FortiGate(OS 7.2)における クライアント証明書認証設定 手順

2025 年 01 月 22 日

Ver. 2.00

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	
Ver. 1.10	2024/12/6	CRL 更新間隔の設定方法について追記	
Ver. 2.00	2025/1/22	ルート、中間証明書および CRL を新認証局(G2)に変更	

<目　次>

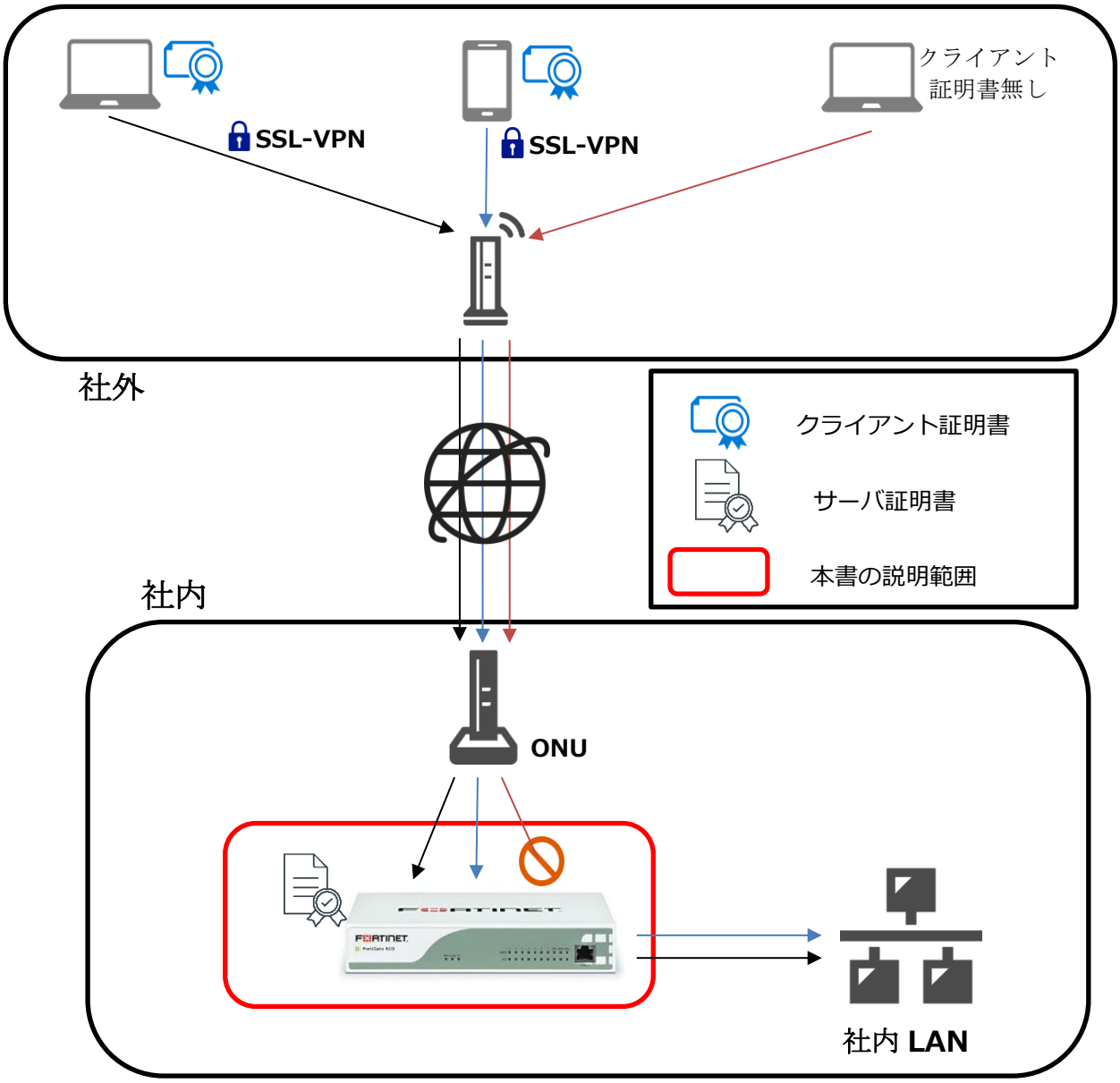
1. 概要 3
2. 事前準備 4
3. クライアント証明書認証をするための設定手順 6
3.1. 証明書メニューの有効化 7
3.2. 証明書のインポート 8
3.3. PKI ユーザの作成 15
3.4. グループの作成 17
3.5. SSL-VPN の設定 18
3.6. ポリシーの設定 19
4. ユーザ側での準備 20
4.1. Windows（Windows11） 21
4.2. iOS（iOS16.2） 22
4.3. Android（Android11） 26
5. サーバ証明書の入れ替え手順 29
5.1. 新しいサーバ証明書のインポート 30
5.2. サーバ証明書の設定 32

1. 概要

本書は Fortinet 社が提供している FortiGate(OS7.2)における SSL-VPN 機能について、クライアント証明書認証設定手順を説明いたします。

あくまで一例としてご紹介させていただいておりますので、詳細な設定等は FortiGate の販売店もしくはメーカーへお問い合わせください。

【構成イメージ】



2. 事前準備

■SSL サーバ証明書

初期状態では自己署名のサーバ証明書が入っていますが、信頼性の観点から証明書ベンダーから調達することを推奨します。インストールする際には、PEM 形式に変換する必要があります。

■ルート証明書（G2）

以下 URL よりダウンロードしてください。

・https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt

■中間証明書

ご利用中の中間認証局の証明書を以下の URL からダウンロードしてください。

・中間証明書(CA3 G2)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt

・中間証明書(CA4 G2)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt

■失効リスト配布 URL

失効リストをインポートする際に使用します。

・中間認証局(CA3 G2)
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl

・中間認証局(CA4 G2)
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl

【ご利用中の中間認証局の確認方法】

以下画像の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックしていただくと、適用されているサービス名が表示されます。サービス名の後に**（CA4）**という表記があれば CA4 G2、なければ CA3 G2 をご利用いただいております。

3. クライアント証明書認証をするための設定手順

本項から詳細な設定手順に関する説明になります。

流れは次の通りです。

1. 証明書メニューの有効化 7
FortiGate にて証明書を利用できるように設定します。

2. 証明書のインポート 8
準備していただいた SSL サーバ証明書、ルート証明書、中間証明書、失効リストをインポートします。

3. PKI ユーザの作成 15
SSL-VPN を利用するユーザを登録します。

4. グループの作成 17
登録した SSL-VPN を利用するユーザのグループを作成します。

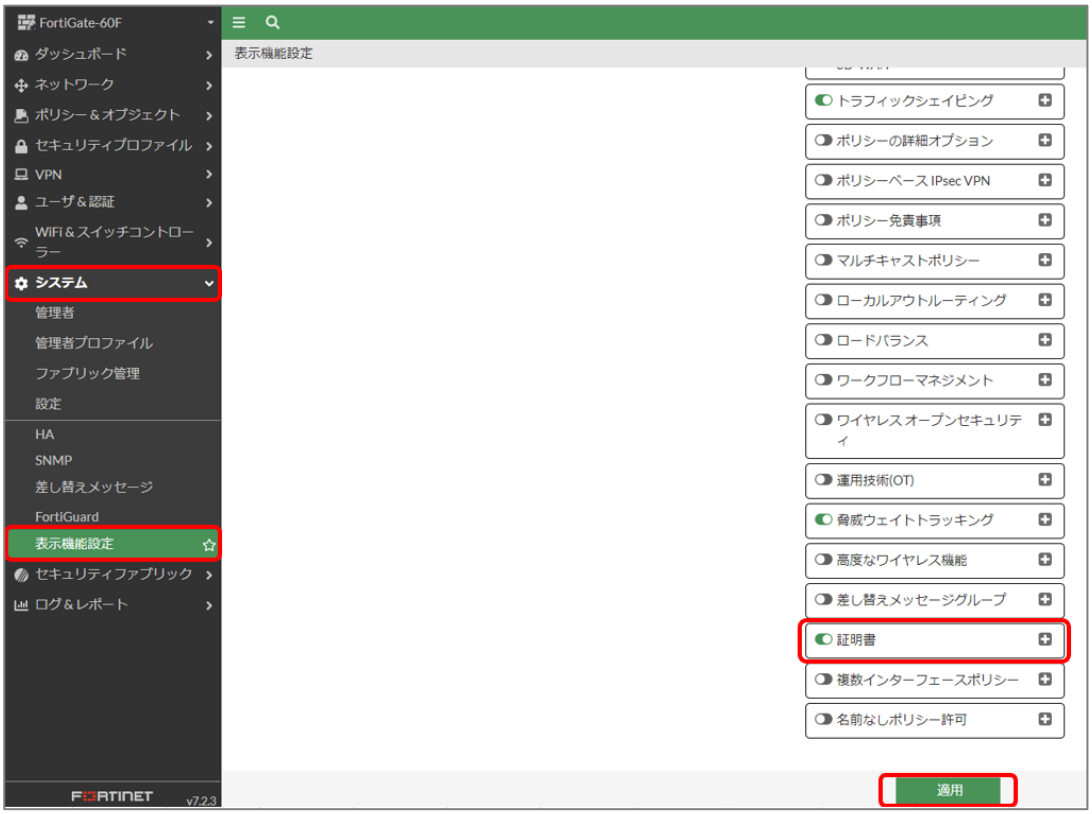
5. SSL-VPN の設定 18
SSL-VPN の機能に関する詳細設定をします。

