



iPhone IPSec VPN 接続テスト with サイバートラスト デバイスID

Fortinet Japan
Kazunori Miyanishi

Rev. 2
Jul. 26th, 2010

改訂履歴

第 1 版	(05/11/2010)
第 2 版	(07/26/2010)

免責事項

本ドキュメントに関する著作権は、フォーティネットジャパン株式会社へ独占的に帰属します。フォーティネットジャパン株式会社が事前に承諾している場合を除き、形態及び手段を問わず、本ドキュメント又はその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもフォーティネットジャパン株式会社はいかなる責任も負わないものとします。本ドキュメント及びその記述内容は予告なしに変更されることがあります。

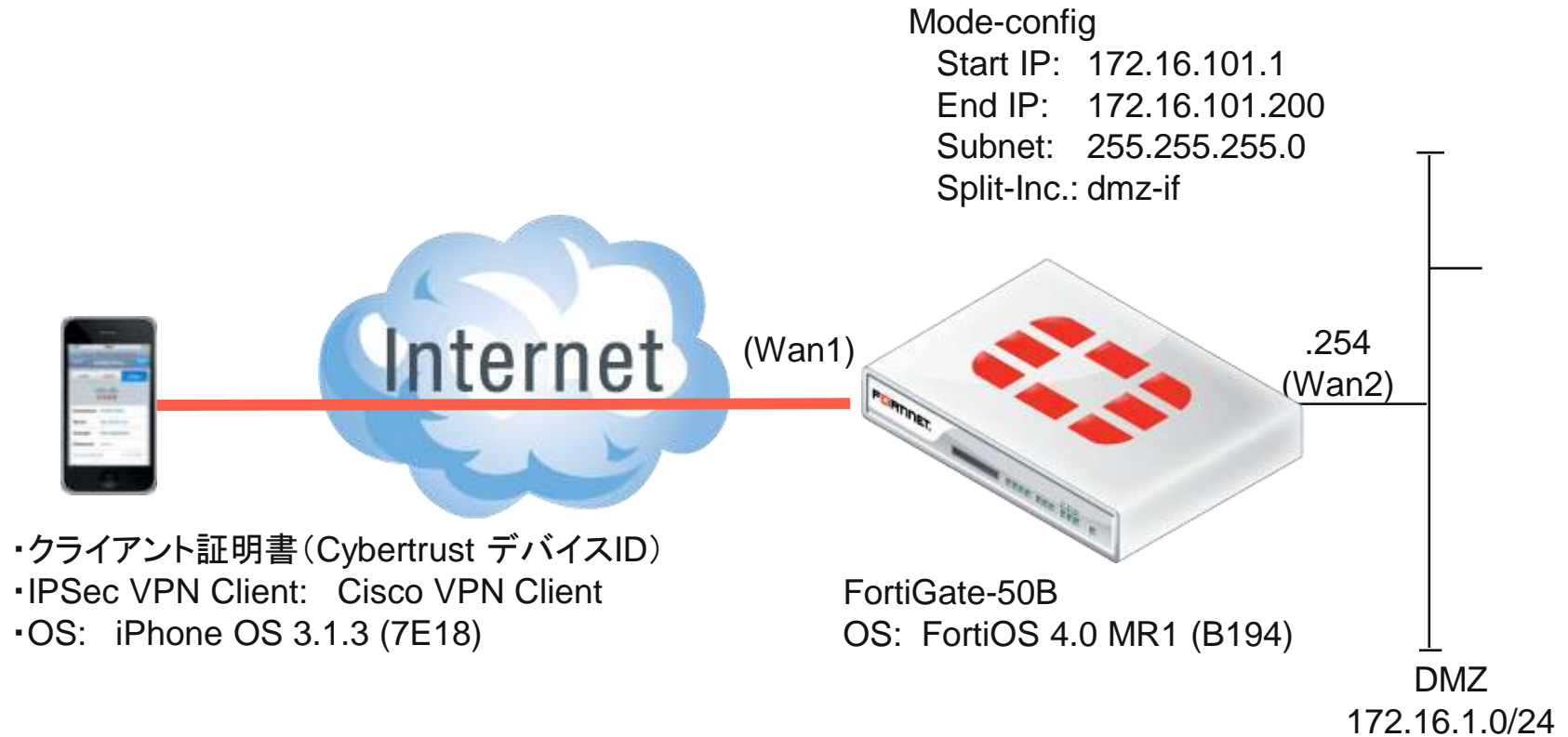
本テストの目的

- iPhone/Cisco VPNとFortiGateとのIPSec接続性テスト
 - サイバートラスト デバイスID(以下、デバイスID)を用いたIPSec VPNの基本的な接続性
 - デバイスIDによるアクセス制御
 - CRLチェック
- ターゲットプラットフォーム
 - Cisco VPN client for iPhone + サイバートラスト デバイスID
 - FortiOS 4.0 MR1

注意)

本テストは、iPhoneでデバイスIDを用いた場合の基本的なIPSec接続性の確認を目的としております。実環境への適用をご検討の際は、実際のご利用条件のもと、事前の検証等を十分に行ってください。

検証構成



本試験では、IPSec接続後、WAN2インターフェースへのアクセス (ping/http) で接続を確認。
(実際には、サーバやネットワークレンジを使用することになります。)

1. 証明書の準備とインストール

ご利用証明書について



- 本資料では、例としてサイバートラスト様のご協力を得て、iPhone IPSec VPN(RSA認証)での要件を満たすデジタル証明書を利用することを前提にしております。予めご了承ください。
- 実際に証明書認証をお使いになる場合は、そのご利用条件等に応じて、認証機関(CA)やシステム管理者様等にご確認ください。

1. 証明書の準備・インストール

ローカル証明書： 証明書要求 (CSR) を作成

ローカル証明のための証明書要求 (CSR) を作成します。
「生成」ボタンをクリックしてください。

The screenshot shows the 'WEB CONFIG' interface for Fortinet devices. The 'ローカル証明書' (Local Certificate) tab is selected. A red box highlights the '生成' (Generate) button. Below the buttons is a table with the following data:

証明書名	サブジェクト	コメント	ステータス
Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	この証明書はファームウェアに埋め込まれおり、すべてのユニットで同じです (固有ではありません)。これは SSL インスペクションが新しいサーバー証明書を生成するときに利用するデフォルトの CA 証明書です。	OK
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FG10000000000000, emailAddress = support@fortinet.com	この証明書は工場出荷時からハードウェアに組み込まれており、このユニット独自のものです。この証明書は適切な CA によって発行されています。	OK
Fortinet_Factory2		このユニットでは使用できません	使用不可
Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	この証明書はファームウェアに組み込まれており、すべてのユニットで同一です (一意ではない)。この証明書は適切な CA によって発行されています。他のどんなユニットもこの証明書を使用してこのユニットの識別を偽装できるため、サーバータイプの機能用に使用することは推奨できません。	OK

ローカル証明書： 証明書要求 (CSR) を作成

ご利用者の条件に合わせて、証明書要求 (CSR) の内容を設定してください。

本ケースでは、

IDタイプ: ホストIP

IP: FortiGateのグローバルIP

キータイプ: 2048ビット

登録方法: ファイルベース

を選択します。

注意) iPhone VPNにおける証明書要件については、認証機関様とご確認ください。

証明書要求を生成する

証明書名	iphone_eval
サブジェクト情報	
IDタイプ	ホストIP
IP	200.100.200.1
オプション情報	
所属部署名	SE
所属組織	FortinetJapan
市町村名	Minato
都道府県名	Tokyo
国/地域	JAPAN (JP)
Eメール	dane@fortinet.com
キータイプ	RSA
キーサイズ	2048ビット
登録方法	<input checked="" type="radio"/> ファイルベース <input type="radio"/> オンラインSCEP

OK キャンセル

ローカル証明書： 証明書要求 (CSR) を作成

作成した証明書要求 (CSR) が「ペンディング」ステータスになりますので、そのファイルを「ダウンロード」して、認証機関に渡します。

The screenshot shows the Fortinet Web Config interface for managing local certificates. A dialog box titled "iphone_eval.csr を開く" is open, asking how to handle the file. The "Save file" option is selected. Below the dialog, a table lists the certificates and their status.

