JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

Per-App VPN
（BIG-IP APM / Workspace ONE UEM）

Ver. 1.0
2018 年 10 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」と、ヴイエムウェア社のデジタルワークスペース・プラットフォーム「VMware Workspace ONE UEM」（AirWatchの後継サービス）を連携させ、デバイスにプッシュ配信した電子証明書を利用して、F5ネットワークス社の「BIG-IP Access Policy Manager」（APM）をゲートウェイとしたPer-App VPN（アプリケーション単位でのVPN接続）をおこな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、最終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

本書は、以下の環境で検証をおこなっております。

- F5ネットワークス BIG-IP Access Policy Manager（バージョン 13.1.1 Build 0.0.4）
  ※以後、「APM」と記載します
- VMware Workspace ONE UEM（バージョン 9.6.0.7）
  ※以後、「WS1 UEM」と記載します
- JS3 プライベート認証局Gléas（バージョン1.16.9）
  ※以後、「Gléas」と記載します
- Webサーバ：Ubuntu 16.04.4 / Apache 2.4.18
  ※以後、「Webサーバ」と記載します。ApacheはOSのパッケージを利用
- Microsoft Windows 10 Pro
  F5 Access (バージョン 1.2.8.0 Build 51.0) / AirWatch Agent (バージョン 9.7.0.0)
  ※以後、「Windows」と記載します
  ※デスクトップアプリ BIG-IP Edge Client は使いません
- Apple iPad Air 2 (iOS 12.0)
  F5 Access (バージョン 3.0.2) / VMware Browser （バージョン 6.16.1）
  ※以後、「iPad」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。

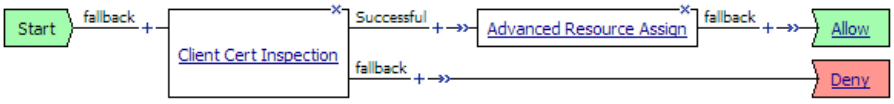
- APMのVPN設定やクライアント証明書認証の設定

  ※APMでの証明書認証設定について、弊社では以下のURLでドキュメントを公開しています。

  https://www.gleas.jp/news/whitepaper/big-ip-apm

  Per-App VPN接続時にはパスワードなどのユーザ入力待ちが発生してはならないので、本書ではクライアント証明書認証のみを前提とします

  以下はAPMでのアクセスポリシーの設定例です



- WS1 UEMの基本操作、およびGléasとの証明書発行連携の設定

  ※WS1 UEM（AirWatch）とGléasの証明書発行連携の設定について、弊社では以下のURLでドキュメントを公開しています

  https://www.gleas.jp/news/whitepaper/airwatch

  事前にWS1 UEMで認証局と証明書発行テンプレートの設定をしておきます

- WindowsやiPadのネットワーク設定や操作方法

  ※F5 Accessはそれぞれのストアからあらかじめインストールしておきます

  ※本検証では、WindowsではFirefoxをVPN接続アプリケーションとします

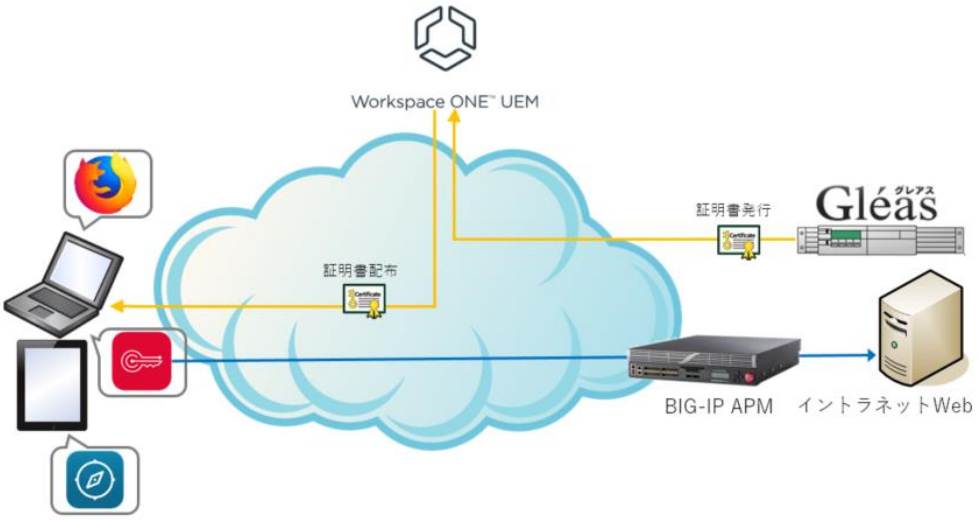
  FirefoxはあらかじめMozilla CorporationのWebサイトからインストールしておき、実行ファイル（firefox.exe）のパスを調べておきます