6. ポリシーの設定 19
SSL-VPN を利用時のアクセスに関するルールを作成します。

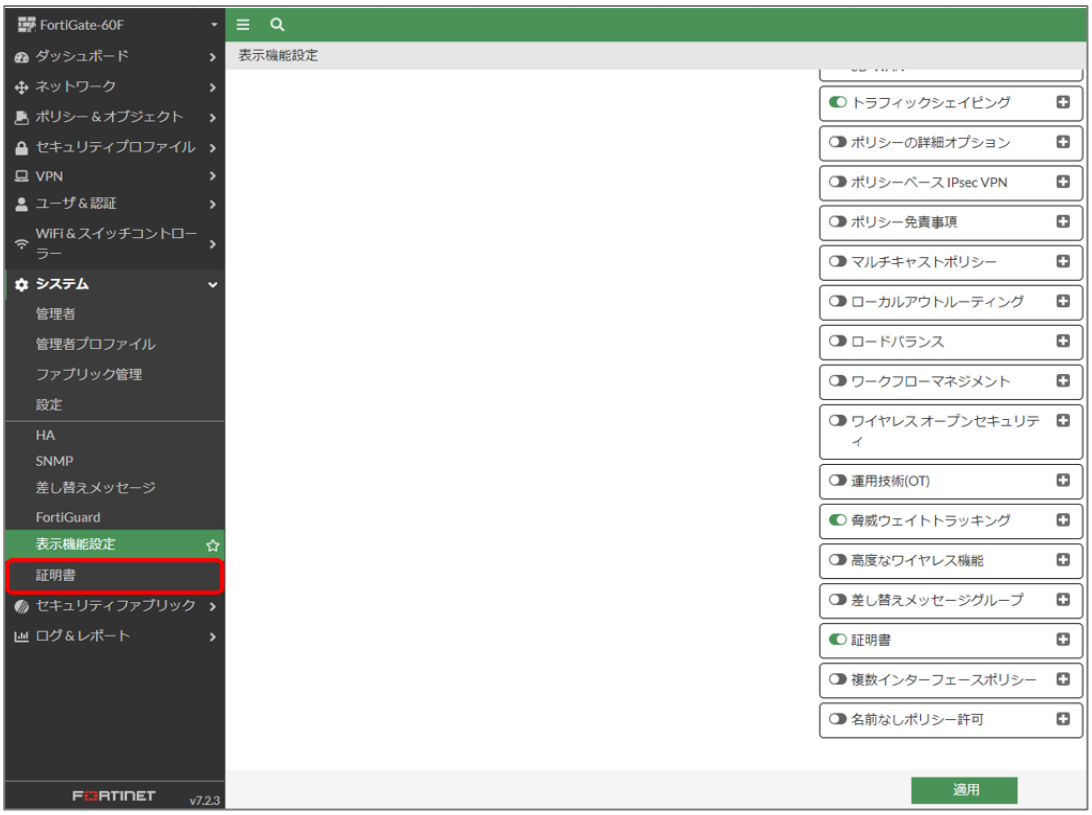
項目は以上です。次ページから各項目の説明の記載になります。

3.1. 証明書メニューの有効化

管理画面から「システム」-「表示機能設定」より証明書を有効化し適用をクリックします。



下図のように「表示機能設定」の下に「証明書」の項目が表示されます。

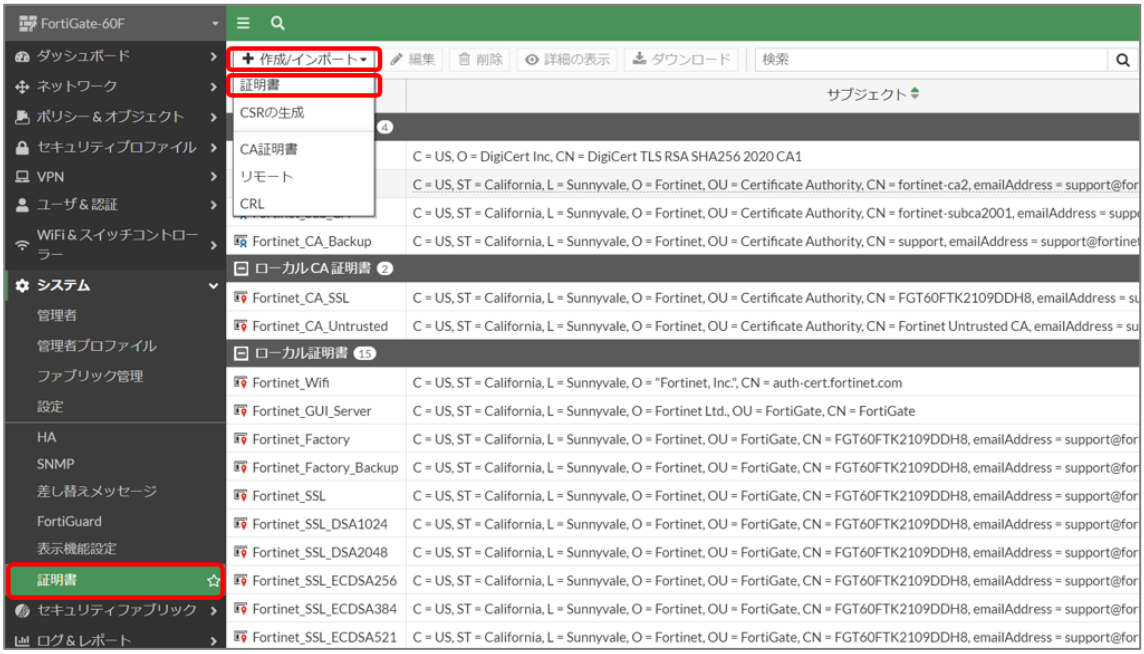


3.2. 証明書のインポート

事前準備で用意した各証明書と CRL(失効リスト)をインポートします。

■サーバ証明書

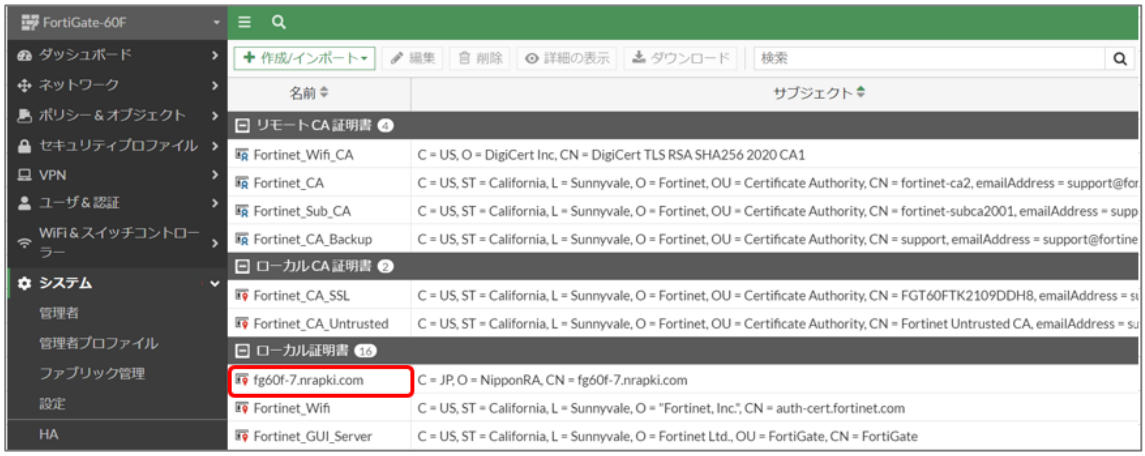
「システム」-「証明書」を選択し、「作成/インポート」から「証明書」を選択します。



