# FortiClient (1.6 current) to FortiGate VPN

FortiClient is a flexible and secure application for creating various types of IPsec VPN configurations.

Strategies you can employ include:

- Basic dialup A computer connection to a private network or several routed private networks behind the FortiGate unit.
- Xauth The user must enter in a username and password to start the VPN connection.
- VIP Assign the client an IP address different from the one currently on their Network Interface Card (NIC) in order to comply with the host network scheme or to provide the user the ability to resolve names on the host network.
- Local / Peer ID Make the VPN connection specific to each user. Useful when an employee leaves the company, the administration needs to remove his user account on the FortiGate unit so they can no longer connect. This is not authentication, but identification. The user does not have to type in anything with this option. The FortiGate will show the user as connected, allowing the administrator to view who is online.
- **Hub and spoke** Allows the client to be a spoke to connect to a central hub, which has another VPN to a second firewall and allows the client to connect through.

This document describes the set up for basic dialup and local/Peer ID to make a standard VPN connection to a remote network.

# **Configuring FortiClient**

- 1. In FortiClient, go to **VPN > Add**.
- 2. Enter the following options:
  - Name: name of VPN connection
  - Remote Gateway: Public IP of the remote FortiGate unit
  - Remote Network: Internal subnet of the private network behind the FortiGate unit
  - Method: preshared key
  - Preshared key: Enter the password of the user you created on the FortiGate unit

Proposais	[		C Main C Accrossing
DES	Authentication MD5	Delete Delete all	DH Group 1 2 7 5 Key Life (sec): 28800 Local ID firewall
Sec Proposals Encryption DES	Authentication MD5	Add Delete Delete all	DH Group 1 2 5 Key Life Seconds KBytes Seconds 1800 KBytes 5120
vanced Options Replay Detecti	on 🔽 PFS 🔽 M	Vat Traversal	Keepalive Frequency 5

- 3. Select Advanced.
- 4. In the policy area, select Config.
- 5. Set the following options:
  - Mode: Select Aggressive mode. It is more compatible than the default Main mode.
  - Local ID: Enter the username of the user you created on the FortiGate unit.
- 6. Select OK to get back to the selection screen.
- 7. Select Connect. A message dialog box appears with the IPSec negotiation information.
- **Note:** This field and the preshared key field are the only differences you need to make when passing these configurations to different users who will use the client. Otherwise you can use the defaults unless you need to make a specific change.
- **Note:** DES-MD5 is the default on the FortiClient if you have not licensed your copy. When you license it, you get all others including 3DES, which is the default for the FortiGate unit.

## Troubleshooting

- PROBLEM: Aggressive mode or Main mode are in Phase 1. Quick mode is in Phase 2.
- SOLUTION: Knowing which phase fails will help you know where to look. In the above example, this failed in Phase 1 since we never got the Aggressive mode message #2 (done) message.

#### Things to check in Phase 1:

- Typo in preshared key/user's password on FortiGate
- Wrong proposal DES-MD5 used, DES-SHA1 configured on client
- Wrong gateway IP address

IKE Negotiation	
May 212451: Initiator: sent 10.12.12.2 aggressive mode message #1 (DK) May 212451: Initiator: sent 10.12.12.2 aggressive mode message #2 (DONE) May 212451: Initiator: sent 10.12.12.2 quick mode message #1 (DK) Negotiation failed! Please check log	2
<u> </u>	>
ОК	

In the above message, we know Phase 1 is completed—it is okay. There is no need to change the preshared key, gateway IP, or anything in Phase 1. Phase 2 has now failed. We know because we went into Quickmode before it failed.

#### Things to check in Phase 2:

- Remote network specified correctly
- PFS
- Key lifetimes
- DH Group correct
- Proposal is correct
- Policy entered correctly on the FortiGate unit
- Addresses correct on the FortiGate unit

# Configuring the FortiGate unit

You need to perform the following configurations in order:

- Local users
- Local group
- Phase 1
- Phase 2
- Firewall addresses
- Firewall Policy, in that order.