証明書名	ステータス	操作
Fortinet_CA_SSLProxy	OK	検索, 完了
Fortinet_Factory	OK	検索, 完了
Fortinet_Factory2	使用不可	
Fortinet_Firmware	OK	検索, 完了
iphone_eval	ペンディング	ダウンロード

ダウンロード

ローカル証明書： 証明書をインポート

認証機関から証明書を入手したら、FortiGateに「インポート」します。(次ページに続く)

WEB CONFIG

ローカル証明書 リモート証明書 CA証明書 CRL

生成 **インポート**

証明書名	サブジェクト	コメント	ステータス
Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	この証明書はファームウェアに埋め込まれおり、すべてのユニットで同じです(固有ではありません)。これはSSLインスベクションが新しいサーバー証明書を生成するときに利用するデフォルトのCA証明書です。	OK
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FG100C3G08600289, emailAddress = support@fortinet.com	この証明書は工場出荷時からハードウェアに組み込まれており、このユニット独自のものであります。この証明書は適切なCAによって発行されています。	OK
Fortinet_Factory2		このユニットでは使用できません	使用不可
Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	この証明書はファームウェアに組み込まれており、すべてのユニットで同一です(一意ではない)。この証明書は適切なCAによって発行されています。他のどんなユニットもこの証明書を使用してこのユニットの識別を偽装できるため、サーバタイプの機能用に使用することは推奨できません。	OK
iphone_eval			ペンディング

ローカル証明書： 証明書をインポート

認証機関から入手した証明書 (*.pemなど) を、FortiGateに「インポート」してください。

WEB CONFIG

ローカル証明書 リモート証明書 CA証明書 CRL

システム

- ステータス
- ネットワーク
- DHCP
- 設定
- 管理者
- 証明書
- メンテナンス

ルータ

ファイアウォール

UTM

VPN

ユーザ

WAN最適化&キャッ

エンドポイント NAC

ログ&レポート

証明書をインポート

タイプ ローカル証明書

アップロードするファイル 参照...

