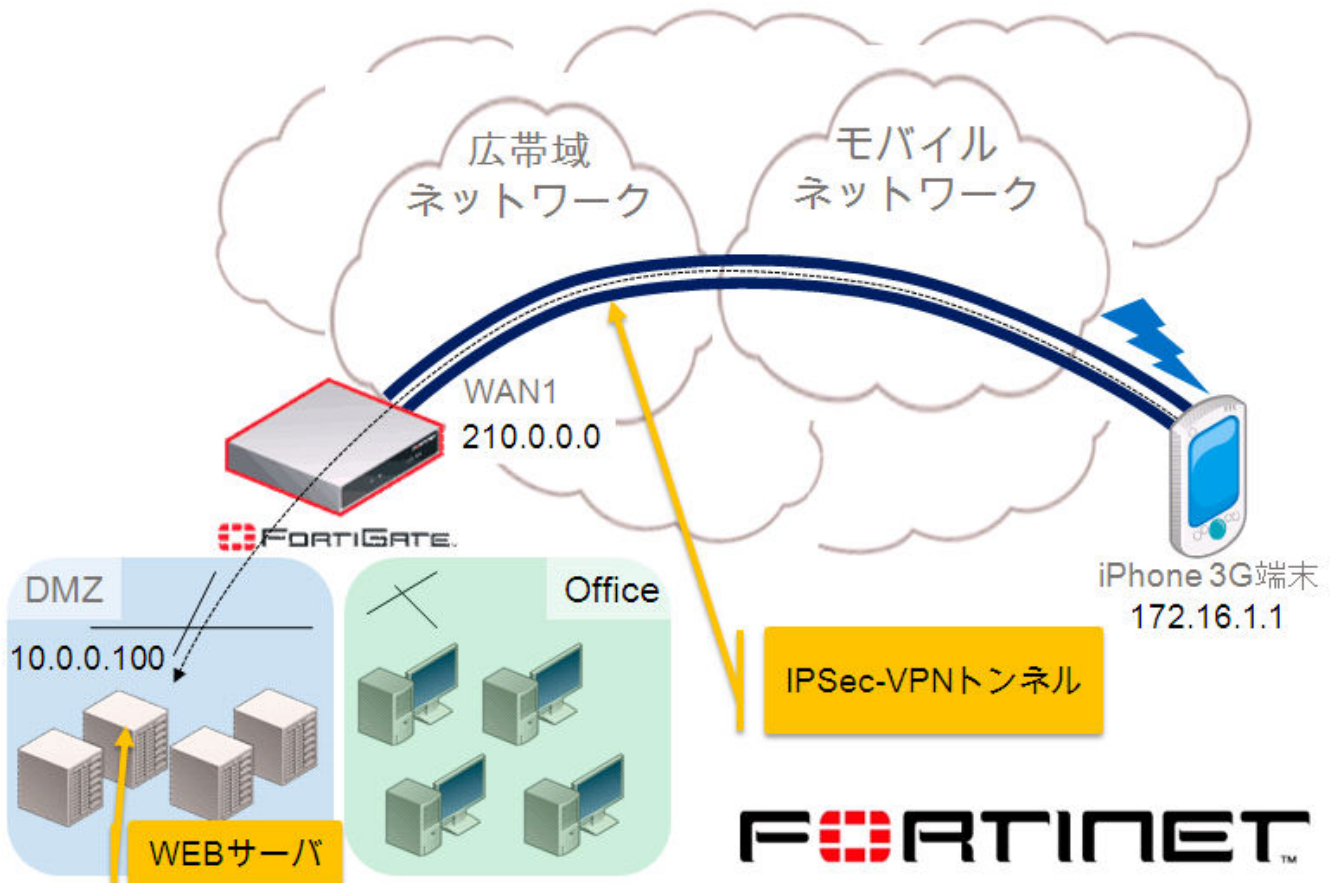


## FortiGate – iPhone 3G IPSec-VPN 簡易設定手順書 (v1.0)

<p>説明</p>	<p>この記事の内容は、FortiGate と iPhone 3G が対応している VPN 機能を利用して、両デバイス間でセキュアな IPSec-VPN 通信を行うための設定手順をまとめたものです。</p> <p>この設定例により、FortiGate と iPhone 3G 間の VPN トンネルが確立されて相互接続ができる事を確認しておりますが、<u>これらは動作を保障するものではありません。</u></p> <p>また、将来にわたり、予告なく記事の改編、削除を行う事があることを前もってご了承ください。</p>
<p>コンポーネント</p>	<ul style="list-style-type: none"> <li>• 全ての FortiGate ユニット FortiOS v4.0 MR1 Patch1 (v4.1.1)</li> <li>• iPhone 3G デバイス</li> </ul>
<p>作成日</p>	<p>2009 年 12 月 11 日</p>
<p>作成者</p>	<p>フォーティネットジャパン株式会社 シニアシステムズエンジニア 児玉 清 【検証協力:住商情報システム株式会社 ネットワーク・セキュリティ西日本営業部】</p>
<p>想定ネットワーク</p>	<p>FortiGateはISPの提供する広域ネットワークへ、iPhone3Gはモバイルオペレータの提供するネットワークへ接続されています。</p> <p>FortiGateのWAN側は静的アドレス、iPhone 3Gは動的なIPアドレスを使用しており、iPhone 3Gユーザはモバイル環境を経由してFortiGateへ接続を行う状況を想定しています。</p> <p>FortiGateのプライベートネットワーク側には、様々なサーバ群が接続されており、VPN接続後のiPhone3Gデバイスはプライベートネットワークリソースへ接続を行うことが可能となります。</p>
