# **FortiClient** (1.6 current) **to FortiGate VPN**

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

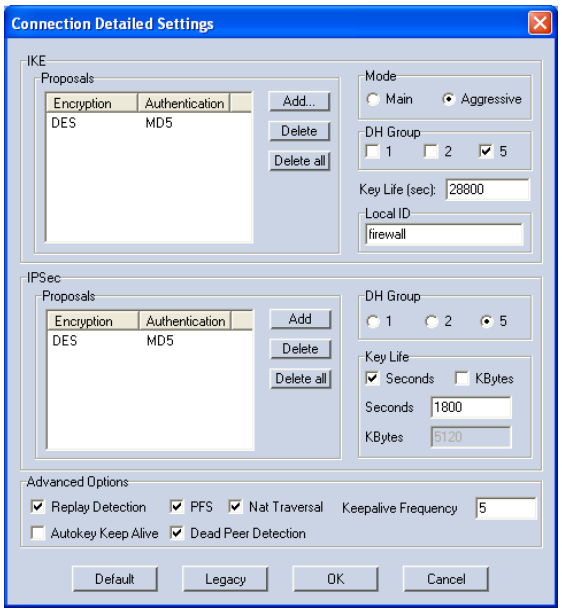
Strategies you can employ include:

- **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



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.

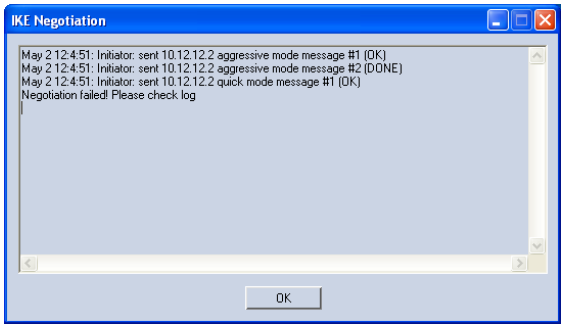
## Troubleshooting

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




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

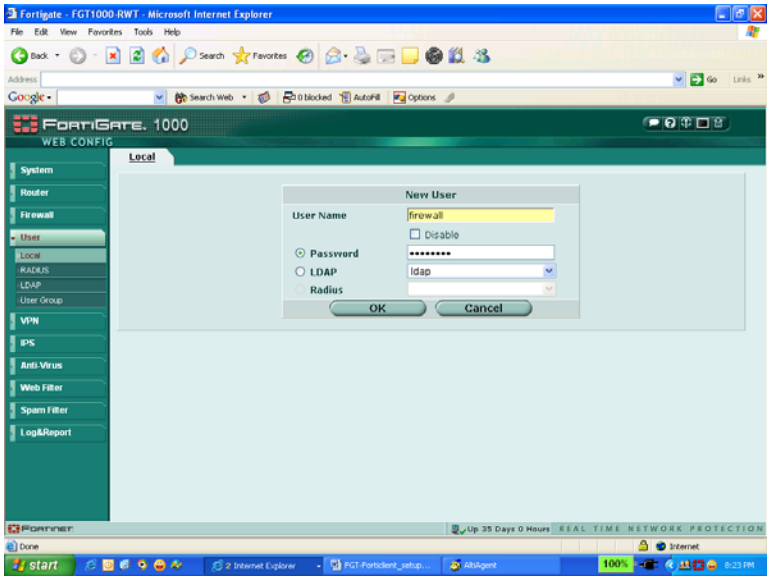
### Configuring the FortiGate unit

You need to perform the following configurations in order:

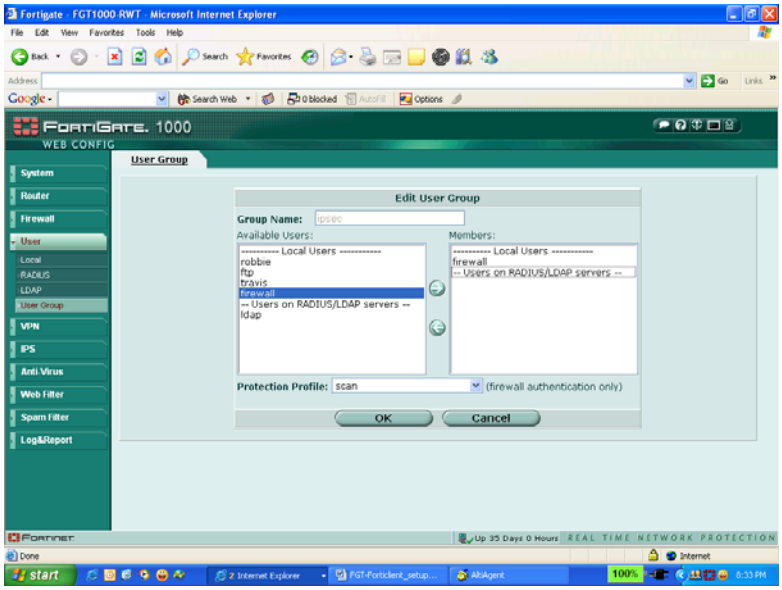
- Local users
- Local group
- Phase 1
- Phase 2
- Firewall addresses
- Firewall Policy, in that order.