OK キャンセル

ローカル証明書: 証明書をインポート

ローカル証明書のインストールは完了です。

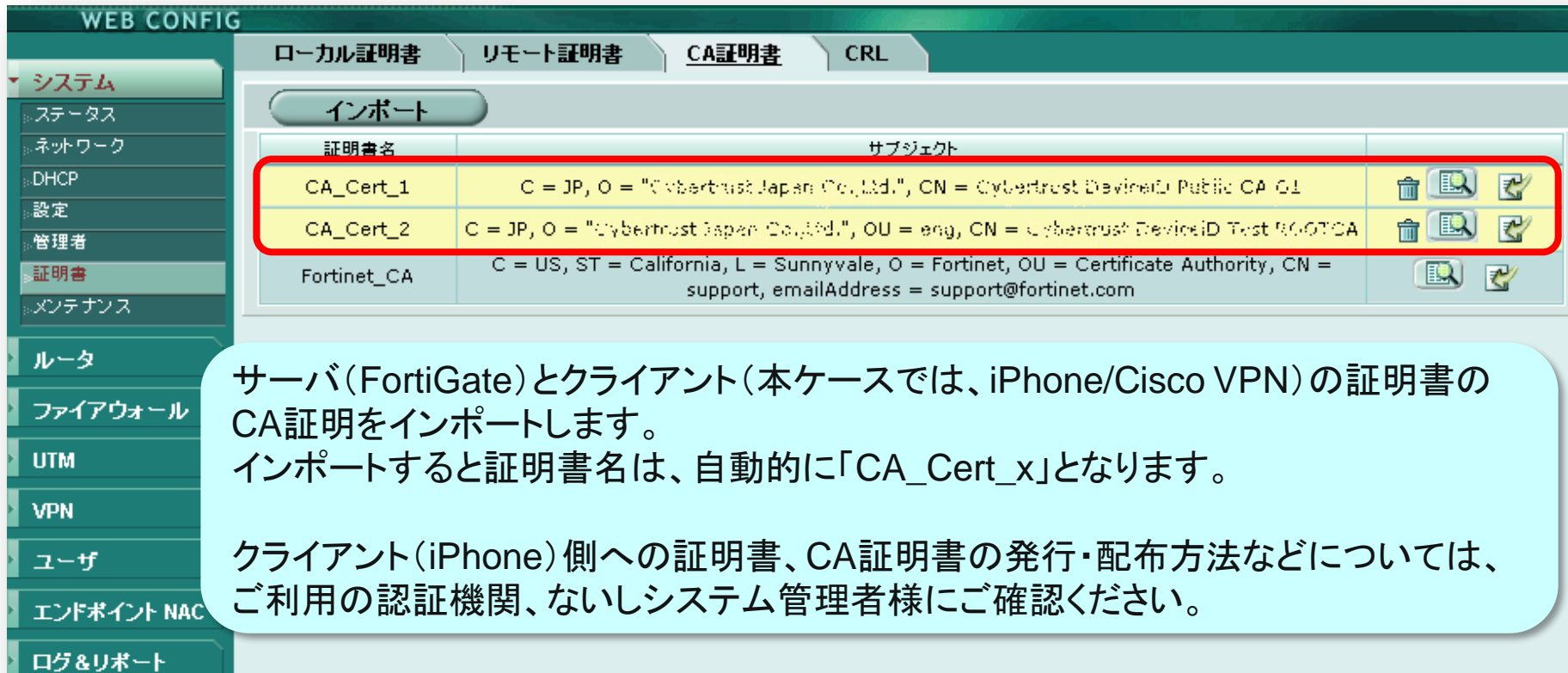
WEB CONFIG

ローカル証明書 リモート証明書 CA証明書 CRL

生成 インポート

証明書名	サブジェクト	コメント	ステータス
Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	この証明書はファームウェアに埋め込まれおり、すべてのユニットで同じです(固有ではありません)。これはSSLインスペクションが新しいサーバー証明書を生成するときに利用するデフォルトのCA証明書です。	OK
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FGT50B3G07520504, emailAddress = support@fortinet.com	この証明書は工場出荷時からハードウェアに組み込まれており、このユニット独自のものです。この証明書は適切なCAによって発行されています。	OK
Fortinet_Factory2		このユニットでは使用できません	使用不可
Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	この証明書はファームウェアに組み込まれており、すべてのユニットで同一です(一意ではない)。この証明書は適切なCAによって発行されています。他のどんなユニットもこの証明書を使用してこのユニットの識別を偽装できるため、サーバータイプの機能用に使用することは推奨できません。	OK
iphone_eval	C = JP, ST = Tokyo, L = Minato, O = Fortinet Japan, OU = SE, CN =		OK









CA証明書： CA証明書をインポート



WEB CONFIG

ローカル証明書 リモート証明書 **CA証明書** CRL

インポート

証明書名	サブジェクト	
CA_Cert_1	C = JP, O = "Cybertrust Japan Co.,Ltd.", CN = Cybertrust DeviceID Public CA G1	  
CA_Cert_2	C = JP, O = "Cybertrust Japan Co.,Ltd.", OU = eng, CN = Cybertrust DeviceID Test ROOTCA	  
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com	 

サーバ(FortiGate)とクライアント(本ケースでは、iPhone/Cisco VPN)の証明書のCA証明をインポートします。
インポートすると証明書名は、自動的に「CA_Cert_x」となります。

クライアント(iPhone)側への証明書、CA証明書の発行・配布方法などについては、ご利用の認証機関、ないしシステム管理者様にご確認ください。

CRL: CRLをインポート

認証機関のCRL提供方法に合わせて、「インポート」してください。
本ケースでは、HTTPを利用します。

The screenshot shows the Fortinet Web Config interface. The left sidebar contains a navigation menu with categories like システム (System), ルータ (Router), and ユーザ (User). The main content area is titled 'WEB CONFIG' and has tabs for 'ローカル証明書' (Local Certificate), 'リモート証明書' (Remote Certificate), 'CA証明書' (CA Certificate), and 'CRL'. The 'CRL' tab is active, and the 'インポート' (Import) button is highlighted with a red box and a red arrow pointing to a dialog box titled 'CRLをアップロード' (Upload CRL). The dialog box contains three options: 'HTTP' (checked), 'LDAP', and 'SCEP'. The 'HTTP' option has a text input field containing 'http://ipkikid.managecsk.ne.jp/mnki/C;bertr...ID'. The 'LDAP' option has a dropdown menu with '[選択してください]' (Please select). The 'SCEP' option has a dropdown menu with 'Fortinet_Firmware' and a text input field for '(SCEPサーバのURL)'. At the bottom of the dialog are 'OK' and 'キャンセル' (Cancel) buttons.