<p>ネットワーク構成 補足</p>	<p>*この図で使用しているIPアドレスは仮想IPアドレスになり、実際にISPサービスなどで提供されているアドレス形態とは異なる場合があります。</p> <p>FortiGate: WAN1 = ISP広域ネットワーク側に接続、DMZ=プライベート側に接続 DMZネットワークにWEBサーバ有り(Fortinetナレッジベース)</p>
<p>ネットワーク IP アドレス体系</p>	<p><b>FortiGate:</b></p> <ul style="list-style-type: none"> <li>- WAN1 : 210.0.0.0/24</li> <li>- DMZ : 10.0.0.99/24</li> <li>- VPN : 172.16.1.0/255.255.255.0 (*iPhoneユーザ用)</li> </ul> <p><b>WEB Server (Fortinetナレッジベース)</b></p> <ul style="list-style-type: none"> <li>- IP : 10.0.0.100/24 (FortiGateのDMZインターフェイスへ接続)</li> </ul>

【ネットワーク構成図】



手順

1. FortiGateの設定
  - 1.1. iPhone(VPN)ユーザのためのローカルID/パスワード登録
  - 1.2. ローカルIDのグループ登録
  - 1.3. DMZアクセスのためのアドレス登録
  - 1.4. VPNフェーズ1作成
  - 1.5. VPNフェーズ2作成
  - 1.6. VPNクライアント端末へ払い出すIPアドレス登録
  - 1.7. ファイアウォールポリシー作成
2. iPhone 3Gの設定
  - 2.1. VPN設定
3. iPhone 3Gの接続テスト
  - 3.1. VPN接続状況の確認
  - 3.2. Ping
  - 3.3. WEBアクセス

