JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

～F5 BIG-IP Edge Gateway連携～

iPhone版 BIG-IP Edge Clientによる BIG-IPへのSSL-VPNトンネリング接続

Ver.2.0

2013 年 1 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行したクライアント証明書・iPhone用の構成プロファイルを利用して、iPhone用VPNクライアントである「BIG-IP Edge Client」からF5 Networks社製「BIG-IP Edge Gateway」とiPhone用VPNクライアントソフトウェアである「BIG-IP Edge Client」を利用してのトンネリング接続を行う環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、6項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で作成しています。

- BIG-IP Edge Gateway （BIG-IP 11.1.0 Build 1943.0 Final）
  以後、「BIG-IP」と記載します
- JS3 プライベートCA Gléas（バージョン1.10）
  以後、「Gléas」と記載します
- iPhone 5（iOS 6.0.2）
  以後、「iPhone」と記載します
- BIG-IP Edge Client（バージョン1.0.4　7060.2012.0629.1）
  以後、「Edge Client」と記載します

以下については、本書では説明を割愛します。

- BIG-IPでのネットワーク設定やサーバ証明書設定等の基本設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- iPhoneでのネットワーク設定等の基本設定

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

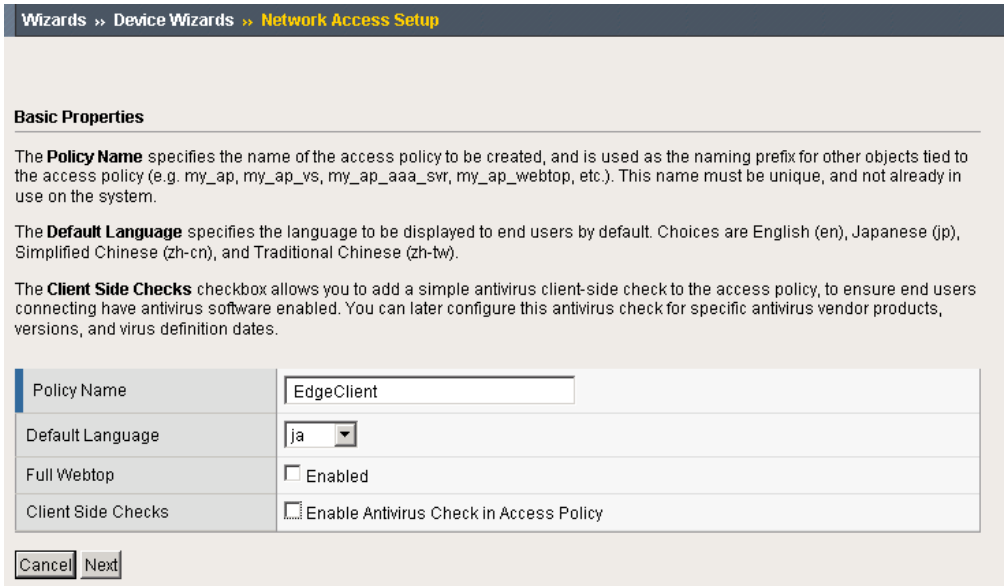
2. BIG-IPの設定

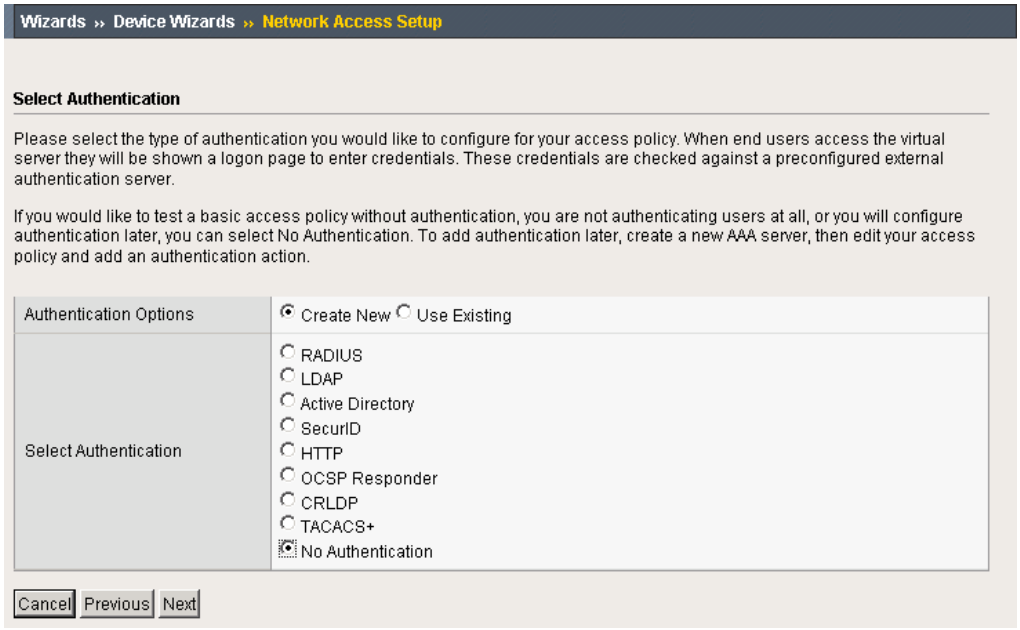
2.1. Network Access の設定

本書ではウィザードを使用して Virtual Server や Network Access をセットアップします。既に作成していれば、本項は実施する必要はありません。2.2 に進んでください。

管理画面にログインし、メニューから Wizards→Device Wizards の順にクリックして、ウィザードの一覧を表示します。Network Access Setup Wizard for Remote Access を利用して、環境に合わせて Network Access をセットアップしてください。