- Gléasの基本操作

以上については、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。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. WindowsとiPadで、WS1 UEMへの加入操作をおこなう
2. WS1 UEMはGléasと連携して発行した証明書と、Per-App VPN設定を含むプロファイルを加入済みのWindowsとiPadに配布する
   またiPadに対しては、VMware Browserアプリも配布する
3. Windowsでは、Firefoxを起動すると自動的にAPMへのVPN接続がおこなわれ、イントラネットWebにアクセス可能となる。
4. iPadでは、VMware Browserを起動すると自動的にAPMへのVPN接続がおこなわれ、イントラネットWebにアクセス可能となる。
5. Windows、iPadともに他のブラウザではイントラネットWebに接続することはできない

2. WS1 UEM での Per-App VPN 設定（iOS 向け）

2.1. プロファイル設定

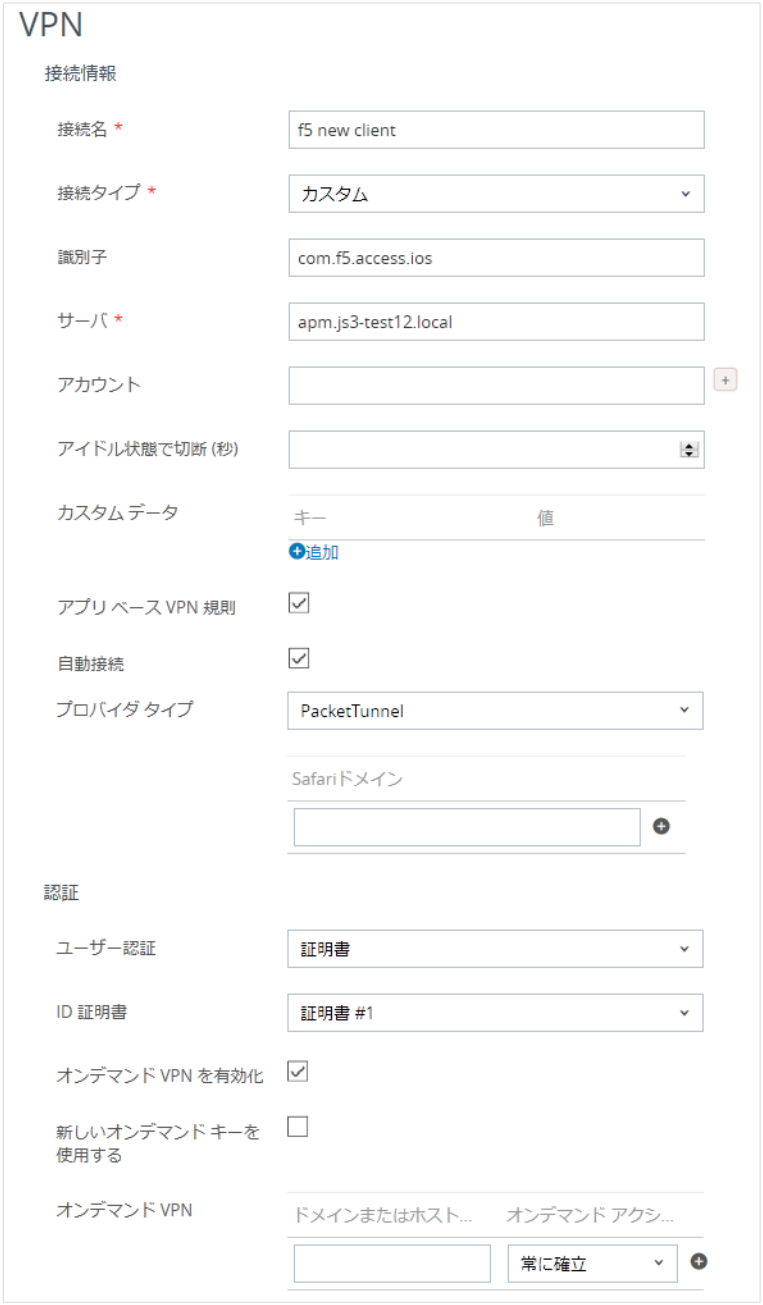
WS1 UEM の Web 管理コンソールにログインし、[デバイス] > [プロファイルとリソース] > [プロファイル]よりプロファイルを新規に追加します。