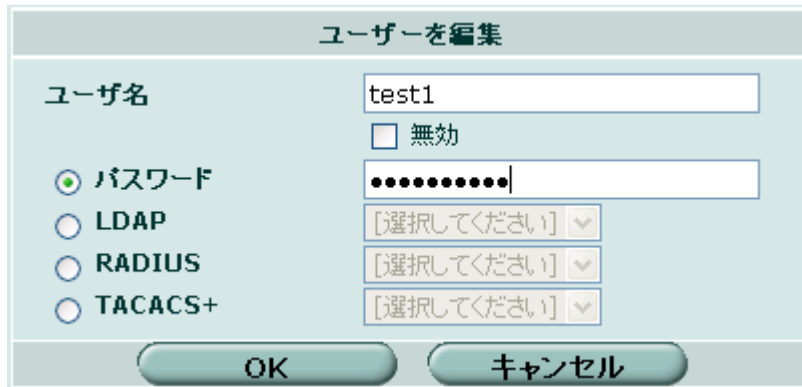
## 1. FortiGateの設定

### 1.1. iPhone(VPN)ユーザのためのID/パスワード登録

WEBベースマネージャを使い設定を行います：

1.1.1. ユーザ > ローカルへ行き、新規作成を選択します。

1.1.2. ユーザ名/パスワードを入力します。



1.1.3. OKを選択します。

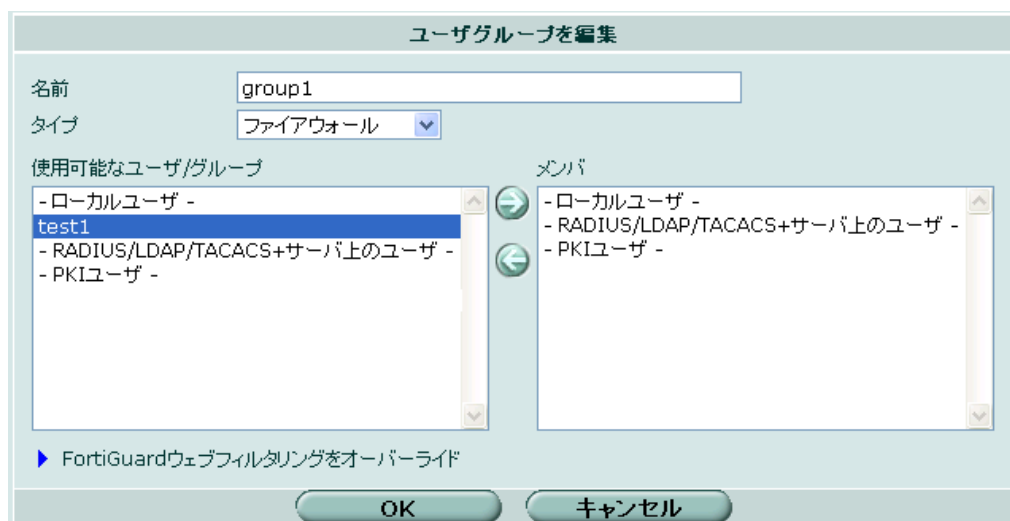
### 1.2. ローカルIDのグループ登録

1.2.1. ユーザ > ユーザグループへ行き、新規作成を選択します。

1.2.2. 名前欄にグループ名を入力。タイプはファイアウォールを選択します。

**選択可能なユーザ/グループ**からローカルユーザを選択。

「→」アイコンをクリックして**メンバ**へ追加を行います。



1.2.3. OKを選択します。

### 1.3. DMZアクセスのためのアドレス登録

1.3.1. ファイアウォール>アドレスへ行き新規作成を選択します。

1.3.2. DMZサーバのセグメント情報を登録します。

1.3.3. アドレス名、サブネット/IP範囲の情報を入力して、タイプ/インターフェイス情報をプルダウンメニューより選択します。

編集	
アドレス名	DMZ_WebServer
タイプ	サブネット/IP範囲指定
サブネット/IP範囲指定	10.0.0.0/255.255.255.0
インターフェイス	internal(DMZ)
OK      キャンセル	

1.3.4. OKを選択します。

1.3.5. 再度、新規作成を選択します。

1.3.6. VPNログイン時の iPhoneユーザのセグメント情報を登録します。

1.3.7. アドレス名、サブネット/IP範囲の情報を入力して、タイプ/インターフェイス情報をプルダウンメニューより選択します。

編集	
アドレス名	iPhoneVPNUsers
タイプ	サブネット/IP範囲指定
サブネット/IP範囲指定	172.16.1.0/255.255.255.0
インターフェイス	Any
OK      キャンセル	

1.3.8. OKを選択します。

### 1.4. VPNフェーズ1作成

WEBベースマネージャを使い設定を行います：

1.4.1. VPN > IPSec > 自動鍵(IKE)へ行き、フェーズ1作成を選択します。

以下の情報を入力します。

名前	iPhone
リモートゲートウェイ	ダイヤルアップ
ローカルインターフェイス	インターネットへ接続されているインターフェイス、例えば WAN1.