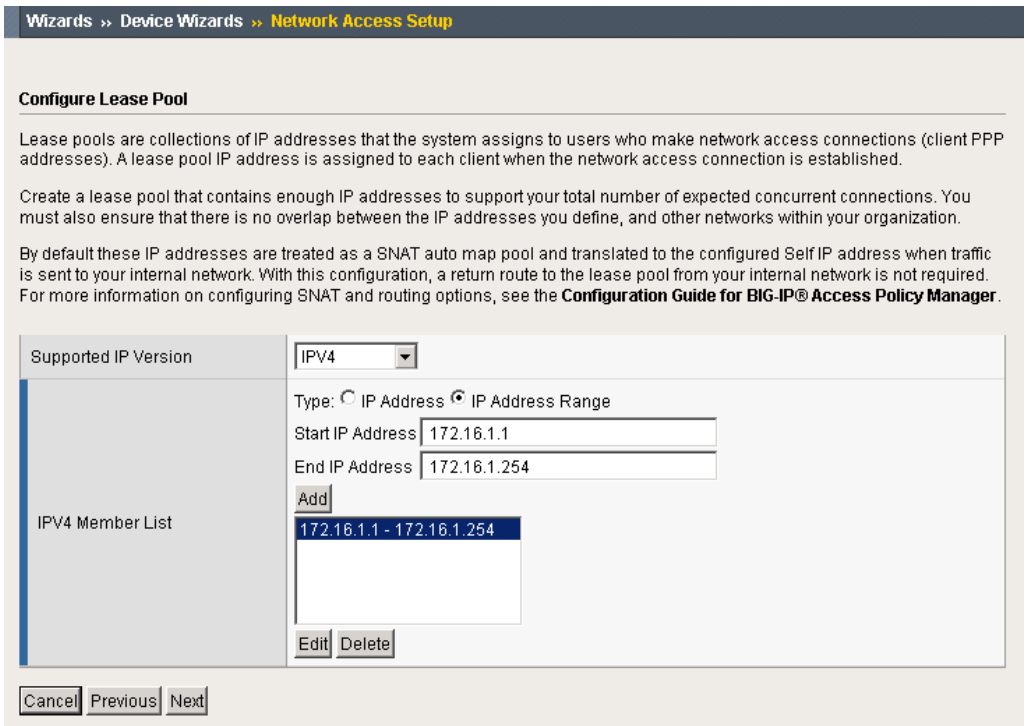
以下は設定例となります。

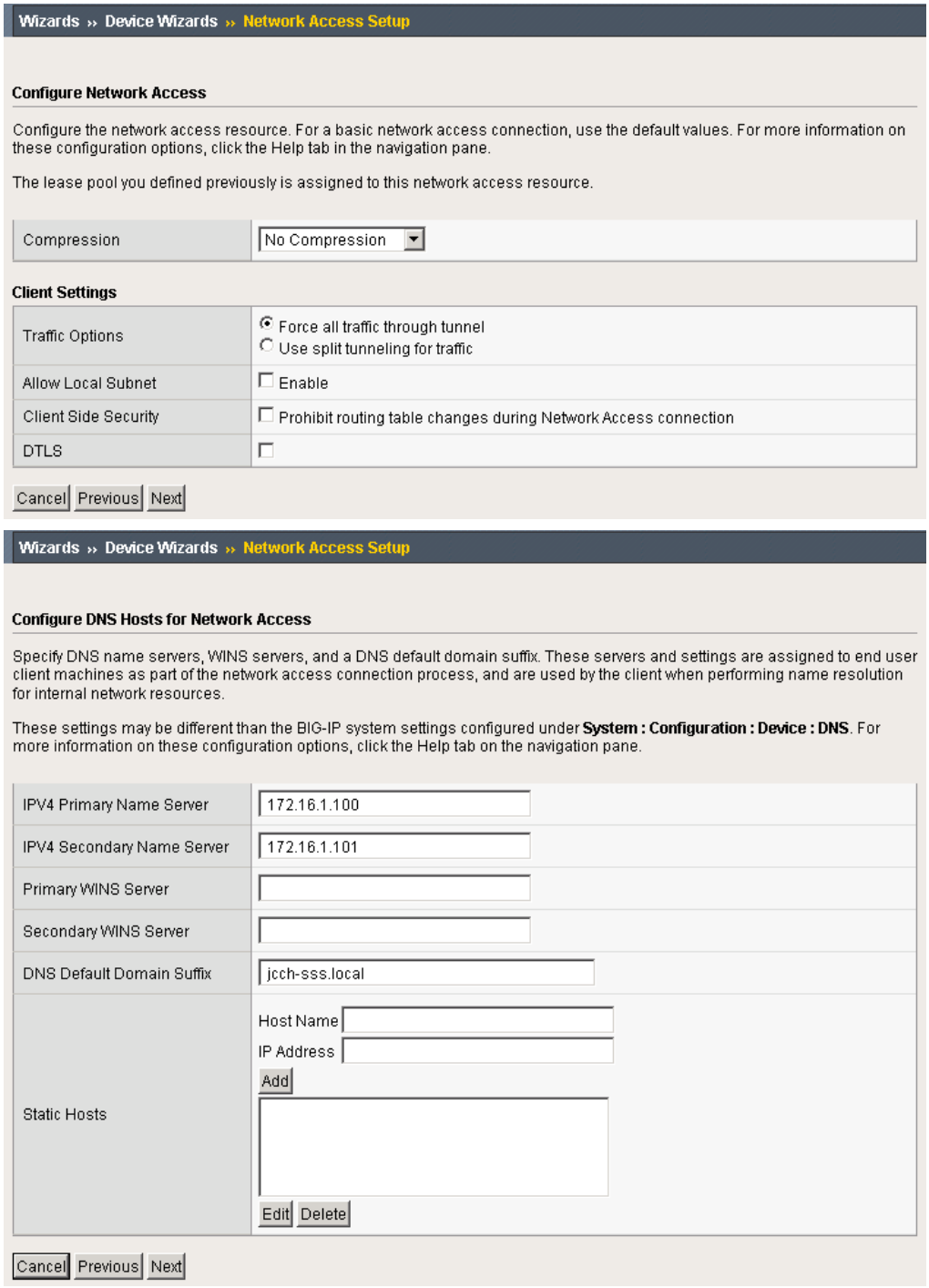


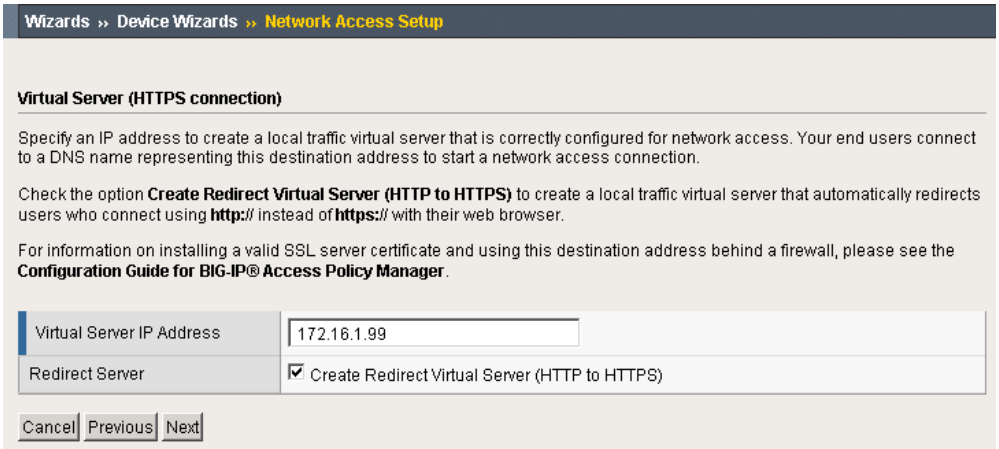


※　本書では、クライアント証明書のみによる認証の設定を記載します。ID/パスワードを併用する 2 因子認証を実施する場合は、ここで No Authentication 以外の認証を選んでください。

※　Gléas の UA で構成プロファイルをダウンロードする場合、UA にログインする時のパスワードが Edge Client に保存され、VPN 接続時に利用されます。



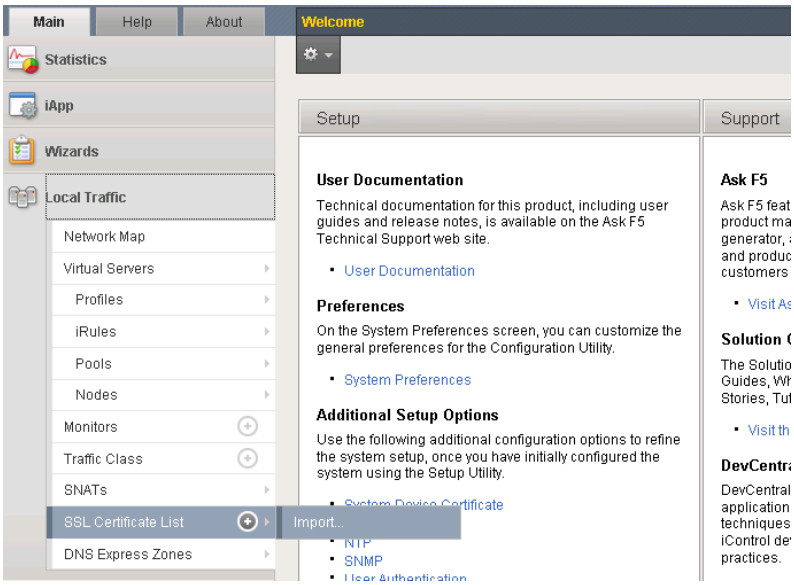

Wizards » Device Wizards » Network Access Setup
Configure Network Access
Configure the network access resource. For a basic network access connection, use the default values. For more information on these configuration options, click the Help tab in the navigation pane.
The lease pool you defined previously is assigned to this network access resource.
Compression
No Compression
Client Settings
Traffic Options
Force all traffic through tunnel
Use split tunneling for traffic
Allow Local Subnet
Enable
Client Side Security
Prohibit routing table changes during Network Access connection
DTLS
Cancel
Previous
Next
Wizards » Device Wizards » Network Access Setup
Configure DNS Hosts for Network Access
Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers and settings are assigned to end user client machines as part of the network access connection process, and are used by the client when performing name resolution for internal network resources.
These settings may be different than the BIG-IP system settings configured under System : Configuration : Device : DNS. For more information on these configuration options, click the Help tab on the navigation pane.
IPV4 Primary Name Server
172.16.1.100
IPV4 Secondary Name Server
172.16.1.101
Primary WINS Server
Secondary WINS Server
DNS Default Domain Suffix
jcch-sss.local
Static Hosts
Host Name
IP Address
Add
Edit
Delete
Cancel
Previous
Next



