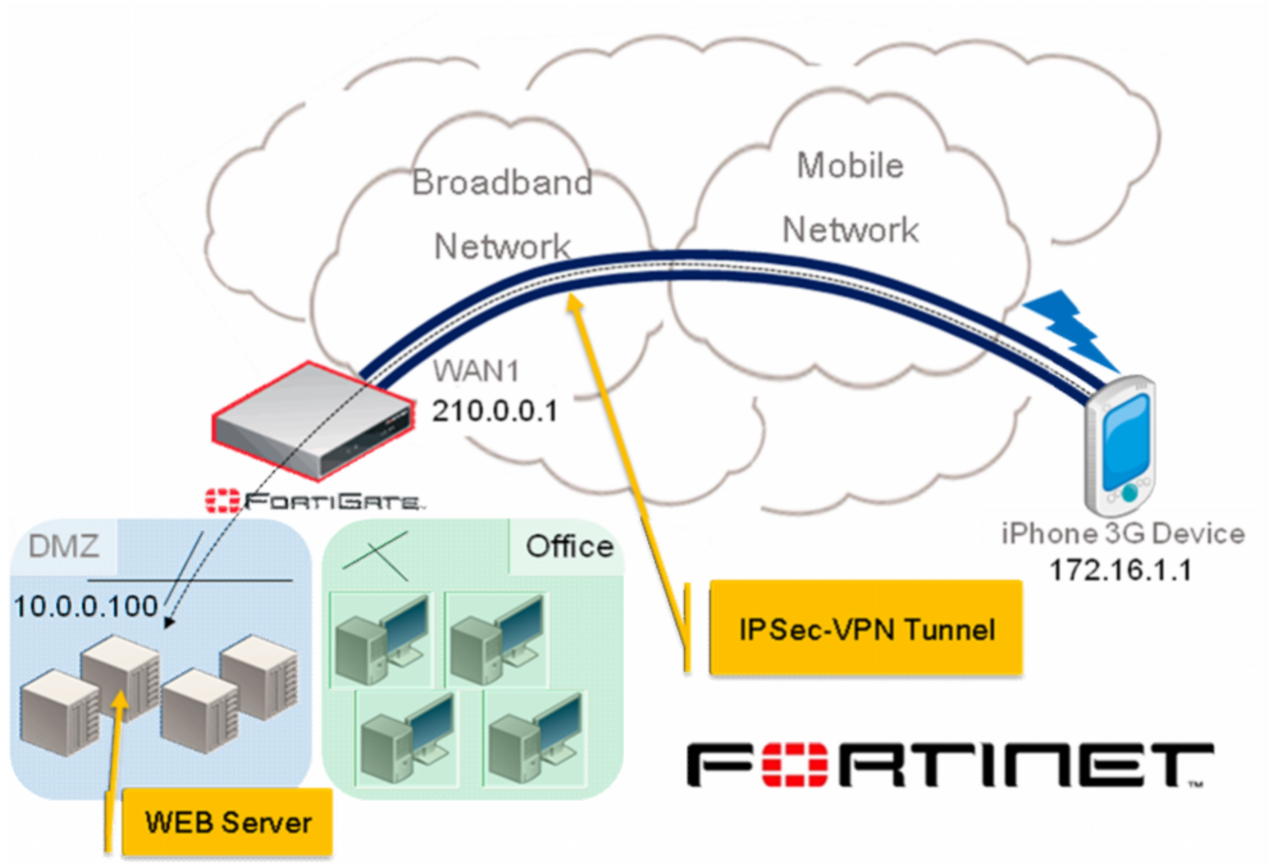
FortiGate – iPhone 3G IPSec-VPN Setup Guide (v1.0)

