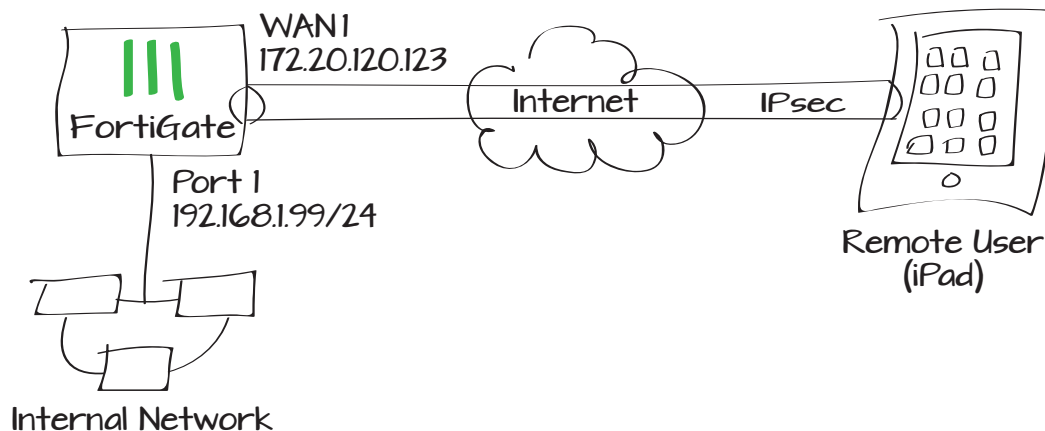


Providing secure remote access to a network for an iOS device

This recipe uses the VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The example enables group members to access the internal network and forces them through the FortiGate unit when accessing the Internet. The example uses an iPad 2 running iOS 6.1.2 (menu options may vary for different iOS versions and devices).

1. Creating a user group for iOS users
2. Adding addresses for the local LAN and remote users
3. Configuring IPsec VPN phases using the VPN Wizard
4. Creating security policies for access to the internal network and the Internet
5. Configuring VPN on the iOS device
6. Results



Creating a user group for iOS users

Go to **User & Device > User > User Definition.**

Create a new user.

Go to **User & Device > User > User Groups.**

Create a user group for iOS users and add the user you created.

Adding addresses for the local LAN and remote users

Go to **Firewall Objects > Address > Addresses.**

Add the address for the local network, including the subnet and local interface.

The screenshot displays the Fortinet configuration interface for user and group management. It is divided into two main sections: user definition and user group creation.

User Definition Section:

- User Name:** A text input field containing "twhite".
- Disable:** A checkbox that is currently unchecked.
- Password:** A radio button is selected, followed by a password input field containing six dots.
- Match user on LDAP server:** A radio button is unselected, followed by a dropdown menu showing "[Please Select]".
- Match user on RADIUS server:** A radio button is unselected, followed by a dropdown menu showing "[Please Select]".
- Match user on TACACS+ server:** A radio button is unselected, followed by a dropdown menu showing "[Please Select]".

User Group Definition Section:

- Name:** A text input field containing "ios_group".
- Type:** Radio buttons for "Firewall" (selected), "Fortinet Single Sign-On (FSSO)", "Guest", and "RADIUS Single Sign-On (RSSO)".
- Available Users:** A list box containing "- Local Users - guest".
- Members:** A list box containing "- Local Users - twhite".

Address Definition Section:

- Category:** Radio buttons for "Address" (selected), "IPv6 Address", and "Multicast Address".
- Name:** A text input field containing "LocalLAN".
- Color:** A color selection icon followed by a "[Change]" link.
- Type:** A dropdown menu showing "Subnet".
- Subnet / IP Range:** A text input field containing "192.168.1.0/255.255.255.0".
- Interface:** A dropdown menu showing "port1".
- Show in Address List:** A checked checkbox.
- Comments:** A text input field containing "Write a comment..." with a character count of "0/255".

Go to **Firewall Objects > Address > Addresses**.

Add the address for the remote user, including the IP range.

Configuring the IPsec VPN phases using the VPN Wizard

Go to **VPN > IPSec > Auto Key (IKE)**.

Select **Create VPN Wizard**. Name the VPN connection and select **Dial Up - iPhone / iPad Native IPsec Client**. Click **Next**.

Enter your pre-shared key and select the iOS user group, then click **Next**. Note that the pre-shared key is a credential for the VPN and should differ from the user's password.

