi & Switch Controller	>			



Fortigate VPN Wizard setup

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

FortiWiFi 30E-3G4C	-INTL FV	V30EI3U16000440	
Dashboard	> +	• Create New 🖋 Edit 🗎	Delete 🔒 Print Instructions
📥 FortiView	>	Tunnel	T Interface Binding
Network	>		
System	>		
Policy & Objects	>		
Security Profiles	>		
	~		
IPsec Tunnels	☆		
IPsec Wizard			
IPsec Tunnel Templates			
SSL-VPN Portals			
SSL-VPN Settings			

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 >

FortiWiFi 30E-3G4G-INTL	FW30EI3U16000440	↓ ² • ⑦• >_ [] admin•
n Dashboard	VPN Creation Wizard	
FortiView >	1 VPN Setup 2 2 Authentication 3 9 Policy & Routing	
+ Network	Name 1 TeltonikalPSec Site to Site - Cisco	
System	Template Type 2 Site to Site Remote Access Custom	
Policy & Objects	Remote Device Type FortiGate	\sim
Security Profiles	3 at Cisco	- Cisco
🖵 VPN 🗸 🗸	NAT Configuration No NAT between sites 4	11
IPsec Tunnels	This site is behind NAT This FortiGate	Cisco
IPsec Wizard 🕺	The remote site is behind NAT	
IPsec Tunnel Templates	6	
SSL-VPN Portals	< Back Next > Cancel	
SSI-VPN Settings		



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 >

VPN Setup 2 Authentication 3 Policy & Routing					
Remote Device	IP Address Dynamic DNS				
IP Address					
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.

VPN Setup	Authentication 🔰 3 Po	licy & Routing	
Local Interface	🔀 internal	-	TeltonikalPSec: Site to Site - 0
Local Subnets 🛈	192.168.100.0/24		
Remote Subnets 🕄	192.168.1.0/24		This FortiGate
		< Back	Create Cancel



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

VPN Creation Wizard					
VPN Setup 💙 🗸 A	\checkmark VPN Setup \checkmark \checkmark Authentication \checkmark \checkmark Policy & Routing				
The VPN has been set	up				
Summary of Created Obj Phase 1 Interface	ects TeltonikalPSec				
Local Address Group	TeltonikalPSec_local				
Remote Address Group	TeltonikalPSec_remote				
Phase 2 Interface	TeltonikalPSec				
Static Route	8				
Blackhole Route	9				
Local to Remote Policy	12				
Remote to Local Policy	13				
	Add Another Show Tunnel List				

Configuring RUT950

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

- 1. My identifier ought to be set to TeltonikalPSec (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 •
Туре	Tunnel •
My identifier type	FQDN •
My identifier	TeltonikalPSec
Local IP address/Subnet mask	+
Left firewall	
Force encapsulation	
Dead Peer Detection	
Pre shared key	teltonika1
Remote VPN endpoint	
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 mu	st match with a	another incoming connec	tion to establish IPSec	
Phase 1	Phase 2			
		Encryption algorithm	3DES V	
		Authentication	SHA1 V	
		DH group	MODP1536 •	
		Lifetime (h)	86400	Seconds 🔻

2. Phase 2

Phase			
The phase mu	st match with a	nother incoming connec	tion to establish IPSec
Phase 1	Phase 2		
		Encryption algorithm	3DES V
		Hash algorithm	MD5 T
		PFS group	MODP1536 •
		Lifetime (h)	43200 Seconds V

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

🕇 Create New 🖋 Edit 🗎	Delete 🔒 Print Instructions			
Tunnel	T Interface Binding	▼ Template	T Status	T Ref.
TeltonikalPSec	💷 wan (DSL)	tere Site to Site - Cisco	OUp	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**

ro	ot@Telt	tonika	a-RUT95	5:~# ping	-I 192	2.168.1.	1 192.168.100	.99
PII	NG 192	.168.1	100.99	(192.168.	100.99) from 1	92.168.1.1: 5	6 data bytes
64	bytes	from	192.16	8.100.99:	seq=0	tt1=255	time=976.729) ms
64	bytes	from	192.16	8.100.99:	seq=1	tt1=255	time=935.275	ms
64	bytes	from	192.16	8.100.99:	seq=2	tt1=255	time=894.905	i ms
64	bytes	from	192.16	8.100.99:	seq=3	tt1=255	time=854.529) ms

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

FortiWiFi 30E-3G4G-IN	ΠL	FW30EI3U160	000440					↓ ² • ?• >_	[] admin∓
🕐 Dashboard	>	C Refresh	🗊 Reset Statistics 🛛 🐼 Bri	ng Up 🔮 Bring Down					
E FortiView	>	▼ Name 🖨	▼ Type 🖨	▼ Remote Gateway 🖨	▼ Username ≑	▼ Status 🖨	▼ Incoming Data 🗢	▼ Outgoing Data 🗘	▼ Phase 1 🖨
+ Network	>	TeltonikalPSec	므 Custom			🖸 Up	133.96 kB	82.74 kB	TeltonikalPSec
System	>								
📕 Policy & Objects	>								
Security Profiles	>								
U VPN	>								
💄 User & Device	>								
🗢 WiFi & Switch Controller	>								
🔟 Log & Report	>								
C Monitor	~								
Routing Monitor									
DHCP Monitor									
SD-WAN Monitor									
FortiGuard Quota									
IPsec Monitor	☆								