資格情報の項目で、クライアント証明書の発行・配布設定と、ルート証明書の配布設定をおこないます。

※設定内容の詳細は 1.2 項に記載の弊社ホワイトペーパーを参照

VPN の項目で、以下を設定します。

- [接続名]には、任意の接続名称を入力
- [接続タイプ]は、”カスタム”を選択
- [識別子]には、”com.f5.access.ios”を入力
- [サーバ]には、VPN の接続先ホスト名を入力
- [アプリベース VPN 規則]をチェック
- [自動接続]をチェック
- [プロバイダタイプ]は、”PacketTunnel”を選択
- [ユーザー認証]には、”証明書”を選択
- [ID 証明書]には、資格情報プロファイルで設定したクライアント証明書を選択
  ※以下のスクリーンショットでは、資格情報の 1 番目にクライアント証明書を設定した場合の例となります
- [オンデマンド VPN を有効化]をチェック



設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

2.2. アプリケーション配布設定

Web 管理コンソールで[アプリとブック] > [ネイティブ] > [パブリック]と進み、[アプリケーションの追加]をクリックし、VMware Browser を検索、追加します。

追加したのちに、[編集]タブをクリックし以下の設定をおこないます。

- SDK タブの[SDK プロファイル]で、作成した SDK プロファイルを選択
  ※SDK プロファイルは、[グループと設定]＞[すべての設定]＞[アプリ]＞[設定とポリシー]＞[プロファイル]で作成できます。VMware Browser の機能制限など各種設定をおこなうことが可能ですが、本書の主旨から外れるので説明は省きます

また[割り当て]をクリックして、[割り当ての追加]、或いは既に割り当ててあるグループを選択し、以下の設定をおこないます。

- [管理アクセス]で、”有効”を選択
- [アプリトンネル]で、”有効”を選択
- [アプリベース VPN プロファイル]で、3.1 項で設定した VPN 項目を含むプロファイルを選択

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

2.3. VMware Browserの設定

Web 管理コンソールで[グループと設定] > [すべての設定] > [アプリ] > [Browser]と進むと、VMware Browser の各種設定がおこなえます。
本書の主旨から外れるので詳細設定は省きますが、テスト用 Web サイトの URL をブックマークに追加しておきます。

※上のスクリーンショットのようにサーバ URL に IP アドレスを使う場合は、[ブラウザ設定]タブの[IP 閲覧を許可する]を有効にし、[許可された IP アドレス]に Web サーバの IP アドレスを指定する必要があります