Select your Internet-facing interface for the **Local Outgoing Interface**, and enter the IP range from the address range you created.

Category Address IPv6 Address Multicast Address

Name

Color [Change]

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

1 VPN Setup > 2 Authentication > 3 Network

Name

VPN Type

Dial Up - FortiClient Windows, Mac and Android

Dial Up - iPhone / iPad Native IPsec Client

✓ VPN Setup > 2 Authentication > 3 Network

Pre-shared Key

User Group

✓ VPN Setup > ✓ Authentication > 3 Network

Local Outgoing Interface

Address Range

Subnet Mask

DNS Server

Use System DNS

Specify

Enable IPv4 Split Tunnel

Assigning an IP to the VPN interface (optional)

If you wish to control the IP address that will be assigned to any traffic egressing over the IPsec interface, you can assign an IP to the interface.

Go to **System > Network > Interfaces**. Expand your Internet-facing interface and edit the VPN interface.

Assign the **IP** and **Remote IP** addresses. These addresses should not be related to the IPs used for the internal network or the Internet-facing interface.

Creating security policies for access to the internal network and the Internet

Go to **Policy > Policy > Policy**.

Create a security policy allowing remote iOS users to access the internal network.

Name	ios_P1
Type	Tunnel Interface
Interface	wan1
Addressing mode	
IP	10.10.80.1
Remote IP	172.16.2.5
IPv6 Address	::/0

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ios_P1
Source Address	all
Outgoing Interface	port1
Destination Address	Local LAN
Schedule	always
Service	ALL
Action	ACCEPT

Go to **Policy > Policy > Policy**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit. Ensure that **Enable NAT** is checkmarked.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ios_P1
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.

Description	To-Office-VPN
Server	172.20.120.123
Account	twhite
Password	••••••
Use Certificate	<input type="checkbox"/> OFF
Group Name	
Secret	••••••••



In order to connect to the VPN tunnel, a **Group Name** may be required. If you are unable to connect, add this field to the VPN client to determine if the blank field is the cause.

Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Select an entry to view more information.

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log >**

Name	Type	Remote Gateway	Username	Proxy ID Sour
ios_P1_0	Dialup	172.20.120.126	twhite	0.0.0.0-255.255.255.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	59 B / 221 B
2	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	60 B / 292 B
3	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	56 B / 288 B
4	11:21:42	port1	wan1	192.168.1.117	208.91.113.70	304 B / 304 B
5	11:20:44	ios_P1	port1	10.10.1.100	192.168.1.114	72 B / 72 B

Dst	192.168.1.114	Virtual Domain	root
Received	72	Source Country	Reserved
Sent / Received	72 B / 72 B	Duration	63
Sent	72	Application Details	
Service	PING	Protocol	1
Destination Country	Reserved	roll	65428
Status	✓	Timestamp	Thu Feb 21 11:20:44 2013
Tran Display	noop	Sequence Number	220067
Policy ID	6	Src Interface	ios_P1
Src	10.10.1.100	VPN	ios_P1_0
Sent Packets	2	Level	notice
VPN Type	ipsec-dynamic	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:20:44 (Thu Feb 21 11:20:44 2013)
Dst Interface	port1		

Forward Traffic to view the traffic.

Select an entry to view more information.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received	Polic
1	11:28:43	ios_P1	wan1	10.10.1.100	74.121.50.17	1023 B / 579 B	7
2	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	59 B / 221 B	7
3	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	60 B / 292 B	7
4	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	56 B / 288 B	7
5	11:20:42	ios_P1	wan1	10.10.1.100	173.194.73.105	812 B / 642 B	7

Dst	74.121.50.17	Virtual Domain	root
Received	579	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	1023 B / 579 B
Duration	2	Sent	1023
Src NAT Port	50189	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65428	Status	close
Timestamp	Thu Feb 21 11:28:43 2013	Tran Display	snat
Sequence Number	221594	Policy ID	7
Src Interface	ios_P1	Src	10.10.1.100
VPN	ios_P1_0	Sent Packets	6
Level	notice	VPN Type	ipsec-dynamic
Src Port	50189	logid	13
Sub Type	forward	Threat	
Received Packets	4	Date/Time	11:28:43 (Thu Feb 21 11:28:43 2013)
Dst Interface	wan1		

View the status of the tunnel on the iOS device.

On the iPad, go to **Settings > General > VPN** and view the **Status** of the connection.



Using a Ping tool, send a ping packet directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel..