Components	• All FortiGate Unit FortiOS v4.0 MR1 Patch1 (v4.1.1) • iPhone 3G device
Last Modify	10-FEB-2010
Network IP Address	**FortiGate**: - WAN1 : 210.0.0.1/24 - DMZ : 10.0.0.99/24 - VPN : 172.16.1.0/255.255.255.0 (for iPhone user) **WEB Server (Fortinet Knowledge Base)** - IP : 10.0.0.100/24 (FortiGate DMZ I/F)
 Broadband Network Mobile Network WAN1 210.0.0.1 FortiGate DMZ 10.0.0.100 Office iPhone 3G Device 172.16.1.1 IPSec-VPN Tunnel WEB Server FORTINET	
Procedure	1. Setup FortiGate 1.1. Local ID and Password for iPhone(VPN) user 1.2. User Group for Local ID 1.3. Firewall address for DMZ access

1.4. VPN phase1

1.5. VPN phase2

1.6.DCHP address for VPN client (iPhone)

1.7. Firewall Policy

2 . Setup iPhone 3G device

2.1.VPN

3.connection test for iPhone 3G device

3.1. check to VPN connection status

3.2. Ping

3.3. WEB access over VPN (mobile network)

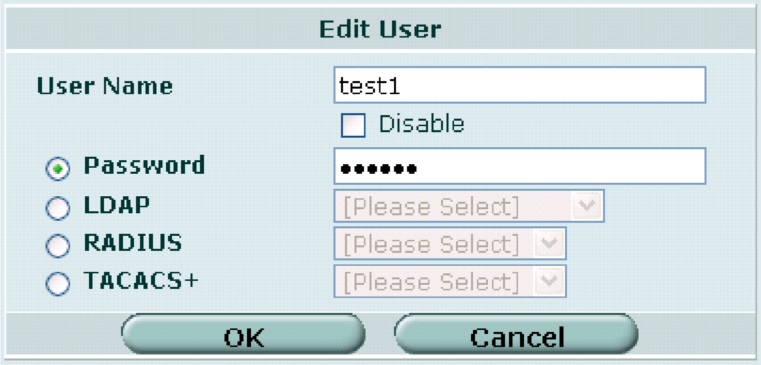
1.Setup FortiGate

1.1. Edit Local ID and password for iPhone(VPN) user

Setup via WEB based manager:

1.1.1. Move to User > Local > Create New.

1.1.2. Enter User ID and Password.



Edit User

User Name: test1

□ Disable

● Password: ●●●●●●

○ LDAP: [Please Select]

○ RADIUS: [Please Select]

○ TACACS+: [Please Select]

1.1.3. Select OK.

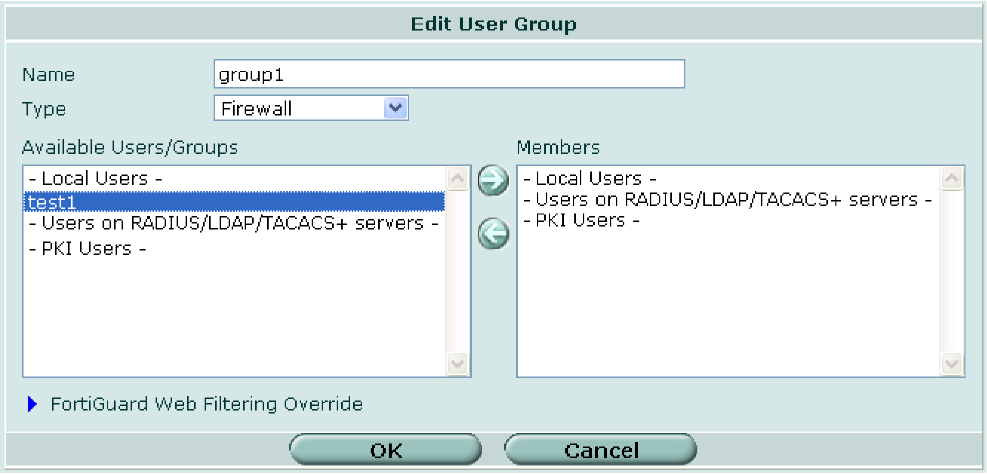
1.2. Edit User group for Local ID

1.2.1. Move to User > User Group > Create New.

1.2.2. Enter group name (e.g. group1), and then select firewall type.

Select local ID from available Users/Groups list.