モード	メイン
認証方式	事前共有鍵
事前共有鍵	共有鍵 (iPhone3G と同じ値)
ピアオプション	あらゆるピア ID を受け入れる

1.4.2. 特別オプションを選択して以下の情報を入力します。

IPSec インタフェースモードを有効にする	有効
ローカルゲートウェイ IP	メインインタフェース IP
1 暗号化	AES256
1 認証	MD5
2 暗号化	AES256
2 認証	SHA1
DH グループ	2
鍵の有効時間(秒)	28800
ローカル ID	オプション
XAUTH	サーバを有効にする
サーバタイプ	AUTO
ユーザグループ	group1 *1.2 の手順で作成したグループ
NATトラバーサル	有効
デッドピアディテクション(DPD)	有効

1.4.3. OK を選択します。

\*XAUTH:サーバをご利用になる場合は、項目 1.1,1.2 の手順が必要です。  
アカウントの設定方法等は管理ガイド等を参考に行ってください、購入元の代理店までお問い合わせください。

## 1.5.VPNフェーズ2の設定

WEBベースマネージャを使い設定を行います:

1.5.1. **VPN > IPSec > 自動鍵(IKE)**へ行き**フェーズ2作成**を選択します。

1.5.2. 以下の情報を入力します。

名前	iPhone-P2
フェーズ1	フェーズ1の名前を選択します。(iPhone)

1.5.3. 特別オプションを選択して以下の情報を入力します。

1 暗号化	AES256
-------	--------

1 認証	MD5
2 暗号化	AES256
2 認証	SHA1
リプレイ検知	有効
PFS	有効
DH グループ	2
鍵の有効時間(秒)	1800
自動鍵キープアライブ	有効
クイックモードセクタ	送信元アドレス: 0.0.0.0/0.0.0.0 宛先アドレス: 0.0.0.0/0.0.0.0

1.5.3. OKを選択します。

## 1.6. VPNクライアント端末へ払い出すIPアドレス登録

1.6.1. CLIからログインを行い。以下の設定を使用してVPNダイヤルアップ端末へ割り当てるIPアドレスを登録します。

コマンド	補足
config vpn ipsec phase1-interface	VPN フェーズ 1 設定へ移動
edit iPhone	項目 1.4 で設定した VPN フェーズ 1 の名前
set mode-cfg enable	mode-cfg の有効
set ipv4-start-ip 172.16.1.1	開始 IP アドレス
set ipv4-end-ip 172.16.1.254	終了 IP アドレス
set ipv4-netmask 255.255.255.0	サブネットマスク
set ipv4-split-include "DMZ_WebServer"	VPNユーザをDMZアドレスグループへアクセスさせるための設定

## 1.7. ファイアウォールポリシー作成

ファイアウォール設定は、iPhoneデバイスがFortiGateのプライベート側に位置するホストへ通信を行うために必要です。

WEBベースマネージャを使い設定を行います：

1.7.1. **ファイアウォール** > **ポリシー**へ行き、**新規作成**を選択します。

1.7.2. 以下の情報を入力します。

送信元インターフェイス/ゾーン	iPhone (IPSec-VPN インターフェイス)
送信元アドレス	iPhoneVPNUsers

	*項目 1.3.で作成したアドレスグループ
宛先インターフェイス/ゾーン	DMZ
宛先アドレス	DMZ_WebServer *項目 1.3.で作成したアドレスグループ
スケジュール	Always
サービス	ANY
アクション	Accept

1.7.3.OKを選択します。

## 2.iPhone 3Gの設定

VPNアカウント情報を編集します。

キャンセル VPN TEST 保存

説明	VPN TEST
サーバ	210.0.0.0
アカウント	Test1
パスワード	●●●●●●●●
証明書を使用	<input type="checkbox"/> オフ
グループ名	
シークレット	●●●●●●●●