CRL: CRLをインポート

CRLのインストールは完了です。
インポートすると証明書名は、自動的に「CRL_x」となります。

The screenshot shows the Fortinet Web Config interface. The left sidebar contains a navigation menu with items like システム, ステータス, ネットワーク, DHCP, 設定, 管理者, 証明書, メンテナンス, ルータ, ファイアウォール, UTM, VPN, ユーザ, エンドポイント NAC, and ログ&レポート. The main content area is titled 'WEB CONFIG' and has tabs for 'ローカル証明書', 'リモート証明書', 'CA証明書', and 'CRL'. The 'CRL' tab is active, and an 'インポート' button is visible. Below the button is a table with two columns: '証明書名' and 'サブジェクト'. A red box highlights the first row of the table, which contains the text 'CRL_1' and '/C=JP/O=CyberAgent Japan Co.,Ltd./CN=CyberAgent Digital Security Profile CA C1'. To the right of the table row are icons for delete, edit, search, and refresh.

証明書名	サブジェクト
CRL_1	/C=JP/O=CyberAgent Japan Co.,Ltd./CN=CyberAgent Digital Security Profile CA C1

2. ユーザ・ユーザグループの設定

PKI(Peer)ユーザ・グループ作成

PKIユーザを作成します。

本ケースでは、以下のようなPKIユーザを作成。

名前: pki01(任意)

件名: OU = Div-xxx

(OUなどSubjectで制御したい場合)

CA: CA_Cert_1

(インストール済みのクライアント証明書
のCA証明書)

The screenshot shows the Fortinet Web Config interface. On the left is a navigation menu with categories like システム, ルータ, ファイアウォール, UTM, VPN, ユーザ, and エンドポイント NAC. The 'PKI' section is selected, and the '新規作成' (New Creation) button is highlighted with a red box. A red dashed arrow points from this button to a modal dialog box titled '新規PKIユーザ' (New PKI User). The dialog box contains the following fields: '名前' (Name) with the value 'pki01', '件名' (Subject) with the value 'OU = Div-xxx', and 'CA' with a dropdown menu showing 'CA_Cert_1'. Below these fields is a checkbox for '二要素認証' (Two-Factor Authentication) which is currently unchecked. At the bottom of the dialog are 'OK' and 'キャンセル' (Cancel) buttons.

PKI (Peer) ユーザ・グループ作成

PKIグループを作成しますが、CLIで作成する必要があります。

```
# config user peergrp
```

PKIグループ設定コマンド

```
(peergrp) #
```

```
(peergrp) # edit peer-g  
new entry 'peer-g' added
```

PKIグループ(peer-g)を追加

```
(peer-g) #  
(peer-g) # set member pki01
```

PKIグループ(peer-g)に、PKIユーザ(pki01)を追加

```
(peer-g) # get  
name          : peer-g  
member:  
  == [ pki01 ]  
  name: pki01
```

内容確認 (*これは実行必須ではありません)

```
(peer-g) # end
```

設定を確定し終了。

```
#
```

ローカルユーザ・グループ作成

本ケースでは、ローカルユーザ(demo-01)を作成します。

The screenshot displays the Fortinet Web Config interface. On the left is a navigation menu with categories like システム, ルータ, ファイアウォール, UTM, VPN, ユーザ, WAN最適化&キャッチ, エンドポイント NAC, and ログ&レポート. The 'ユーザ' (Users) category is expanded, showing sub-options for ローカル (Local), リモート (Remote), ディレクトリサービス (Directory Services), PKI, ユーザグループ (User Groups), オプション (Options), and モニタ (Monitor). The main area shows the 'ローカル' (Local) tab selected, with a '新規作成' (New) button highlighted by a red box. A red dashed arrow points from this button to a modal dialog titled 'ユーザを追加' (Add User). The dialog contains the following fields and options:

- ユーザ名 (Username): demo-01
- 無効 (Inactive)
- パスワード (Password): [Redacted]
- LDAP: [選択してください] (Please select)
- RADIUS: [選択してください] (Please select)
- TACACS+: [選択してください] (Please select)

At the bottom of the dialog are 'OK' and 'キャンセル' (Cancel) buttons.