「証明書をインポート」を選択します。

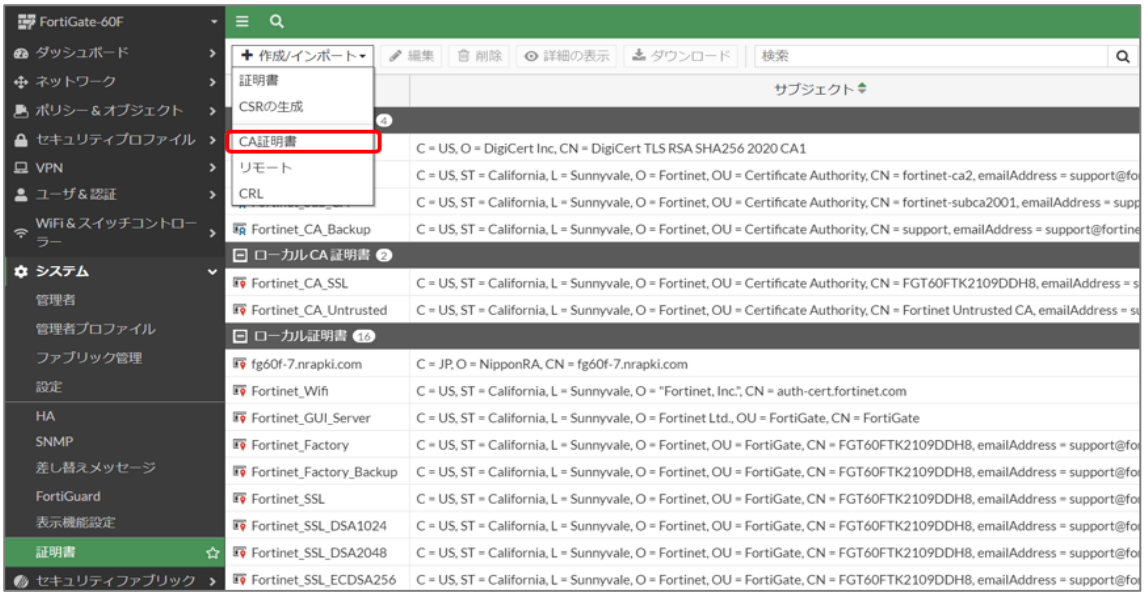
「証明書の作成」画面が表示されます。「証明書」を選択し、証明書ファイル、キーファイル、パスワード(任意)を指定し作成をクリックします。