Via CLI:

E W S	30E130	160004	440 #						
EWS	30EI3U	160004	440 #	execute	ping-	-optior	is sour	ce 192.168.	100.99
					F3				
FWS	30EI3U	160004	440 #	exec pi	ng 192	2.168.1	1.1		
IPIN	IG 192	.168.1	1.1 (1	192.168.	1.1):	56 dat	ta bytes	3	
							_		
64	bytes	from	192.1	168.1.1:	icmp	seq=0	ttl=64	time=868.0	ms
64	bytes	from	192.1	168.1.1:	icmp	seq=1	ttl=64	time=703.8	ms
64	bytes	from	192.1	168.1.1:	lcmp	seq=2	tt1=64	time=121.6	ms
		_							
64	bytes	from	192.1	168.1.1:	lcmp	seq=3	tt1=64	time=123.7	ms
64	bytes	from	192.1	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:

🕇 Create New 🔗 Edit 🗎	Delete 🔒 Print Instructions			
Tunnel	T Interface Binding	▼ Template	T Status	T Ref.
TeltonikalPSec	💷 wan (DSL)	🚟 Site to Site - Cisco	OUp	4

Hit Convert To Custom Tunnel:

Edit VPN Tunnel	
Tunnel Template	🗮 Site to Site - Cisco Convert To Custom Tunnel
Name	TeltonikalPSec
Comments	VPN: TeltonikaIPSec (Created by VPN wizard) // 43/255

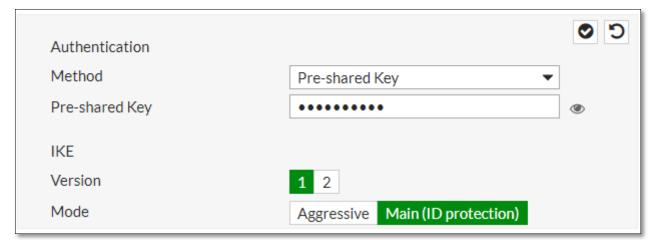
You will now have full control of IPSec tunnel settings:

1. Network settings:

Network	C 🔊
IP Version	IPv4
Remote Gateway	Static IP Address 🔹
IP Address	
Interface	💷 DSL (wan) 🔻
Mode Config	
NAT Traversal	Enable Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable On Idle On Demand

7

2. Authentication settings:



3. Phase 1 settings:

Phase 1 Propo	Al O Add	C
Encryption	3DES - Authentication SHA1 - 🗙	
Encryption	3DES Authentication MD5 X	
Diffie-Hellmar	Group 21 20 19 18 17 16 15 14 2 5 2 1	
Key Lifetime (s	conds) 86400	
Local ID		

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

XAUTH		0
Туре	Disabled	

5. Phase 2 settings:

Name	Local Address	Remote Address			
	TeltonikalPSec_local	TeltonikalPSec_remote 🔗			
Edit Phase 2	-		C 🛇		
Name		TeltonikalPSec			
Comments		VPN: TeltonikalPS wizard)	Sec (Created by VPN		
Local Addre	SS	Named Addre 🔻	TeltonikalPSec_local 🔹		
Remote Add	Iress	Named Addre 🔻	TeltonikalPSec_remote 🔻		
Advance	ed				

TELTONIKA

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

Advanced	
Phase 2 Proposal O Add	
Encryption 3DES - Autr	nentication MD5
Enable Replay Detection 🕑	
Enable Perfect Forward Secrecy (PF	S) 🖉
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:

Name	Local Addr	ess	R	emote Address
TeltonikalPSec	192.168.100.0/25 .0	5.255.255 192	2.16	8.1.0/255.255.255.0
Edit Phase 2				0 0
Name		TeltonikaIPSe	С	
Comments		VPN: Teltonik wizard)	alPs	Sec (Created by VPN
Local Address		Subnet	•	192.168.100.0/255.255.
Remote Address		Subnet	•	192.168.1.0/255.255.25



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

Policy & Objects -> Addresses menu:

🏠 Dashboard	>	+ Create New - 🖋 Edit 🔚 Clone 🚺	🗊 Delete 🛛 🔍 Sea	rch		Address	Group A
E FortiView	>	Name 🗢	Type 🌲	Details 🌲	Interface 🌲	Visibility 🌲	Ref. 🌲
Network	>	TeltonikalPSec_local_subnet_1	Subnet	192.168.100.0/24	any	•	1
🗘 System	>	TeltonikalPSec_remote_subnet_1	Subnet	192.168.1.0/24	any	⊘	1
Policy & Objects	~						
IPv4 Policy	☆						
Addresses	<∽						

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

Dashboard	>	🕇 Create New 🕜 Edit 🔚 Clone 🛍] Delete		
📥 FortiView	>	▼ Destination ≑	▼ Gateway ≑	▼ Interface ≑	▼ Comment 🜩
Network	~ T	TeltonikalPSec_remote		TeltonikalPSec	VPN: TeltonikalPSec (Created by
Interfaces	Ţ	TeltonikalPSec_remote		Blackhole	VPN: TeltonikaIPSec (Created by
DNS					
SD-WAN					
SD-WAN Status Check					
SD-WAN Rules					
Static Routes	\$				
Static Routes	~				