ローカルユーザ・グループ作成

WEB CONFIG

ユーザグループ

ユーザグループ(ipsec)を作成します。

新規作成

グループ名	メンバ
ディレクトリサービス	
FSAE_Guest_Users	

ユーザグループを追加

名前: ipsec

タイプ: ファイアウォール

使用可能なユーザ/グループ

- ローカルユーザ - demo-02
- RADIUS/LDAP/TACACS+サーバ上のユーザ -
- PKIユーザ - pki01

メンバ

- ローカルユーザ - demo-01
- RADIUS/LDAP/TACACS+サーバ上のユーザ -
- PKIユーザ -

FortiGuardウェブフィルタリングをオーバーライド

OK キャンセル

3. IPSec VPNの設定

IPSec: フェーズ1の設定の前に

IPSecやファイアウォールポリシーの設定の前に、WAN2のインターフェースのファイアウォールアドレス「dmz-if」を作成します。
(実際には、使用条件に基づいて、アドレスなど各オブジェクトを作成してください。)

The screenshot shows the 'WEB CONFIG' interface with a sidebar on the left containing menu items: システム, ルータ, ファイアウォール (expanded), ポリシー, アドレス, サービス, スケジュール, トラフィックシェーパ, バーチャルIP, ロードバランス, プロテクションプロファイル, UTM, VPN, ユーザ, エンドポイントNAC, and ログ&レポート. The main area is titled 'アドレス' and 'グループ' with a '編集' button. The configuration form contains the following fields:

アドレス名	dmz-if
タイプ	サブネット/IP範囲指定 ▼
サブネット/IP範囲指定	172.16.1.254/255.255.255.255
インタフェース	wan2(dmz) ▼

At the bottom of the form are two buttons: 'OK' and 'キャンセル'.

IPSec: フェーズ1の設定

WEB CONFIG

自動鍵(IKE) | 手動鍵 | コンソレータ | モニタ

システム
ルータ
ファイアウォール
UTM
VPN
IPsec
SSL
ユーザ
エンドポイント NAC
ログ&レポート

フェーズ1を編集

名前	p1
リモートゲートウェイ	ダイヤルアップユーザ
ローカルインタフェース	wan1
モード	<input type="radio"/> アグレッシブ <input checked="" type="radio"/> メイン(IDプロテクション)
認証方法:	RSAシグネチャ
証明書名	iphone_eval

ピアオプション

- あらゆるピアIDを受け入れる
- このピアIDを受け入れる peer-g
- このピア証明書のみを受け入れる pki01
- このピアの証明書グループのみを受け入れる peer-g

特別オプション (XAUTH, NATトラバーサル, DPD)

インストールした証明書

作成したPKIグループ

リモートゲートウェイ: ダイヤルアップユーザ
ローカルインタフェース: wan1
モード: メイン
認証方法: RSAシグネチャ
証明書: 「iphone_eval」
ピアオプション: このピアの証明書グループを受け入れる「peer-g」

IPSec: フェーズ1の設定(特別オプション)

The screenshot shows the 'WEB CONFIG' interface for configuring IPSec Phase 1 Special Options. The left sidebar lists various system settings, with 'VPN' expanded to show 'IPsec'. The main panel is titled '特別オプション (XAUTH, NATトラバーサル, DPD)' and includes the following settings:

- IPSecインターフェースモードを有効にする** (Callout: インターフェースモードを有効化)
- IKEバージョン: 1 2
- ローカルゲートウェイIP: メインインターフェースIP 指定
- フェーズ1**
 - 1 - 暗号化: 3DES 認証: SHA1
 - 2 - 暗号化: AES128 認証: SHA1
 - 3 - 暗号化: AES256 認証: SHA1
- DHグループ: 1 2 5 14
- 鍵の有効時間: 28800 (120-172800 秒)
- ローカルID: (オプション)
- ローカルID: C = JP, ST = Tokyo, L = Minato, O = Fortinet Japan, OU = SE, CN =
- XAUTH**: 停止する クライアントを有効にする サーバを有効にする (Callout: XAUTHを設定)
- サーバタイプ: PAP CHAP AUTO
- ユーザグループ: ipsec (Callout: 作成したローカルユーザグループ)
- NATトラバーサル: 有効
- キーアライブの頻度: 10 (10-900 秒)
- デッドピアディテクション(DPD): 有効