### 2.1.設定

**iPhoneホーム>設定>一般>ネットワーク>VPN**

メニューへ行き、新規VPNプロファイル作成を行います。

【VPNアカウント情報】

説明	VPN TEST(任意な名称)
サーバ	FortiGateのVPNインターフェイスIP (例えば WAN1 の IP アドレス)
アカウント	ユーザ ID
パスワード	ユーザパスワード
証明書使用	オフ
グループ名	未使用
シークレット	事前共有鍵(FortiGate と同じ値)
プロキシ	オフ

## 3. 接続テスト(VPN接続状況の確認、Ping、WEBアクセス)

VPN 状況

サーバ	210.0.0.0
接続時間	21:29
接続先	210.0.0.0
IPアドレス	172.16.1.1

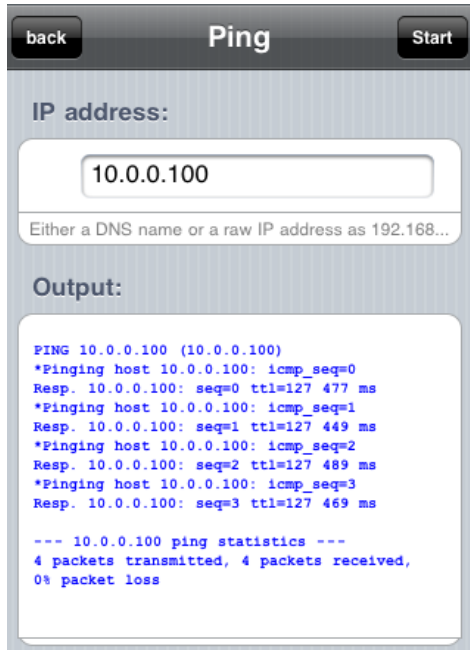
### 3.1. VPN接続状況の確認

iPhone 3GのVPN設定が終了したら、モバイルネットワークヘダイアルアップを行い、FortiGateに対してVPN接続を試みます。FortiGateとのVPNトンネル接続が確立されると、iPhoneのステータス画面で接続状況を確認することができます。

【状況】

サーバ	VPN Gateway
-----	-------------

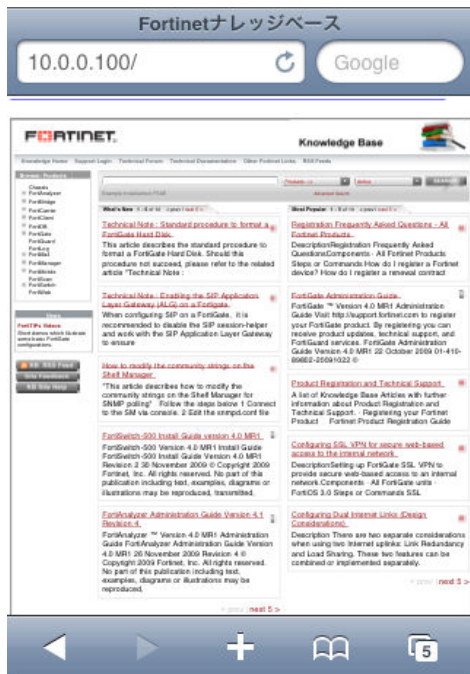
	(FortiGate の WAN1)
接続時間	VPN 接続時間
接続先	VPN Gateway
IP アドレス	DCHP 等によって割り当てられたアドレス



### 3.2. Ping

Pingツールを使い、FortiGateのDMZネットワーク内に位置しているWEBサーバに対してPingを実行し、正常通信を確認します。

\*この例では、サーバ10.0.0.100に対してPingを実行しています。また、PingツールはiPhone端末に標準実装されていないため、サードパーティ製のものを利用しています。



### 3.3.WEBアクセス

ブラウザを開き、FortiGateのDMZネットワーク内に位置しているWEBサーバに対してアクセスを実行し、正常に通信が行われているかを確認します。

\*この例では、WEBサーバ(Fortinetナレッジベース)10.0.0.100に対してアクセスを実行しており、正常表示されていることがわかります。

備考

ここで使用しているIPアドレスは検証用に割り当てた仮想IPアドレスですので、実際にインターネット接続を行う際には、プロバイダから割り当てられたIPアドレスをご利用頂きますようお願い致します。