Click [->] icon to add it to member list.



Edit User Group

Name: group1

Type: Firewall

Available Users/Groups:
- Local Users -
test1
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -

Members:
- Local Users -
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -

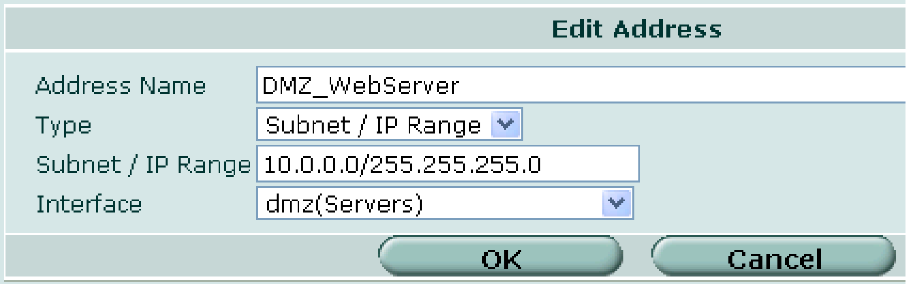
1.2.3. Select OK.

1.3. Edit Firewall address for DMZ access

1.3.1. Move to Firewall > Address > Create New**.**

1.3.2. Enter DMZ server info.

1.3.3. Enter address name, type, subnet/IP range, and interface.



Edit Address

Address Name: DMZ_WebServer

Type: Subnet / IP Range

Subnet / IP Range: 10.0.0.0/255.255.255.0

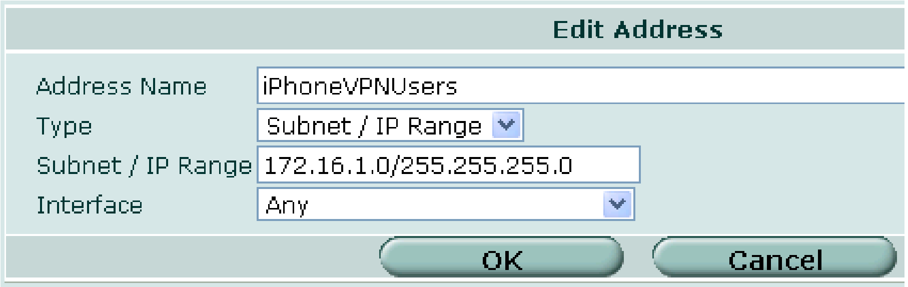
Interface: dmz(Servers)

1.3.4. Select OK.

1.3.5. Click Create new again.

1.3.6. Edit Firewall address for iPhone user.

1.3.7. Enter address name, type, subnet/IP range, and interface.



Edit Address

Address Name: iPhoneVPNUsers

Type: Subnet / IP Range

Subnet / IP Range: 172.16.1.0/255.255.255.0

Interface: Any

1.3.8. Select OK.

1.4. Edit VPN Phase1

Setup via WEB based manager:

1.4.1. Move to VPN > IPSec > auto Key > Create Phase1**.**

Enter following info.