To create a local user

1. Go to **User > Local**, select Create New and enter the user information.

Fortigate - FGT1000-RWT - Microsoft Int	ernet Explorer		🗖 🗗 🗖 🔀
File Edit View Favorites Tools Help			a da
🔇 Back + 🕲 - 🖹 🗟 🏠 🔎 S	earch 👷 Favorites 🕢 🍰 😓 👳	8 🔜 🚳 🏛 🦓 🔜 👘	
Address			🛩 🛃 Go Links 🎽
Google - 😽 😽 Sea	ch Web 🔹 🤣 🔂 0 blocked 📲 AutoFill	Ciptions 🥒	
FORTIGATE. 1000			<b>-</b> ?† <b>-</b> 2
Local			
System			
Router		New User	
Firewall	User Name	firewall	
line		Disable	
local	Password		
RADUS	O LDAP	Idap 💌	
LDAP	Radius		
User Group	ОК	Cancel	
VPN			
PS			
Anti-Virus			
Web Filter			
Sparn Filter			
Log&Report			
C Forner		Up 35 Days 0 Hours	IEAL TIME NETWORK PROTECTION
2 Done			🚔 🔮 Internet
🏄 start 🛛 🥴 🖸 🗳 🏕	🖉 2 Internet Explorer 🔹 📑 FGT-Forbolio	nt_setup 🧕 AkiAgent	100% - C 👪 😭 🥥 8:23 PM

3. Add this user to a group. Click on **User > Group**, and add this user to an appropriate group. Create a new group, if required.

Fortigate - FGT1000	-RWT - Microsoft In	ernet Explorer				
File Edit View Favorit	es Tools Help					A*
😋 Back + 🕤 - 🖪	a 😰 🏠 🔎 s	earch 🤺 Favorites	🖉 - 🍓 🖂 🗾 🚳	🗱 🦀 🔜 💷		
Address						🖌 🄁 Go Links 🎽
Google -	🗹 😚 Sea	ch Web 🔹 🦪 🔂 0 bloc	ked 📲 Autofil 🛛 💽 Options	1		
	are. 1000					-09-2
System	User Group					
Router			Edit User	Group		
Firewall		Group Name:				
• User		Available Users:	Nr5	Members:		
Local RADUS		robbie		firewall Users on RADIUS/LDA	P servers	
LDAP		travis	9			
User Group		Users on RADIU	IS/LDAP servers			
VPN			G			
PS						
Anti-Virus						
Web Filter		Protection Profile	scan	<ul> <li>(firewall authent)</li> </ul>	ication only)	
Spam Filter			ОК	Cancel		
Log&Report						
CFORTIGET.				Rev Up 35 Days 0 Hours	REAL TIME N	ETWORK PROTECTION
Done						🚔 🥶 Internet
📲 start 🛛 🖉 🖸	6 🧿 🖨 🛷 👘	😂 2 Internet Explorer	FGT-Forticlent_setup	🍯 AltiAgent	100%	

### **Configure Phase 1**

- 1. Go to **VPN > Phase 1**.
- 2. Select Create New.

Fortigate - FGT1000-RWT - Micro	ssoft Internet Explorer	
File Edit View Favorites Tools H	de de	🕂 🖉 🖉 🖓 🖉
🌀 Back 🔹 🐑 🕐 😰 🏠	🔎 Search 🤺 Favorites 🤣 🔂 😓 🔂 🍘 🛍	🤁 🦝
Address		💙 🋃 Go 🛛 Links 🎢
Google -	🚯 Search Web 👻 🤯 🗧 0 blocked 🔞 AutoFill 🛛 🚾 Options 🥒	
FORTIGATE. 10	00	
System	Phase 2 Manual Key Concentrator Gateway Name Forticlient_p1	Ping Generator Monitor
Router	Remote Gateway Dialup User	
Firewall User	Authentication Method Preshared Key	Main (ID protection)
- VPN	Pre-shared Key Peer Options	
PSEC PPTP L2TP	<ul> <li>Accept any p</li> <li>Accept this p</li> </ul>	peer ID
Certificates	Accept peer	ID in dialup group ipsec 💌
IPS	Advanced (XAUTH, Nat	Traversal, DPD)
Anti-Virus	P1 Proposal	Authentication MD5 V
Snam filter	DH Group 1 2 5 9	
Log&Report	Keylife 28800 (120-17 Local ID (option	72800 seconds)
	XAuth  ODisable OEna	able as Client OEnable as Server
	Nat-traversal 🕑 Enable	
	Keepalive Frequency 5 (0-900	seconds)
Former	Dead Peer Detection V Fnable	Up 35 Days 0 Hours REAL TIME NETWORK PROTECTION
Done		🚔 🔮 Internet
🛃 start 👘 🖉 💽 🕼 😜	😵 🥂 2 Internet Explorer 🔹 💀 FGT-Forticlent_setup 👩	🖇 Aklagent 100% 🖓 🚛 🏟 🗰 🗱 🔍 🖨 7:49 PM

- 3. Enter the following options:
  - Gateway name: Enter a name for the gateway
  - Remote Gateway: dial-up user
  - Mode: Aggressive or Main
  - Authentication Method: preshared key
  - Peer option

The phase 1 setup is mostly default. Use the same mode as in FortiClient. Ensure the Peer Options are set to 'Accept peer ID in dialup group' and select the name of the group you just made.