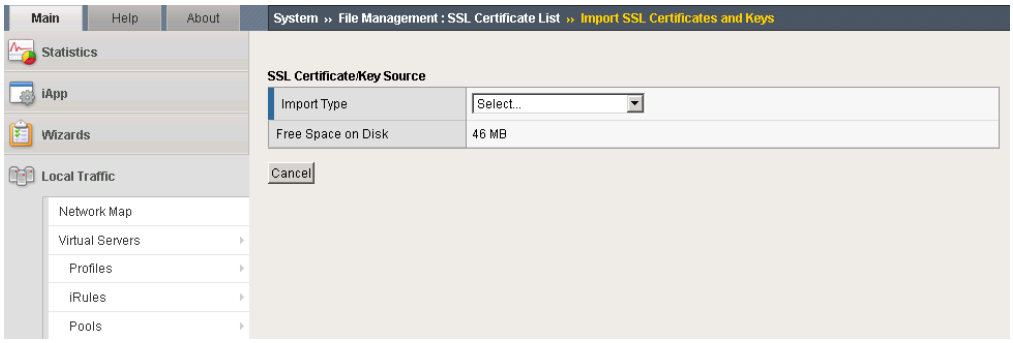
2.2. ルート証明書の登録

クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、クライアントPCから提示されるクライアント証明書が正しいことを検証する際に利用するためです。

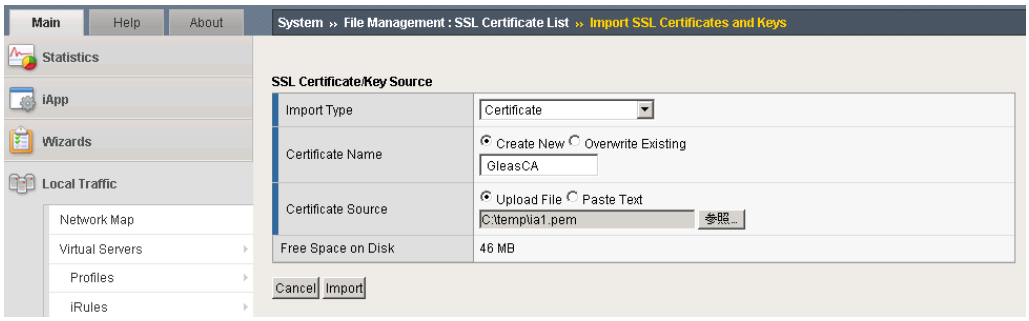
1．Local Traffic→SSL Certificate List→import の順にクリックする。



2．Import Type にて、Certificate を選択する。



３．ルート証明書を指定する。
Certificate Nameには、任意の名前を入力します。Certificate Sourceには、ルート証明書ファイルの場所を指定します。
入力が完了したら、Import ボタンをクリックします。



2.3. 失効リスト（CRL）の登録

Gléasで失効したクライアント証明書でのアクセスを防ぐために、CRLの登録をします。

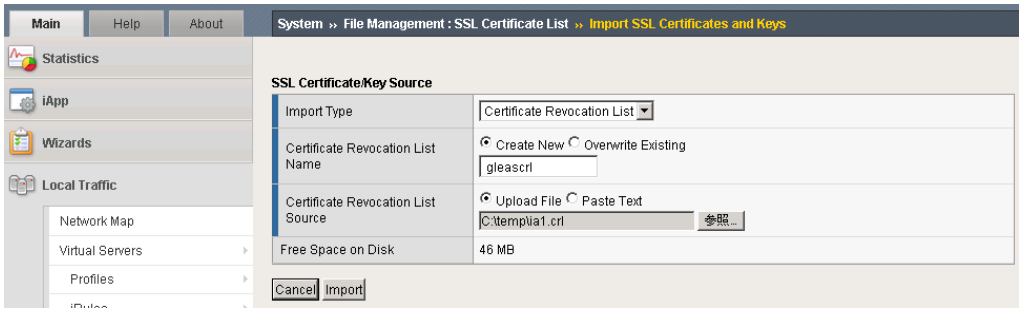
あらかじめGléasよりCRLをダウンロードしておき、以下の操作をおこないます。
※　Gléas の初期設定での CRL ファイルの公開場所は以下のとおりです
　　http://hostname.example.local/crl/ia1.crl