サーバ証明書がインポートされたことを確認します。

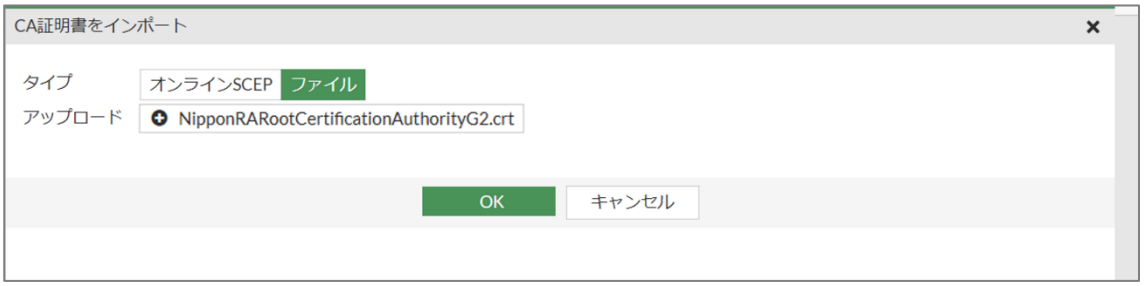


■ルート証明書、中間証明書

「システム」-「証明書」を選択し、「作成/インポート」から「CA 証明書」を選択します。

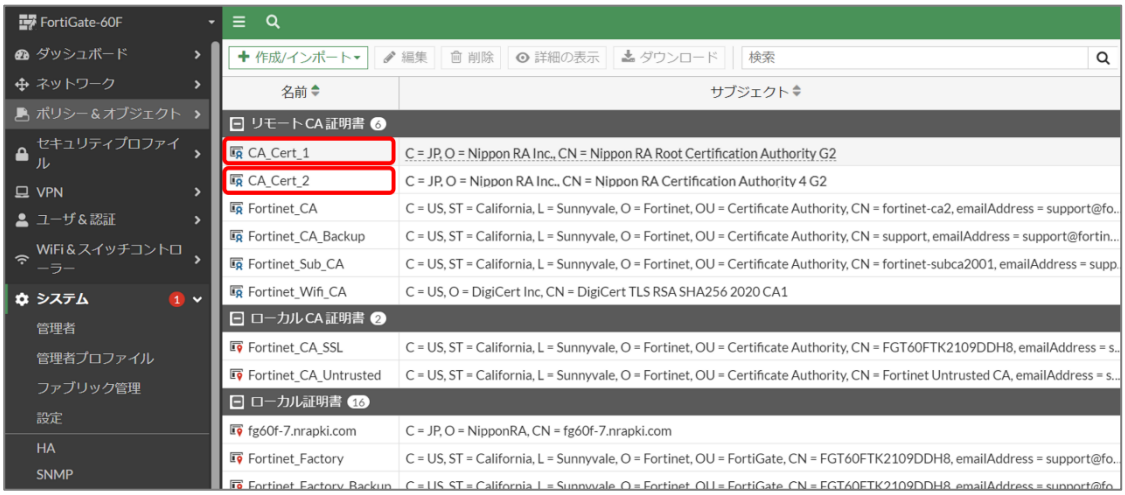


「ファイル」を選択し、ルート証明書を指定し OK をクリックします。



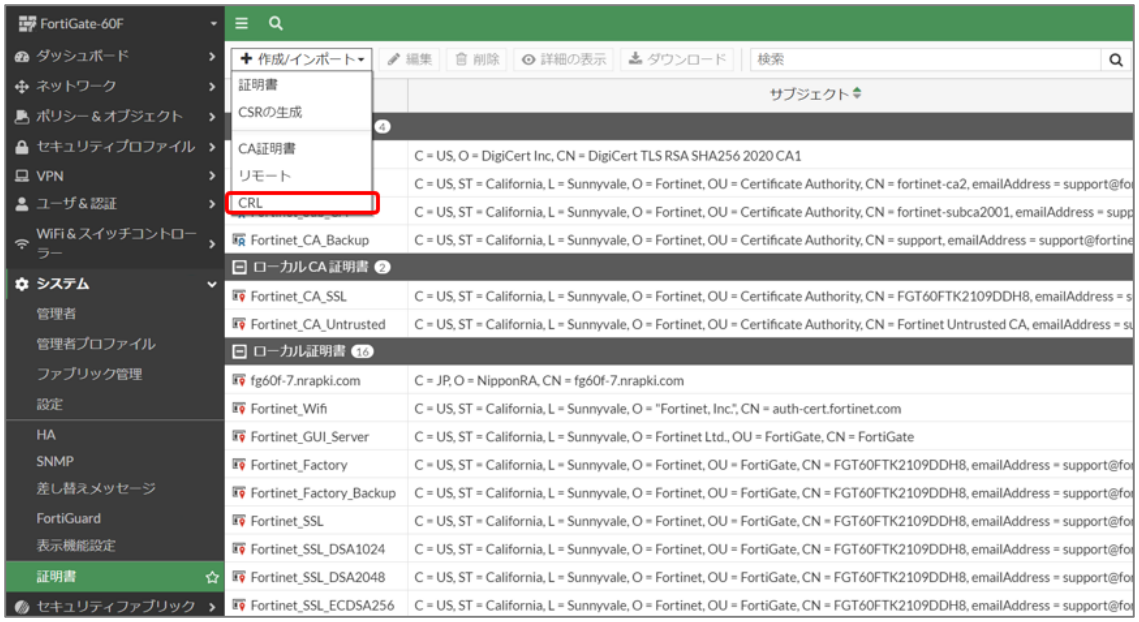
同手順にて中間証明書もインポートします。

ルート証明書、中間証明書がインポートされたことを確認します。



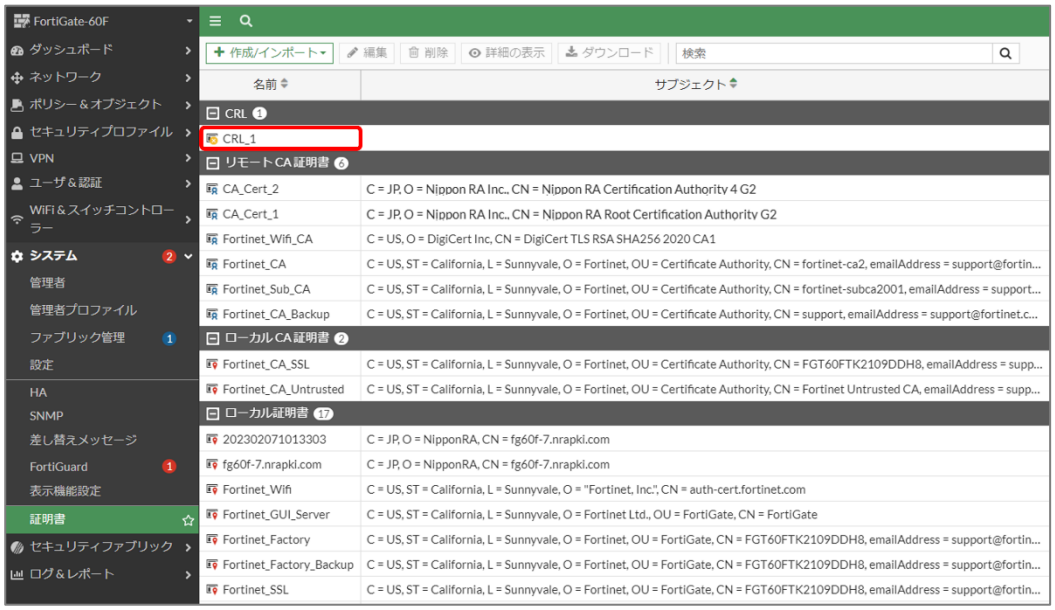
■CRL(失効リスト)

「システム」-「証明書」を選択し、「作成/インポート」から「CRL」を選択します。



「オンライン更新」-「HTTP」を選択し、CRL 配布ポイントの URL を入力し、OK をクリックします。

CRL がインポートされたことを確認します。



【補足】

既定の CRL の更新間隔は CRL の有効期限毎（NRA-PKI では 10 日間）となります。

■CRL 更新間隔の設定方法

CLI コンソールを使って以下コマンドを<>の中を実際の値にして設定します。

「update-interval」に更新間隔（秒）を指定してください。

config vpn certificate crl

edit <CRL の登録名>

set update-interval <任意の値>

next

end

設定が変更されているかを確認します。

■確認コマンド

show vpn certificate crl

【設定確認画面(例)】

CRL_1 の更新間隔（update-interval）を 3600（秒）に設定

```
FortiGate-60F  # show vpn certificate crl CRL_1
config vpn certificate crl
    edit "CRL_1"
        set range global
        set http-url "http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl"
        set update-interval 3600
    next
end
```

CRL(失効リスト)がうまく取得できない場合は OCSP レスポンダをお試しください。

OCSP レスポンダ URL
http://mpkiocsp.managedpki.ne.jp/mpkiocsp

■OCSP レスポンダの設定方法
CLI コンソールを使って以下コマンドを<>の中を実際の値にして設定します。

config vpn certificate ocsp-server
edit <任意の値>※画像では mpki_ocsp
set url http://mpkiocsp.managedpki.ne.jp/mpkiocsp
set cert <中間 CA の登録名>
set unavail-action revoke
end
exit

設定が変更されているかを確認します。

■確認コマンド①
config vpn certificate ocsp-server
edit <設定した任意の値>
get

【設定完了画面①(例)】

```
FortiGate-60F (mpki_ocsp) # get
name                : mpki_ocsp
url                 : http://mpkiocsp.managedpki.ne.jp/mpkiocsp
cert                : CA_Cert_2
secondary-url       :
secondary-cert      :
unavail-action      : revoke
source-ip           : 0.0.0.0
```

■確認コマンド②

config vpn certificate setting

get

【設定完了画面②(例)】

```
FortiGate-60F (setting) # get
ocsp-status          : enable
ocsp-option          : server
ocsp-default-server  : mpki_ocsp
interface-select-method: auto
check-ca-cert        : enable
check-ca-chain       : disable
subject-match        : substring
subject-set          : subset
cn-match             : substring
cn-allow-multi       : enable
crl-verification:
    expiry               : ignore
    leaf-crl-absence     : ignore
    chain-crl-absence    : ignore
strict-ocsp-check    : disable
ssl-min-proto-version: default
cmp-save-extra-certs: disable
cmp-key-usage-checking: enable
cert-expire-warning  : 14
certname-rsa1024     : Fortinet_SSL_RSA1024
certname-rsa2048     : Fortinet_SSL_RSA2048
certname-rsa4096     : Fortinet_SSL_RSA4096
certname-dsa1024     : Fortinet_SSL_DSA1024
certname-dsa2048     : Fortinet_SSL_DSA2048
certname-ecdsa256    : Fortinet_SSL_ECDSA256
certname-ecdsa384    : Fortinet_SSL_ECDSA384
certname-ecdsa521    : Fortinet_SSL_ECDSA521
certname-ed25519     : Fortinet_SSL_ED25519
certname-ed448       : Fortinet_SSL_ED448
```

差異がある場合は以下コマンドを参考に変更してください。

config vpn certificate setting

set ocsp-status enable

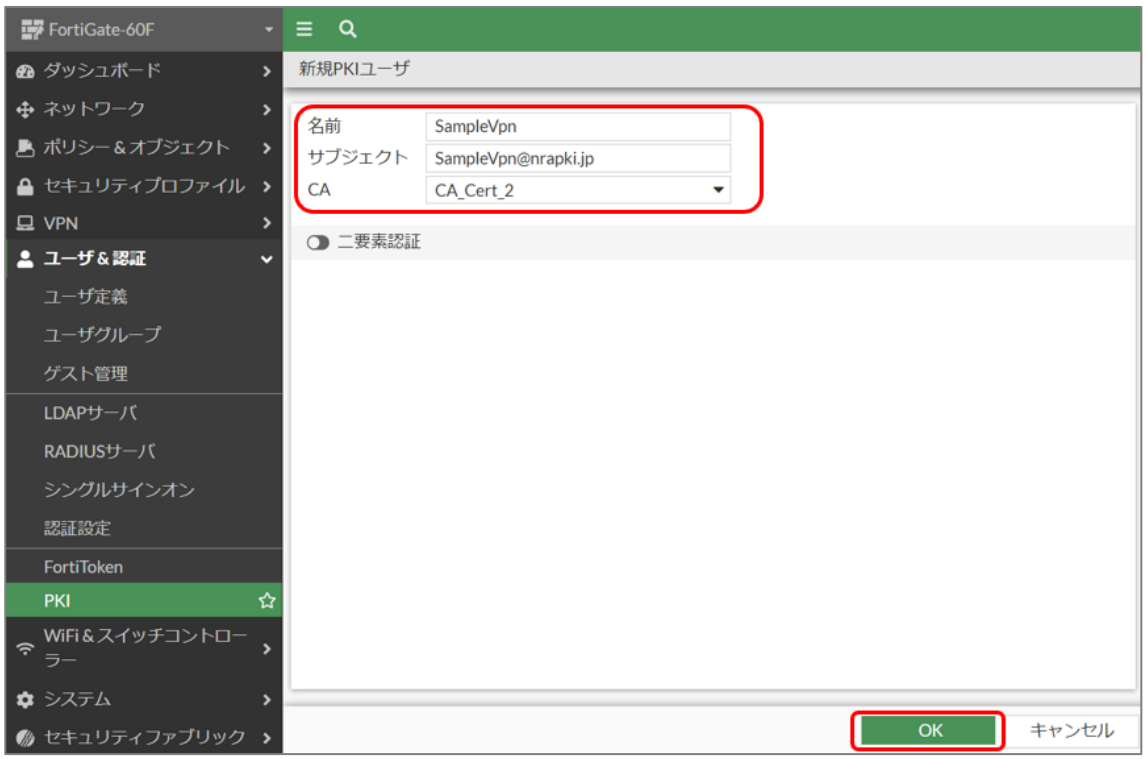
end

exit

3.3. PKI ユーザの作成

「ユーザ&認証」-「PKI」を選択し、「新規作成」を選択します。

下図の赤枠内の項目を設定し OK をクリックします。



■設定例

名前：任意の値

サブジェクト：任意の値　※【補足 1】参照

CA：インポートした中間証明書

※二要素認証は必要に応じて設定してください。

【補足 1】サブジェクトについて

認証する証明書をサブジェクトにより制限します。証明書のサブジェクト O（会社名）で制限する場合は、『O = xxxxxxx』の形式で入力して下さい。サブジェクト E(メールアドレス)で判断する場合には『xxxx@xx.xx』のように、E=などは入力せずメールアドレスのみ入力してください。