4. Enter a preshared key as a placeholder. You will not be using this on the client.

The local username is the LOCAL ID on the FortiClient.

How Peer IDs work:

- The local username is the LOCAL ID on the FortiClient.
- The local password is the PRESHARED KEY on the FortiClient side.

#### **Configure Phase 2**

- 1. Got to **VPN > IPSec > Phase 2**.
- 2. Select Create New.
- 3. Select the tunnel you created in Phase 1.
- 4. Select advanced and select DES MD5 to match FortiClient. The rest are defaults.
- 5. Select OK.

Fortigate - FGT1000-RWT - Micross	oft Internet Explorer		
File Edit Wew Favorites Tools Help			4
🌀 Back 🔹 🕥 🕐 🛃 🙆 🔥	🔎 Search 🤺 Favorites 🥳	🔗 · 🍓 🖂 📒 🚳 🛍 🦓	
ddress			🖌 🔁 Go Links 🤇
Google - 🛛 💌 🔞	🏚 Search Web 🔹 🤯 🗗 0 block	ed 📲 Autorial 🛛 🚾 Options 🥒	
📰 FostiGste, 100	0		- 9 <b>+</b> = 8
WEB CONFIG			
Phase 1	Phase 2 Manual Ke	y Concentrator Ping Generator Monitor	
System		New VPN Tunnel	
Router	Tunnel Name	forticlient_p2	
Firewall	Remote Gateway	Fortidient_p1	
User	Concentrator		
VPN	Advanced		
IPSEC	P2 Proposal	1-Encryption: DES Authentication: MD5 V 0	
4.27P		Enable replay detection	
Certificates		Enable perfect forward secrecy(PFS).	
IPS		DH Group 1 ○ 2 ○ 5 ⊙	
Anti-Mirus	Keylife:	Seconds V 1800 (Seconds) 4608000 (KBytes)	
Web Filter	Autokey Keep Alive	Enable	
Spam Filter	DHCP-IPsec	Enable	
Log&Report	Internet browsing	None	
	Quick Mode Identit	les   Use selectors from policy	
		O Use wildcard selectors	
		O Specify a selector	
		OK Cancel	
Former		SUD 35 Days O Hours REAL TIME N	STWORK PROTECTIO
Done			🔒 🔮 Internet
🛃 start 🔰 🥖 🖸 🕼 🔌	🖉 Z Internet Explorer 🔹	🔮 FGT-Forticient_setup 🍯 AltAgent 100% 🖂	🖹 🕤 🖬 🕄 🔍 🖨 7:51 РМ.

## **Configure the Firewall Address**

- 1. Go to **Firewall > Address**.
- 2. Enter the address name.

Our example local internal network is 10.11.11.0 255.255.255.0 so that is what I will use for this. Normally, define whatever your local subnet is.

3. Enter the firewall IP address and subnet.

Fortigate - FGT1000-RWT - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	AT
😮 Back + 🕥 - 😠 😰 🏠 🔎 Search 🤺 Favorites 🤣 🍰 😓 📃 🚳 🎉 🥸	
Address	🖌 🄂 Go Links 🍟
Coogle - 🦉 🍪 Search Web - 🤯 🗗 Oblocked 🐄 AutoFil 💽 Options 🥒	
Address Group	
System	
Router Now Addrocc	
Address Name LOCAL LAN	
Price ID Range (Subert 10.11.11.0/24	
Address	
Service	
Schedue	
-Vitual P	
IP Pool	
User	
VPN	
IPS	
Anti Virus	
Web Filter	
Spam Filter	
Log&Report	
Up 35 Days 0 Hours	REAL TIME NETWORK PROTECTION
2 Done	🚔 🔮 Internet
🛃 Start 🖉 🖉 🖉 🗳 🍣 🏕 🧭 🖉 2 Internet Explorer 🔹 💁 FGT-Forbident_setup 🦉 AtlAgent	100% 📲 🔍 🖬 🕄 😜 7:54 PM

You do not need to define the remote side since we will use the all address that is there by default.