### To create a local user

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

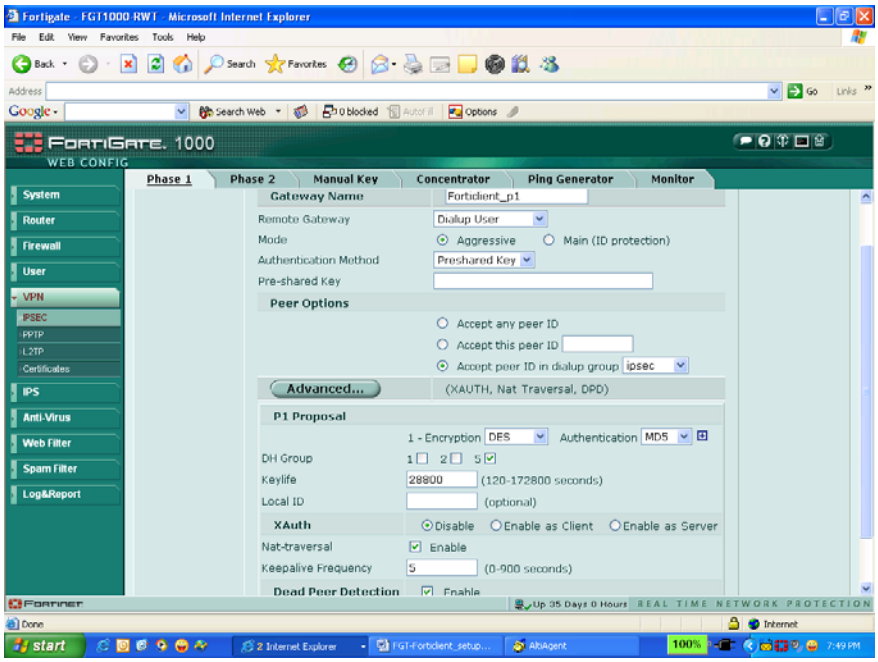



3. Add this user to a group. Click on **User > Group**, and add this user to an appropriate group. Create a new group, if required.



**Configure Phase 1**

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




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.

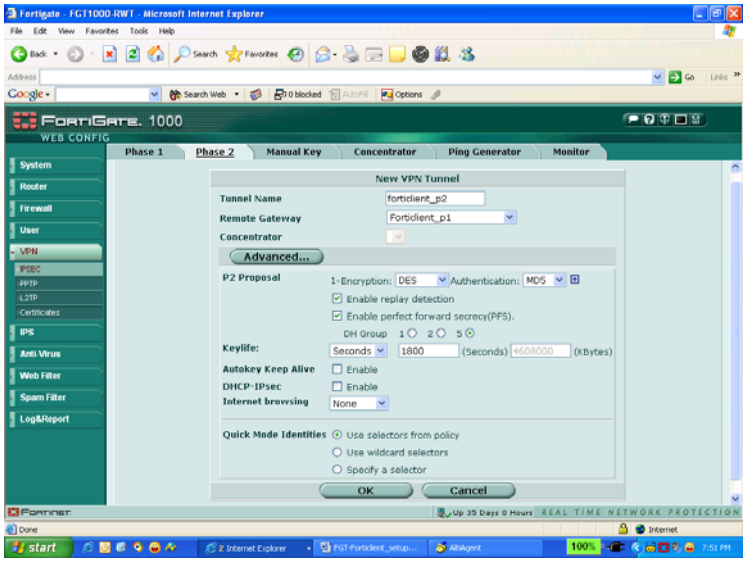
.

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.