空欄の場合、CA で設定した中間証明書の認証局で発行した証明書を認証します。

【補足 2】

「ユーザ&認証」に「PKI」の項目がない場合は、CLI から以下コマンドにて一度登録してください。

登録後に管理画面からログアウトし、再度ログインすると管理画面に「PKI」の項目が表示されます。

config user peer

edit <ユーザ名> ※任意の値

set ca CA_Cert_1（CA_Cert_1 は中間証明書。必要に応じて名前は変更）

<Email アドレス>（あとで UI で変更可能。今設定しなくても OK。）

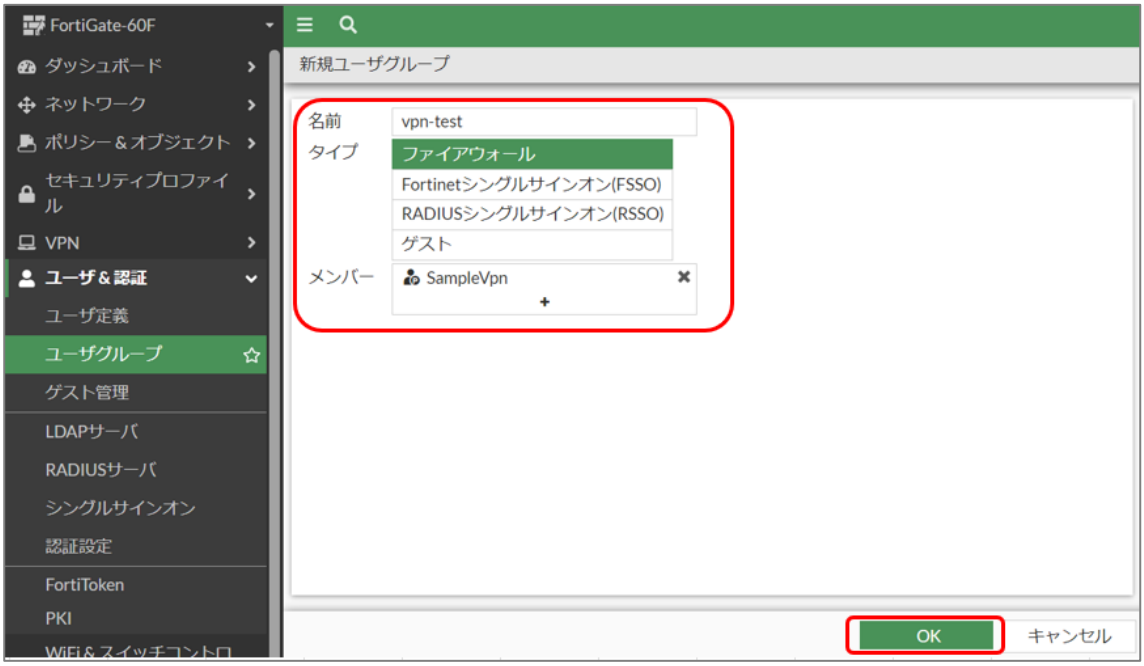
end

exit

3.4. グループの作成

「ユーザ&認証」-「ユーザグループ」から「新規作成」を選択します。

下図の赤枠内の項目を設定し OK をクリックします。



■設定例

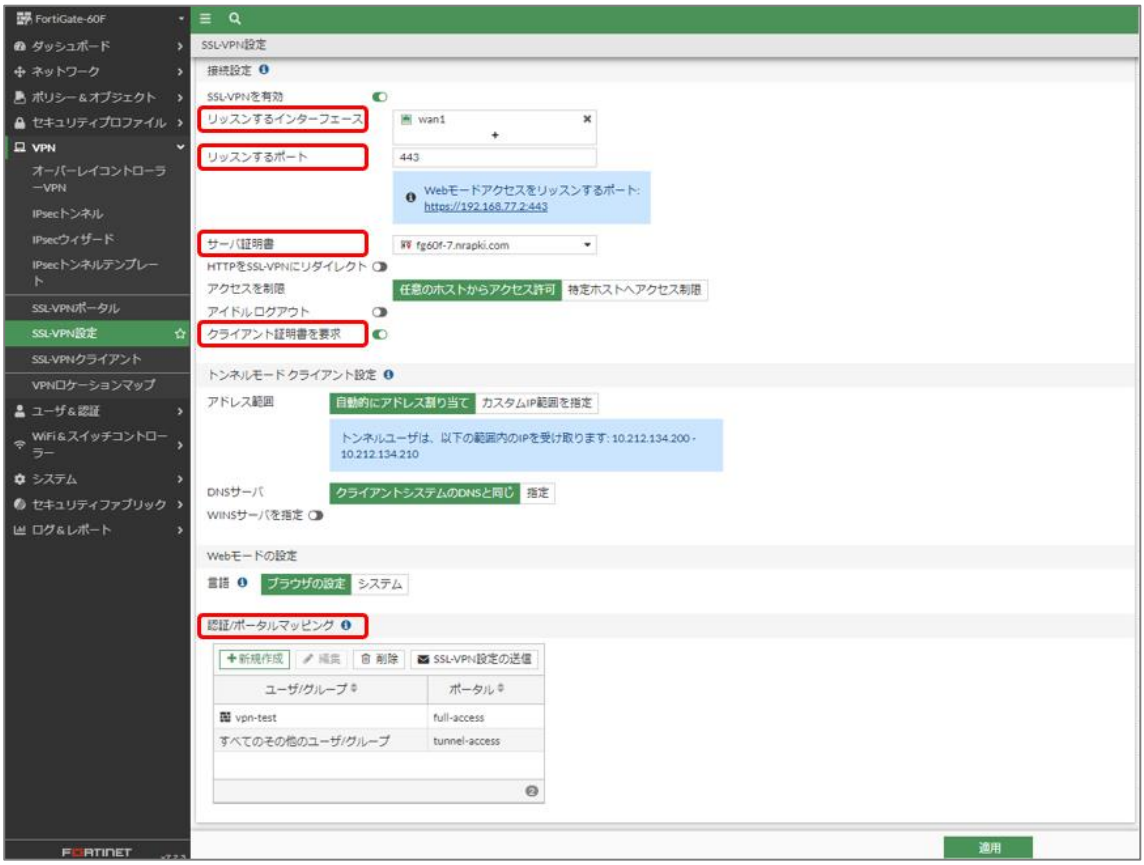
名前：任意の値

タイプ：ファイアウォール

メンバー：作成した PKI ユーザを選択

3.5. SSL-VPN の設定

「VPN」-「SSL-VPN 設定」から下図の赤枠の項目を設定し「適用」をクリックします。



■設定例

リッスンするインターフェース：wan1

リッスンするポート：任意（後述「ユーザ側での準備」で使用します）

サーバ証明書：インポートしたサーバ証明書を選択

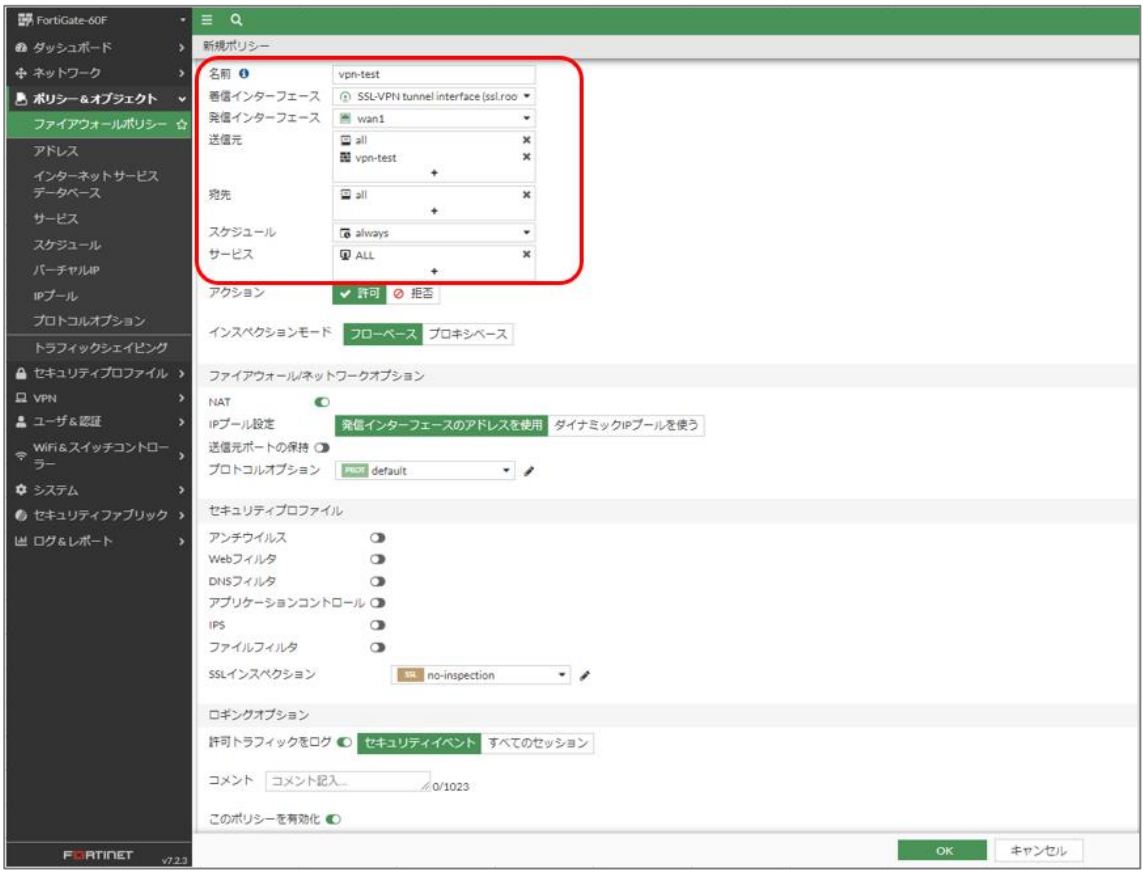
クライアント証明書を要求：チェック

認証/ポータルマッピング：新規作成をクリックし、「ユーザ/グループ」は作成した PKI ユーザが入っているグループ、ポータルは任意で設定

3.6. ポリシーの設定

「ポリシー&オブジェクト」-「ファイアウォールポリシー」から「新規作成」を選択します。

下図の赤枠内の項目を設定し OK をクリックします。



■設定例

着信インターフェース：SSL-VPN トンネルインターフェース

発信インターフェース：wan1（内側の設定は lan）

送信元：all、SSLVPN-UserGroup

宛先：all（スプリットトンネリング使う際は接続先アドレスを指定）

スケジュール：always

サービス：ALL

※その他の項目は任意で設定してください。

以上で FortiGate(OS7.2)における SSL-VPN 機能の設定は完了です。

4. ユーザ側での準備

本項はユーザ側の端末で使用する FortiClient の設定手順の説明になります。