Name	iPhone
Remote Gateway	Dialup users
Local Interface	WAN1
Mode	Main
Authentication Method	Pre-shared Key
Pre-shared Key	Key (same as iPhone3G VPN configuration)
Peer Options	Accept any peer ID

1.4.2. Select Advance option and then enter following info.

Enable IPsec Interface Mode	Enable
Local gateway IP	Main interface IP
1 Encryption	AES256
1 Authentication	MD5
2 Encryption	AES256
2 Authentication	SHA1
DH Group	2
Key life (sec)	28800
XAUTH	Enable as Server
Server Type	AUTO
User Group	group1 (when you created it at 1.2 section)
NAT Traversal	Enable
Dead Peer Detection	Enable

1.4.3. Select OK.

1.5.Edit VPN Phase2

Setup via WEB based manager:

1.5.1. Move to VPN > IPSec > Auto Key > Create Phase2.

1.5.2. Enter following info.

Name	iPhone-P2
Phase1	Select Phase1 name(iPhone)

1.5.3. Select Advanced option and then enter following info.

1 Encryption	AES256
1 Authentication	MD5
2 Encryption	AES256
2 Authentication	SHA1
Enable replay detection	Enable
PFS	Enable
DH Group	2
Key life(sec)	1800
Auto-key keep arrive	Enable
Quick mode selector	Source Address: 0.0.0.0/0.0.0.0 Destination Address: 0.0.0.0/0.0.0.0

1.5.3. Select OK.

<u>1.6. Edit DHCP address for iPhone VPN client</u>

1.6.1. Login to FortiGate via CLI. Then use following commands.

Command	comment
config vpn ipsec phase1-interface	Move to VPN phase1
edit iPhone	Edit VPN Phase1 configuration.
set mode-cfg enable	Enable mode-cfg
set ipv4-start-ip 172.16.1.1	DHCP start IP address
set ipv4-end-ip 172.16.1.254	DHCP end IP address
set ipv4-netmask 255.255.255.0	Subnet mask
set ipv4-split-include "DMZ_WebServer"	For VPN user access to DMZ address group.

<u>1.7. Edit Firewall Policy</u>

Setup via WEB based manager:

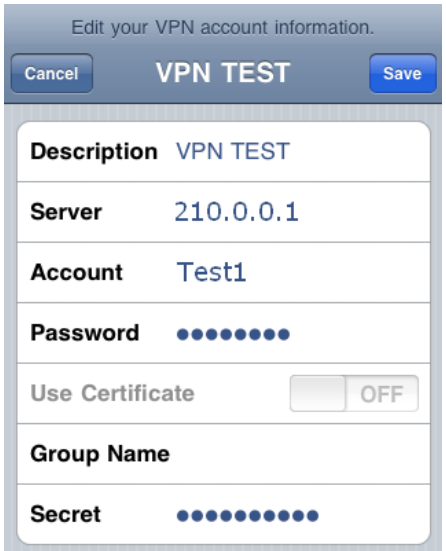
1.7.1. Move to Firewall Policy > Policy > Create new**.**

1.7.2. Enter following info.

Source Interface/Zone	iPhone (IPSec-VPN Interface)
Source Address	iPhoneVPNUsers
Destination Interface/Zone	DMZ
Destination Address	DMZ_WebServer
Schedule	Always
Service	ANY
Action	Accept

1.7.3. Select OK.

2.Setup iPhone 3G device



Edit your VPN account information.

VPN TEST

Description	VPN TEST
Server	210.0.0.1
Account	Test1
Password	●●●●●●●●
Use Certificate	OFF
Group Name	
Secret	●●●●●●●●●●

2.1.Edit VPN

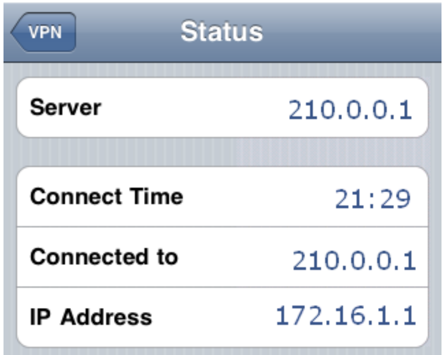
Move to VPN account setup menu.

Create new profile.