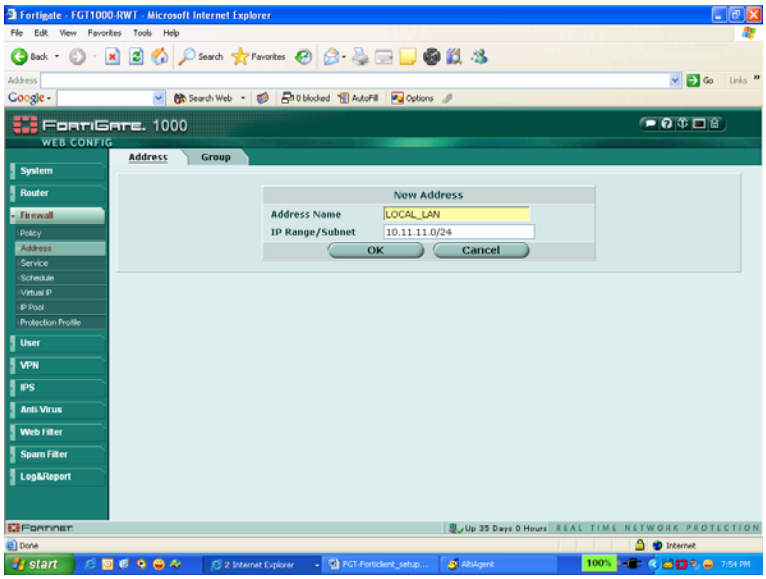



### Configure the Firewall Address

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.



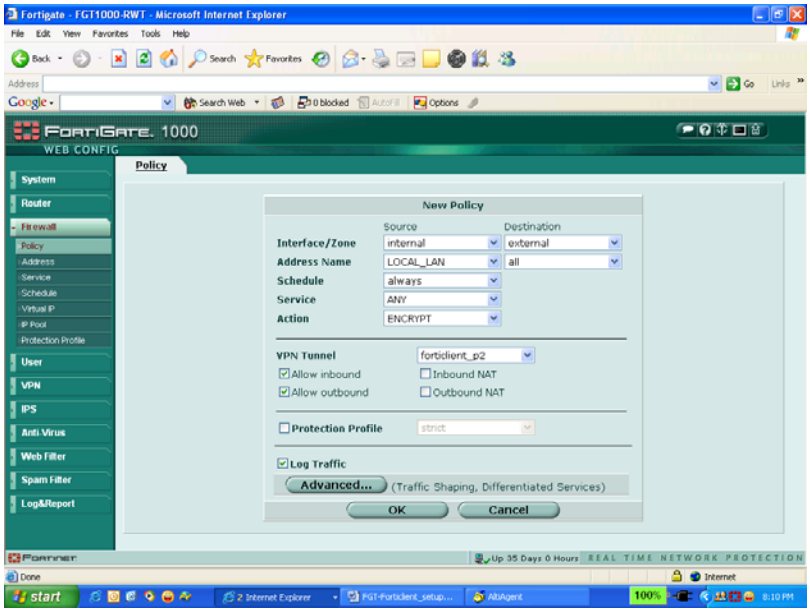

You do not need to define the remote side since we will use the all address that is there by default.

### Configure a firewall policy

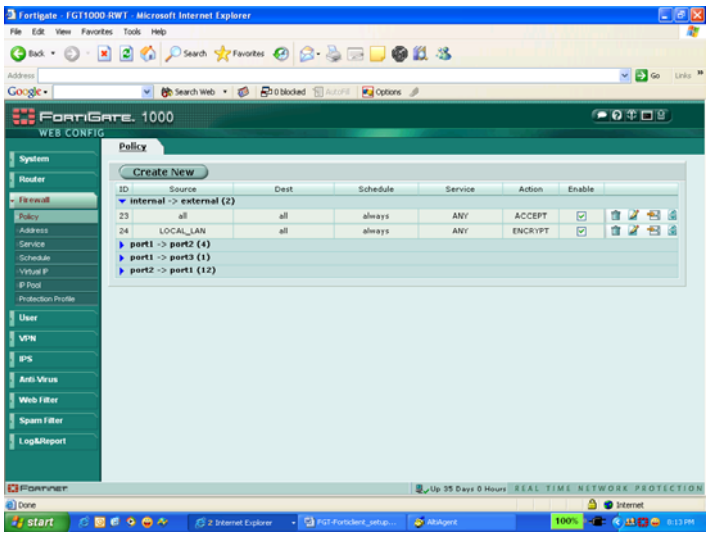
You need to create the encrypt rule that gives permission. This policy must be before any non-encrypt policies.

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.




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).




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.