流れは次の通りです。

4.1. Windows（Windows11） 21
Windows 端末における FortiClient の設定をします。

4.2. iOS（iOS16.2） 22
iOS 端末における FortiClient の設定をします。

4.3. Android（Android11） 26
Android 端末における FortiClient の設定をします。

項目は以上です。次ページから各項目の説明の記載になります。

4.1. Windows（Windows11）

ご利用の Windows 端末にて FortiClient をダウンロード･インストールしてください。

FortiClient を起動し、「新規接続の追加」より、以下を参考に設定を追加してください。

■設定例

VPN：SSL-VPN

接続名：任意の値

説明：任意の値

リモート GW：FortiGate のグローバル IP アドレス

ポートの編集：チェックを入れ、SSL-VPN 設定で設定した「リッスンするポート」を指定

クライアント証明書：PKI ユーザ作成時に指定した証明書を選択

認証：任意

4.2. iOS（iOS16.2）

■クライアント証明書のインポート

FortiClient へのクライアント証明書のインポートは iTunes を使用します。iOS 標準のプロファイル（証明書ストア）にインストールしたクライアント証明書は FortiClient で指定できません。

iTunes を実行するデバイス（例：WindowsPC）の任意のローカルフォルダにクライアント証明書ファイル（拡張子 P12 形式）を配置してください。

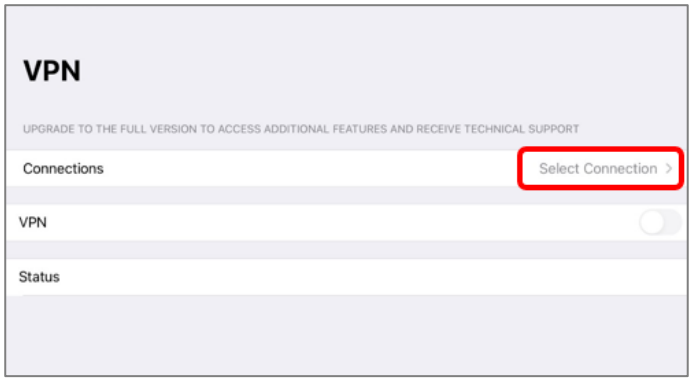
iOS 端末を USB で接続し、iTunes を起動し「ファイル共有」-「FortiClientVPN」を選択してください。

「ファイルを追加」よりクライアント証明書を指定し、クライアント証明書がインポートされたことを確認し「同期」をクリックしてください。

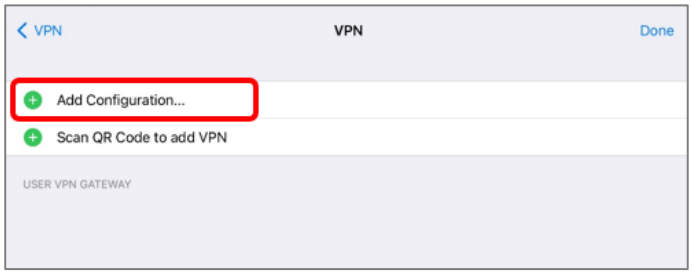
以上でクライアント証明書のインポートは完了です。

ご利用の iOS 端末にて FortiClient をダウンロード･インストールしてください。

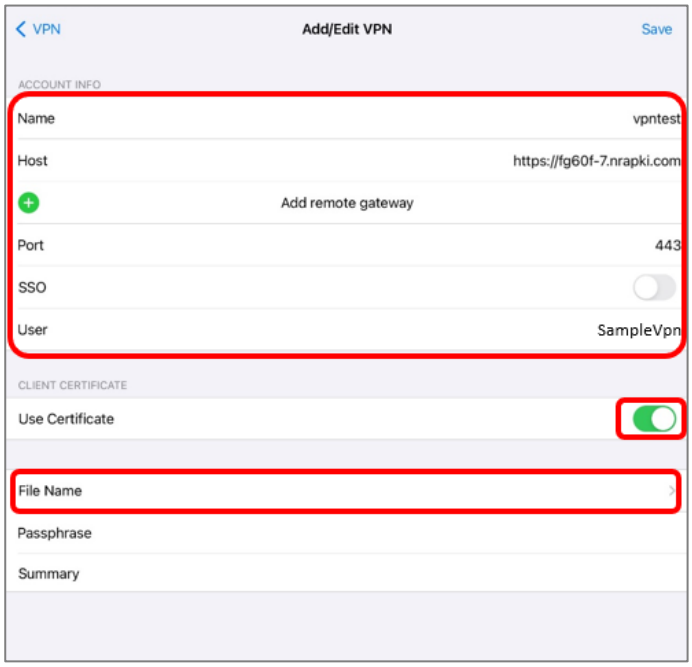
FortiClient を起動し、「Select Connection」をタップします。