１．Local Traffic→SSL Certificate List→import の順にクリックする。

２．Import Type にて、Certificate Revocation List を選択する。

３．CRLを指定する。
Certificate Revocation List Nameには、任意の名前を入力します。Certificate Revocation List Sourceには、CRLファイルの場所を指定します。

入力が完了したら、Import ボタンをクリックします。



CRLを更新する場合は、Certificate Revocation List Name で Overwrite Existing を選択し、更新されたCRLファイルをアップロードします。

コマンドライン（tmsh。BIG-IPの管理用シェル）からCRL更新をおこなうことも可能です。以下はコマンド例です。

```
tmsh modify /sys file ssl-crl gleascrl.crl source-path
http://host.example.local/crl/ia1.crl
```

※　crontab で動かすことで定期取得の設定も可能です

また失効確認には、LDAP（Lightweight Directory Access Protocol）やOCSP（Online Certificate Status Protocol）を利用する方法もあります。

2.4. SSL プロファイルの作成

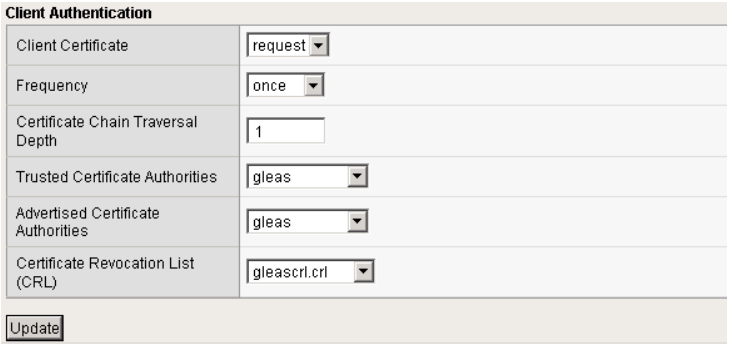
クライアント証明書による認証を実施するプロファイルを作成します。

1．Local Traffic → Virtual Servers → Profiles → SSL → Client の順にクリックします。

2．Client Authentication の各項目を設定します。

- Client Certification を request に変更
  ※ require とすると、Edge Client がトンネリング接続に失敗します。認証時は、Access Policy にてクライアント証明書の正当性を検証します。
- Trusted Certificate Authorities を 2.2 で登録したルート証明書に変更
- Advertised Certificate Authorities を 2.2 で登録したルート証明書に変更
- Certificate Revocation List (CRL)を 2.3 で登録した CRL に変更