[VPN account info】

Description	VPN TEST (unique name)
Server	VPN Gateway address (FortiGate WAN1 IP address)
Account	User ID
Password	Password
Certification	Off
Secret	Pre-shared Key (same as FortiGate)

3. Connection test (VPN access, Ping, WEB access)



Status

Server	210.0.0.1
Connect Time	21:29
Connected to	210.0.0.1
IP Address	172.16.1.1

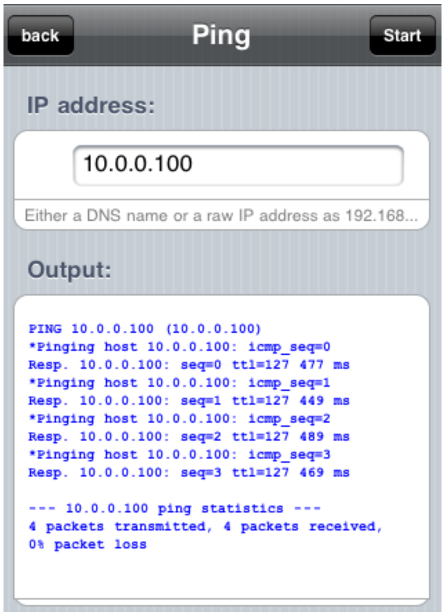
3.1. Confirm to VPN access

When you finished VPN configuration on iPhone 3G device. Please dial-up 3G network and then connect VPN gateway (FortiGate). After that you can see connection status when VPN tunnel is up.

[Status]

Server	VPN Gateway

	(FortiGate WAN1 IP address)
Connect Time	Tunnel up time
Connect to	VPN Gateway
IP address	IP address release by DHCP. *refer to section 1.6.



IP address:

10.0.0.100

Either a DNS name or a raw IP address as 192.168...

Output:

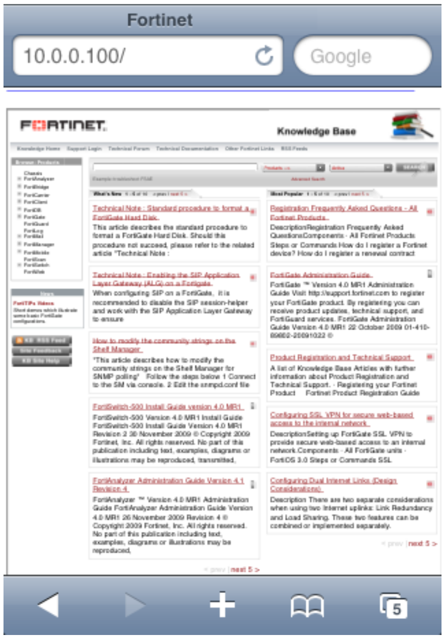
```
PING 10.0.0.100 (10.0.0.100)
*Pinging host 10.0.0.100: icmp_seq=0
Resp. 10.0.0.100: seq=0 ttl=127 477 ms
*Pinging host 10.0.0.100: icmp_seq=1
Resp. 10.0.0.100: seq=1 ttl=127 449 ms
*Pinging host 10.0.0.100: icmp_seq=2
Resp. 10.0.0.100: seq=2 ttl=127 489 ms
*Pinging host 10.0.0.100: icmp_seq=3
Resp. 10.0.0.100: seq=3 ttl=127 469 ms

--- 10.0.0.100 ping statistics ---
4 packets transmitted, 4 packets received,
0% packet loss
```

3.2. Ping

Open Ping tool and then send ping packet to WEB server IP address (e.g. 10.0.0.100) behind of FortiGate DMZ network. You can confirm to receive response from server.

Note: Ping tool doesn't default apps on iPhone 3G device. You will need download it from somewhere (e.g. iTunes Store)



3.3.WEB access

Open WEB browser and then enter WEB server IP address (e.g. 10.0.0.100) behind of FortiGate DMZ network. You can confirm to see some contents of corporate internal resource.

Note	Those IP addresses are for evaluation purpose. Please ask your ISP when you need public IP address.