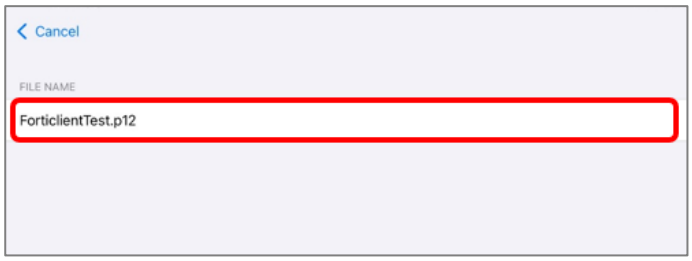
「Add Configuration」をタップします。



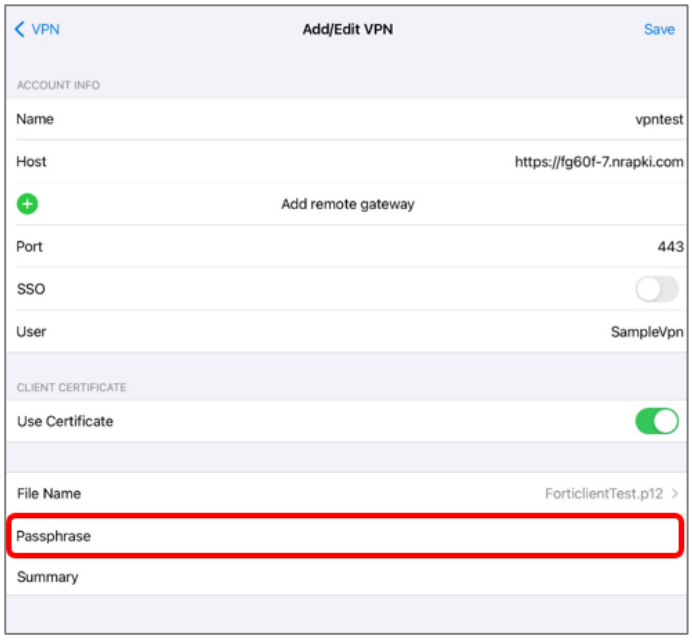
下図の赤枠内の項目を入力し「Use Certificate」を有効にし、「File Name」をタップします。



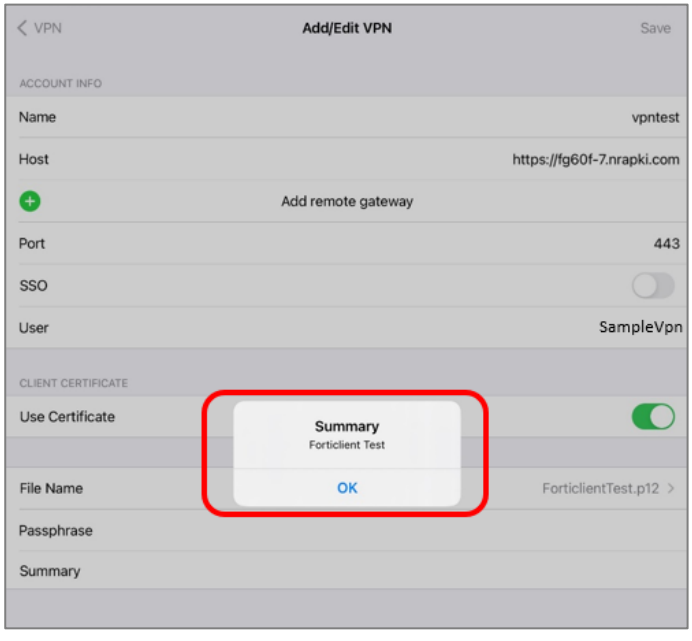
事前にインポートしたクライアント証明書を選択します。



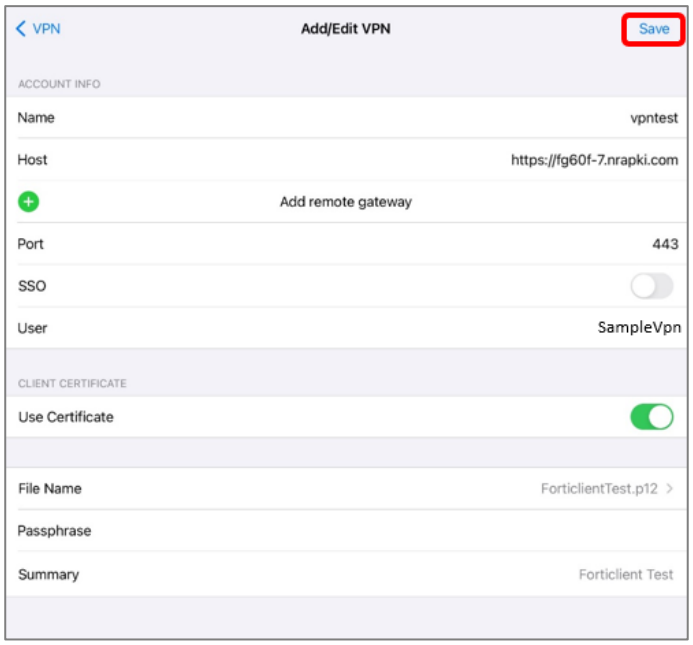
「Passphrase」にクライアント証明書のパスワードを入力してください。



クライアント証明書のコモンネームを確認して「OK」をタップします。



「Save」をタップします。



以上で iOS 端末における FortiClient の VPN 設定は完了です。

■設定例

Name：任意の値

Host：FortiGate の FQDN

Port：SSL-VPN 設定で設定した「リッスンするポート」を指定

SSO：任意

User：SSL-VPN 設定で設定した PKI ユーザ

Use Certificate：有効

File Name：PKI ユーザ作成時に指定したクライアント証明書

Passphrase：クライアント証明書のパスワード

4.3. Android（Android11）

■クライアント証明書のインポート

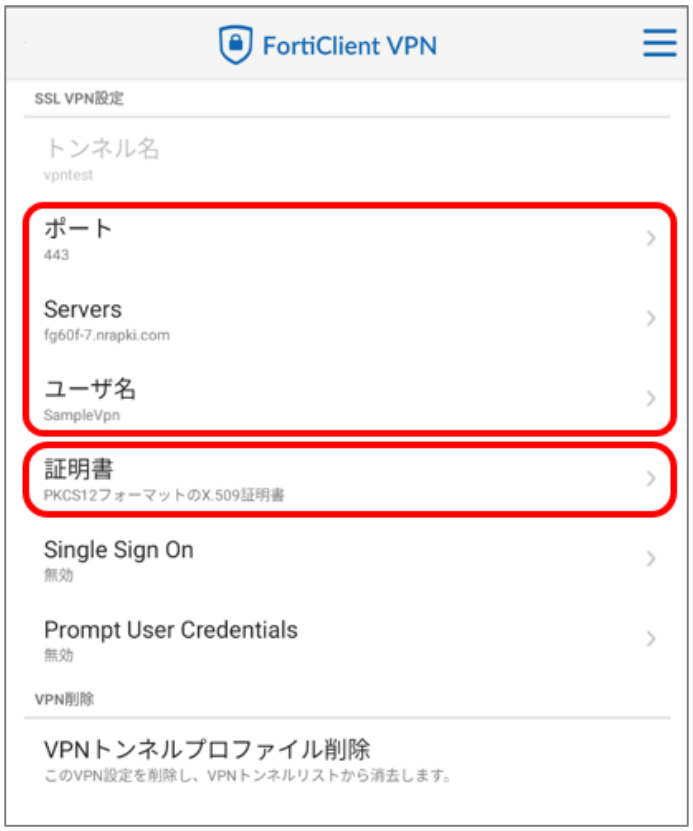
FortiClient から指定するクライアント証明書は内蔵ストレージから選択します。Android 標準の認証ストレージにインストールしたクライアント証明書は FortiClient で指定できません。

事前に Android の内蔵ストレージにクライアント証明書ファイル（拡張子 P12 形式）を配置してください。

ご利用の Android 端末にて FortiClient をダウンロード･インストールしてください。

FortiClient を起動し、任意のトンネル名を入力してください。VPN タイプ「SSL VPN」を選択して「作成」をタップします。

下図の赤枠内の項目を入力し、「証明書」をタップします。



クライアント証明書を指定し、クライアント証明書のパスワードを入力し「OK」をタップします。

クライアント証明書が指定されます。

以上で Android 端末における FortiClient の VPN 設定は完了です。

■設定例

トンネル名：任意

ポート：SSL-VPN 設定で設定した「リッスンするポート」を指定

Servers：FortiGate の FQDN

ユーザ名：SSL-VPN 設定で設定した PKI ユーザ

証明書：PKI ユーザ作成時に指定したクライアント証明書

Single Sign On：任意

Prompt User Credentials：任意

5. サーバ証明書の入れ替え手順

本項ではインポートしたサーバ証明書の入れ替え手順の説明になります。
サーバ証明書の有効期限が切れる前に実施してください。

事前準備

・新しい SSL サーバ証明書(PEM 形式)