3．Update ボタンをクリックします。



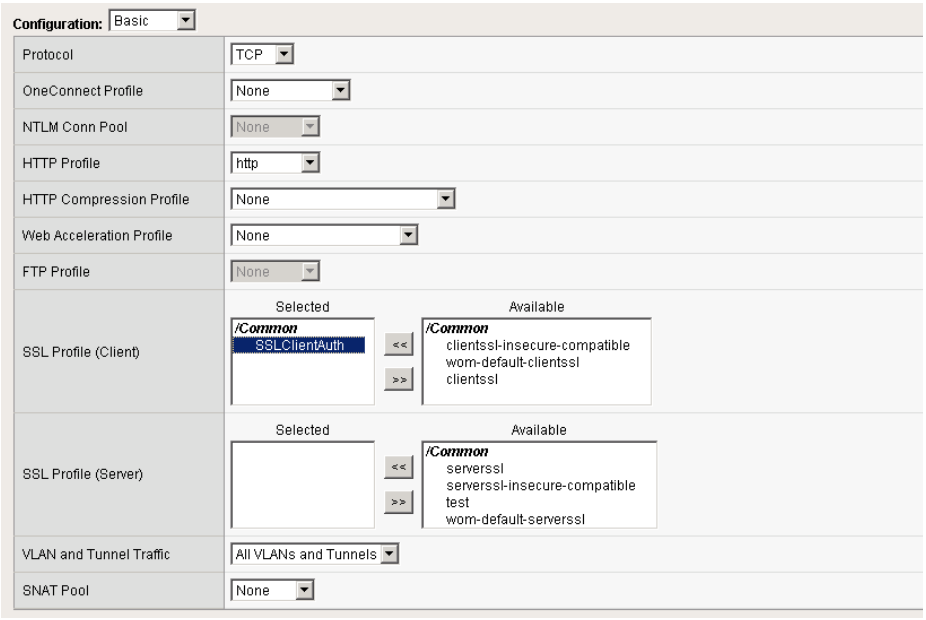
2.5. SSL プロファイルの適用

2.4 で作成したプロファイルを対象のバーチャルサーバに適用します。

1．Local Traffic → Virtual Servers → Virtual Server List の順にクリックします。

2．2.1 のウィザードで作成された Virtual Server をクリックします。

3．SSL Profile (Client)を 2.4 で作成した Profile に変更します。



4．Update ボタンをクリックします。

2.6. アクセスポリシーの設定

Access Policy を変更します。

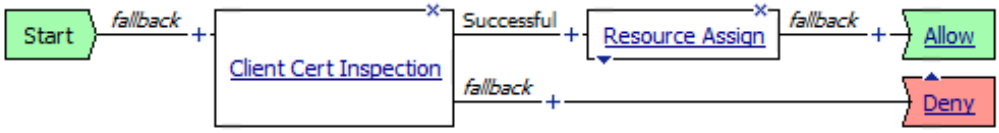
１．Access Policy→Access Profiles の順にクリックし、Access Profile List を表示します。

２．2.1 のウィザードで作成された Access Profile を編集するため、Access Policy の Edit をクリックします。

３．Logon Page の×をクリックして、削除します。

４．Resource Assign の左側の＋をクリックして、Authentication 内の Client Cert Inspection を選び、Add Item ボタンをクリックします。

５．Save ボタンをクリックします。



上記のようになったら、Apply Access Policy をクリックします。

※　上記は 2.1 のウィザードで No Authentication を選んだ場合の手順になります。クライアント証明書のみによる認証ではなく、ID/PW 認証も同時に行う 2 因子認証を実施する場合は、Logon Page は削除せず、Logon Page と Resource Assign の間に RADIUS Auth などを追加してください。

以上でBIG-IPの設定は終了です。

3. Gléas の管理者設定

Gléas で、発行済みのクライアント証明書を含む Edge Client 設定（構成プロファイル）を iPhone にインポートするための設定を本書では記載します。

※　下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

※　Edge Client 用の構成プロファイル作成機能はオプションとなります。詳細は弊社営業までお問い合わせください。

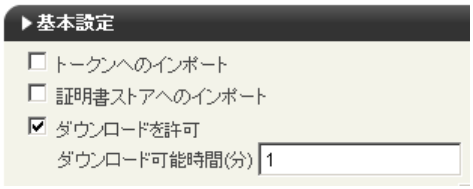
3.1. UA（ユーザ申込局）設定

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一

覧]画面に移動し、設定を行うUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定
  この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、構成プロファイルのダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のiPhoneへの構成プロファイルのインストールを制限することができます。



[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

iPhone構成プロファイル基本設定

- [名前]、[識別子]に任意の文字を入力（必須項目）
- [削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPhoneユーザの誤操作等によ

る構成プロファイルの削除を防止できます）

F5 SSL-VPNの設定

- [SSL-VPN接続名]に任意の名前を入力（Edge Client上ではDescriptionに対応）
- [F5 SSL-VPN ホスト名]にBIG-IPのホスト名を入力（Edge Client上ではServerに対応）
- [オンデマンド接続先]にオンデマンド接続に利用するドメイン名を入力（Edge Client上ではDomain ListのAlways Connectに対応）