Buttons at the bottom: OK, キャンセル

IPSec: フェーズ1の設定(mode-cfg)

IPSecクライアントへの仮想IPアドレスなどのアサインのため、IKE Mode Configを利用します。
(CLIでのみ設定可能)

```
# config vpn ipsec phase1-interface
```

IKE フェーズ1インターフェースの設定

```
(phase1-interface) # edit p1
```

```
(p1) #
```

```
(p1) # set mode-cfg enable
```

IKE Mode Configを有効

```
(p1) # set ipv4-start-ip 172.16.101.1
```

仮想IPレンジの「**開始アドレス**」を指定

```
(p1) # set ipv4-end-ip 172.16.101.200
```

仮想IPレンジの「**終了アドレス**」を指定

```
(p1) # set ipv4-netmask 255.255.255.0
```

仮想IPレンジの「**ネットマスク**」を指定

```
(p1) # set ipv4-split-include dmz-if
```

IPSecユーザにアクセスさせるネットワーク

```
(p1) # end
```

```
#
```

IPSec: フェーズ2の設定

WEB CONFIG

自動鍵(IKE) | 手動鍵 | コンソレレータ | モニタ

システム
ルータ
ファイアウォール
UTM
VPN
IPsec
SSL
ユーザ
エンドポイント NAC
ログ&レポート

フェイズ 2を編集

名前: p2
フェイズ 1: p1

作成したフェーズ1を指定

特別オプション

フェーズ2

1-暗号化: 3DES | 認証: SHA1
2-暗号化: AES128 | 認証: SHA1
3-暗号化: AES256 | 認証: SHA1

リプレイ検知を有効にする
 PFSを有効にする

DHグループ 1 2 5 14

鍵の有効時間: 秒 1800 (秒) 5120 (キロバイト)

自動鍵キーブアライブ 有効
DHCP-IPsec 有効

クイックモードセクタ

送信元アドレス: 0.0.0.0/0
送信元ポート: 0
宛先アドレス: 0.0.0.0/0
宛先ポート: 0
プロトコル: 0

OK | キャンセル

4. ポリシーの設定

ポリシーの設定の例:

ルートベース(インターフェースモード)IPSecのポリシーを作成します。

The screenshot shows the Fortinet Web Config interface for configuring an IPSec policy. The left sidebar contains a navigation menu with categories like システム, ルータ, ファイアウォール, UTM, VPN, ユーザ, エンドポイント NAC, and ログ&レポート. The main area is titled 'WEB CONFIG' and has tabs for 'ポリシー', 'DoS ポリシー', 'Sniffer ポリシー', and 'IPv6 ポリシー'. The 'ポリシー' tab is active, showing a 'ポリシー追加' (Add Policy) form. The form fields are as follows:

送信元インターフェース/ゾーン	p1
送信元アドレス	all
宛先インターフェース/ゾーン	wan2(dmz)
宛先アドレス	dmz-if
スケジュール	always
サービス	ANY
アクション	ACCEPT

Below the form, there are several checkboxes and dropdown menus:

- NAT
- ダイナミックIPプール
- アイデンティティベースポリシーを有効にする
- プロテクションプロファイル: unfiltered
- トラフィックシェーピング: [選択してください]
- リバーストラフィックシェーピング: [選択してください]
- Per-IP トラフィックシェーピング: [選択してください]
- 許可トラフィックをログ
- エンドポイントNACを有効: [選択してください]

Callouts in the image point to specific settings:

- フェーズ1インターフェース「p1」を指定 (Phase 1 interface 'p1')
- 宛先にWAN2を指定 (Specify WAN2 as destination)
- 「dmz-if」を指定 (Specify 'dmz-if')
- 「ACCEPT」* を指定 (Specify 'ACCEPT'*)



以上で、FortiGate側の設定は完了です。

iPhoneに必要な証明書をインストールした後、Cisco VPNで、サーバ(トンネルエンドポイント)、アカウント(ユーザ名)、パスワード、証明書(デバイスID)を設定することで接続可能となります。

なお、デバイスIDのOUによるアクセス制御も確認しております。