流れは次の通りです。

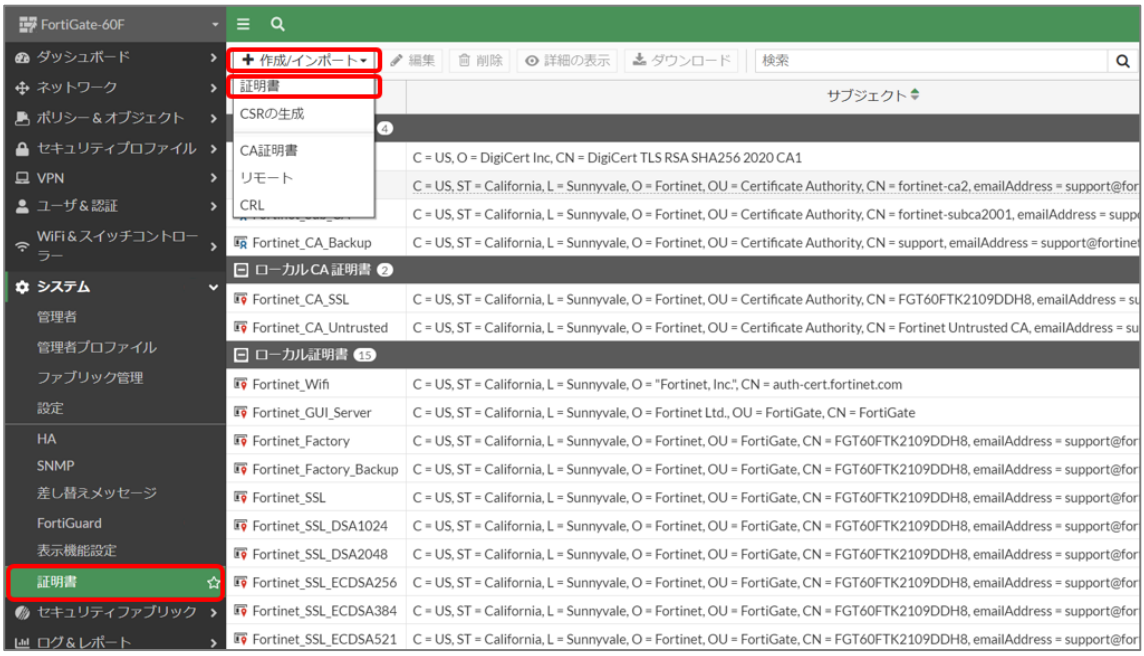
5.1. 新しいサーバ証明書のインポート 30
準備していただいた新しい SSL サーバ証明書をインポートします。

5.2. サーバ証明書の設定 32
インポートした新しいサーバ証明書と現在設定しているサーバ証明書を入れ替えます。

項目は以上です。次ページから各項目の説明の記載になります。

5.1. 新しいサーバ証明書のインポート

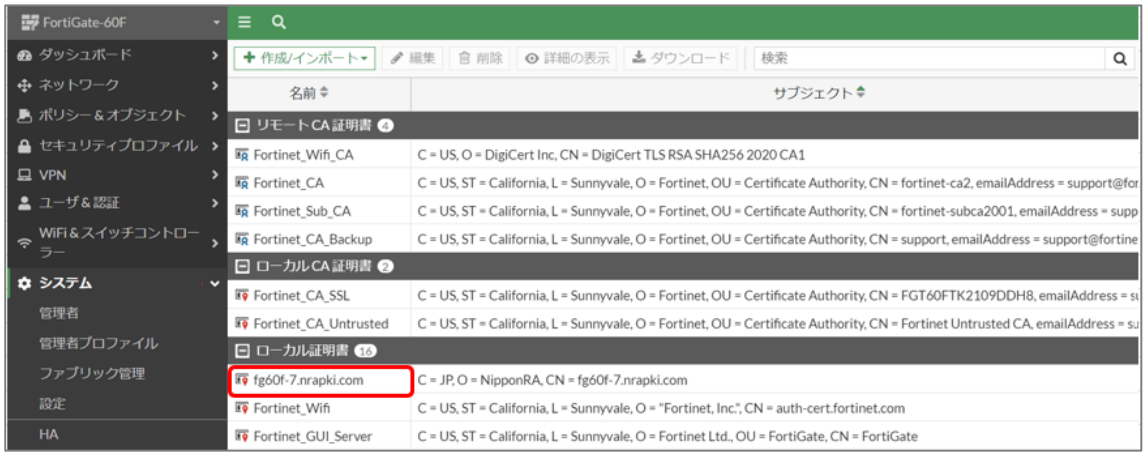
「システム」-「証明書」を選択し、「作成/インポート」から「証明書」を選択します。



「証明書をインポート」を選択します。

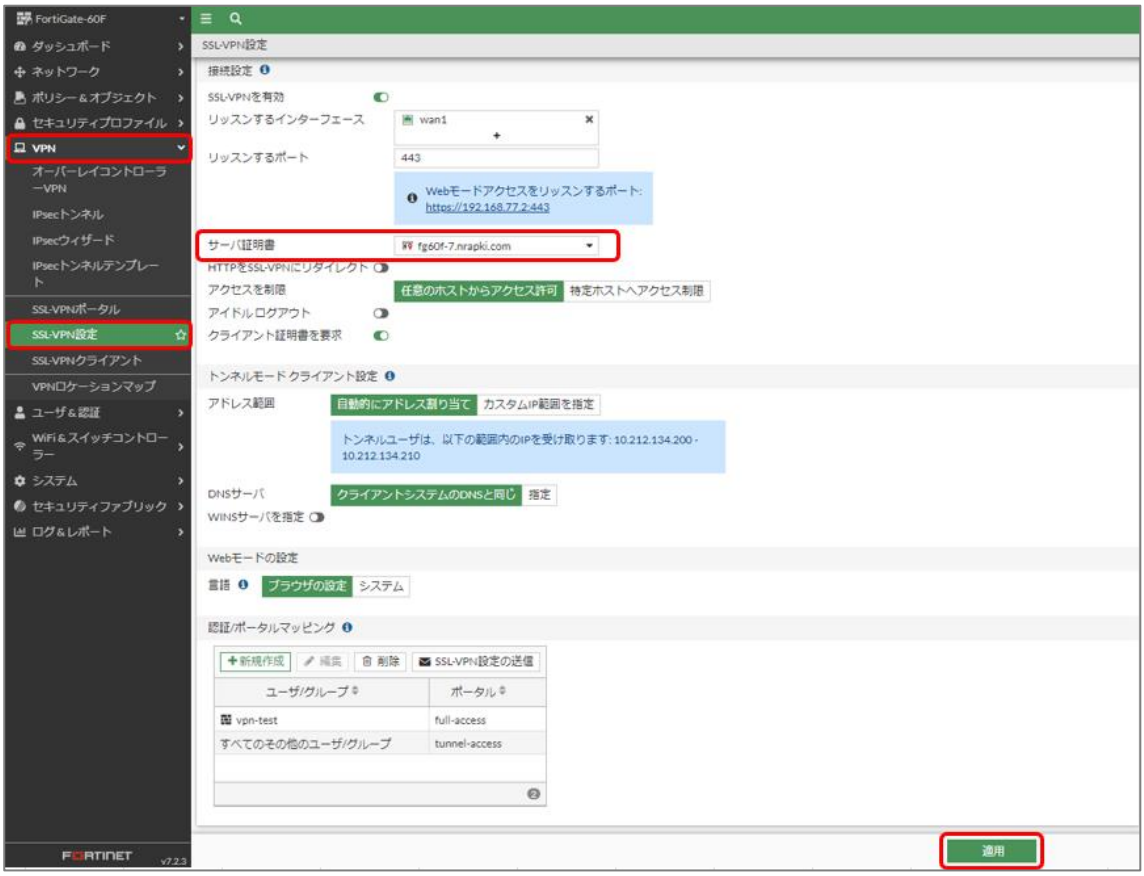
「証明書の作成」画面が表示されます。「証明書」を選択し、証明書ファイル、キーファイル、パスワード(任意)を指定し作成をクリックします。

サーバ証明書がインポートされたことを確認します。



5.2. サーバ証明書の設定

「VPN」-「SSL-VPN 設定」から「サーバ証明書」の項目をインポートした新しい証明書に変更し、「適用」をクリックします。



以上でサーバ証明書入れ替え完了です。古いサーバ証明書は必要に応じて削除してください。