# Configure a firewall policy

You need to create the encrypt rule that gives permission. This policy must be before any non-encrypt policies.

- 1. Go to **Firewall > Policy**.
- 2. Select Create New.

This policy will be from the Local LAN to ALL. Only the boxes shown need to be checked. No need to NAT anything.

Fortigate - FGT1000-RWT	- Microsoft Internet Explor	er			
File Edit Yew Favorites Tr	ools Help				A1
3 Back - 🕑 - 💌 🙎	🕽 🏠 🔎 Search 🤸 Fe	workes 🕢 🔗 🍯	. 🖂 📃 🚳 🎎	8	
Address					💌 🛃 Go 🛛 Links 🎽
Google -	💙 😚 Search Web 🔻 🕴	👂 🛃 0 blocked 🕤 Au	toFil 🛛 🛃 Options 🥒		
📰 FoatiGate	E. 1000				
WEB CONFIG	lieu				
System	mey				
Router			New Policy		
- Firewall			Source	Destination	
Policy		Interface/Zone	internal 💌	external	<ul> <li>Image: A set of the set of the</li></ul>
Address		Address Name	LOCAL_LAN	all	×
Service		Schedule	always 💌		
Schedule		Service	ANY 🍟		
IP Pool		Action	ENCRYPT Y		
Protection Profile					_
User		VPN Tunnel	forticlient_p2	×	
MON		Allow inbound	Inbound NAT		
UPR .		Allow outbound	Outbound NA	σ	
IPS					-
Anti-Virus		Protection Profile	strict		
Web Filter		Log Traffic			
Spam Filter		Advanced	(Traffic Shaning Diff	ferentiated Services)	
Log&Report			(Tranic Shaping, on	erennated Services)	
			OK C	ancel	
Forner			<b>₽</b> ~U	p 35 Days 0 Hours REA	TIME NETWORK PROTECTION
Done					🔒 🔮 Internet
🦺 start 🛛 🧭 🙆 🕫	🝳 🖨 🎸 🛛 🎉 Z Internel	t Explorer 🔹 😼 FGT-	Forticlient_setup 🧕 At	iAgent	100% - C C M 🕄 🖨 8:10 PM

Notice the above policy #24 is below #23. This is a common problem. Policy #24 should be moved to above #23. (Your screen may show different policy numbers).

ECK VIEW Pavo	vites Tools	Help			24 að					
Bak + 💭 -	🔳 🖻 🔇	) Dearch 🎇 Fa	workes 🚱 🔂-	🌣 🖂 🖵 🔞 I	a 48					
1955								~	6	Lit
ogle •	~	😚 Search Web 🔹 🥇	Backed 1	AutoFil 🛛 💽 Options 🚽						
Forme	iare. 1	000					6	0		E)
WEB CONFI	G									
	Policy									
ynstern	Cre	ate New								
louter	10	Same and Same	Dect	Saha da da	Panisa	Action	Eashia			
rewall	- inter	nal -> external (2)	Desc	schebule	Service	Acoon	Linable			_
olicy	23	all	all	always	ANY	ACCEPT		111	/ +8	4
ddress	24	LOCAL_LAN	all	always	ANY	ENCRYPT		11	7 -8	
ervice	) port	-> port2 (4)								
chedule	porti	-> port3 (1)								
itual P	porti	2 -> port1 (12)								
Pool	_									
ratection Profile										
lser										
-										
***										
*5										
nti Virus										
Veb Filter										
nam Eiller										
spann rates										
oolRecort										
og&Report										
og&Report				1	💐 Up 35 Days 0 Ho	REAL TI	ME NETV	VORK	PROT	101

You can say BEFORE 23 and it will be moved.

Test the FortiClient configuration. It should be successful. You should be able to ping an address on the internal subnet or, at the very least, ping the internal interface of the FortiGate.

Some troubleshooting tips:

- Check VPN, IPSEC, Monitor for connection status and to determine what proxy IDs you are using.
- Check the event log to see IPSEC status messages. This will help to see the phases being negotiated. Make sure events are enabled.
- Same concepts apply as for FortiClient—Phase1 and 2 must complete.