各項目の入力が終わったら、 [保存]をクリックします。

今回の設定ではパスワード認証なしでVPN接続が可能となるので、デバイスパスコードを設定しておくことが推奨されますが、構成プロファイルでパスコードを強制させることも可能です。

以上でGléasの設定は終了です。

4. Gléas を利用したクライアント証明書の配布

4.1. Edge Client のインストール

iPhoneでEdge Clientを利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールを行ってください。
本書ではEdge Clientのインストール方法については割愛します。

4.2. Gléas の UA から配布

iPhoneのブラウザ（Safari）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

ログインすると、そのユーザ専用ページが表示されるので、[ダウンロード]をタップし、構成プロファイルのダウンロードを開始します。
※インポートロックを有効にしている場合は、この時点からカウントが開始されます

自動的にプロファイル画面に遷移するので、[インストール]をタップします。
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。

以下のようなルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行してください。
※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります。

デバイスパスコードを設定している場合は、入力を求められます。
パスコード強制が構成プロファイルに含まれていて、デバイスにパスコードを設定していない場合は、以下の画面が出現しパスコードの設定を求められます。

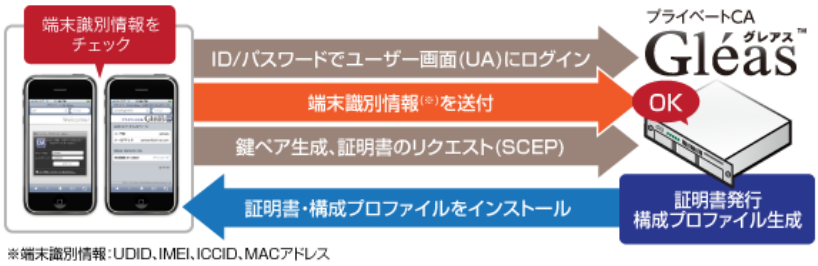
インストール完了画面になりますので、[完了]をタップしてください。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。
以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。

4.3. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air（OTA）エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。
OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。



詳細は最終項のお問い合わせ先までお問い合わせください。

5. Edge Client の利用

インストールした構成プロファイルにより、Edge Clientに認証に利用するクライア

ント証明書やユーザID、オンデマンド接続用のドメインが設定されています。
Edge Clientを起動し[接続]ボタンをタップ、或いは構成プロファイルでオンデマンド接続が設定されている場合は、Safariなど対応アプリのアドレスバーに指定されたアドレスを入力すると、クライアント証明書を利用した認証を行いVPNの接続がおこなわれます。
クライアント証明書によるセキュアな接続をお試しください。

以下はEdge Clientから接続した画面です。
（接続すると、iPhoneの通知エリアに **VPN** アイコンが表示されます）。

なお、失効した証明書でアクセスすると以下のようになり接続することができません。
※失効情報を含むCRLがBIG-IPに伝搬されている必要があります

失効された証明書でアクセスした場合には、BIG-IPに以下のログが記録されます（/var/log/ltm）。

※ファシリティSSLのログレベルをdebugにしておく必要があります

```
debug tmm[xxxx]: 01260003:7: Certificate with serial xxxx revoked per CRL
from issuer Issuer_DN
debug tmm[xxxx]: 01260006:7: Peer cert verify error: certificate revoked
(depth X; cert Subject_DN)
debug tmm[xxxx]: 01260009:7: Connection error: ssl_shim_vfycert:2462:
certificate revoked (44)
```

6. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■BIG-IPに関するお問い合わせ先
F5ネットワークスジャパン株式会社
Tel: 03-5114-3210
URL: http://www.f5networks.co.jp/fc
（上記URLのお問い合わせフォームよりご連絡ください）

■Gléasに関するお問い合わせ先
株式会社JCCH・セキュリティ・ソリューション・システムズ
Tel: 050-3821-2195
Mail: sales@jcch-sss.com