設定完了後、[保存]をクリックして設定を保存します。

3. iPad での Per-App VPN の実行

3.1. WS1 UEMへの加入とVMware Browserのインストール

iPad で WS1 UEM に加入すると、WS1 UEM と Gléas との間で証明書発行がおこなわれ、少しの時間が経つと SSL-VPN やクライアント証明書を含むプロファイルが自動インストールされます。

また WS1 UEM 加入後に、3.2 項で設定した通り VMware Browser をインストールする旨のメッセージが表示されるのでそれに従いインストールをおこないます。

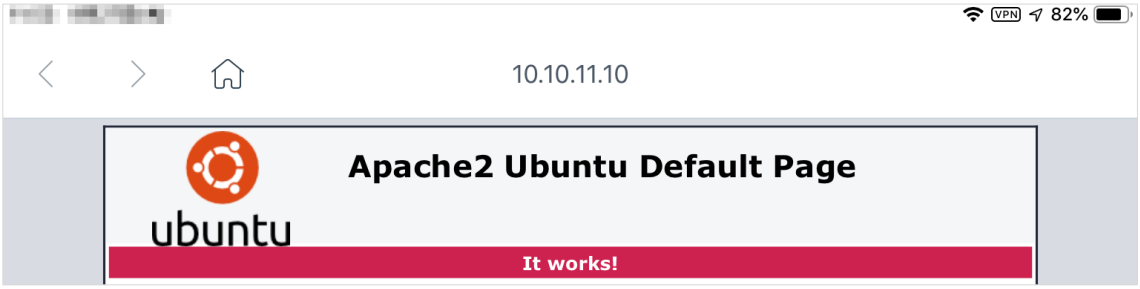
プロファイルは iPad の[設定]アプリで[一般] > [プロファイルとデバイス管理]と進み、[デバイスマネージャ]という名前でインストールされ、タップすることで内容を確認できます。

またその状態で F5 Access を起動すると、[アプリごとの]欄で Per-App VPN が追加されていることがわかります。

3.2. Per-App VPNの動作確認

この状態で VMware Browser を起動すると、自動的に VPN 接続がおこなわれます。
接続時には iPad 画面の右上に VPN マークが表示されます。

ブックマーク設定してある APM の内部セグメントに接続されている Web サーバへアクセスすると閲覧可能となります。



ホームボタンを押下して VMware Browser を閉じると VPN マークの表示は消えます。同じ URL に対して safari などの他のブラウザでアクセスすると、Web サーバに接続できないためエラーとなります。

4. WS1 UEM での Per-App VPN 設定（Windows 向け）

4.1. プロファイル設定

WS1 UEM の Web 管理コンソールにログインし、[デバイス] > [プロファイルとリソース] > [プロファイル]よりプロファイルを新規に追加します。

資格情報の項目で、クライアント証明書の発行・配布設定をおこないます。

※設定内容の詳細は 1.2 項に記載の弊社ホワイトペーパーを参照

VPN の項目で、以下を設定します。

- [接続名]には、任意の接続名称を入力
- [接続タイプ]は、”F5 Edge VPN”を選択
- [サーバ]には、VPN の接続先ホスト名を入力
- [カスタム構成 XML]に以下を入力

```
<f5-vpn-conf><client-certificate><issuer>ISSUER_CA_NAME</issuer>
</client-certificate><prompt-for-credentials>false</prompt-for-credentials>
</f5-vpn-conf>
```

※上記の“*ISSUER_CA_NAME*”の部分は、資格情報プロファイルで指定したクライアント証明書を発行する CA の名前（クライアント証明書の発行者 CN）に変更します

- [アプリ識別子]は、”デスクトップアプリ”を選択し、その下には Per-App VPN の対象アプリケーションの実行ファイルのパスを入力

  例：C:¥Program Files (x86)¥Mozilla Firefox¥firefox.exe
- [VPN オンデマンド]をチェック
- [ルーティングポリシー]には、”外部リソースにダイレクトアクセスを許可”を選択（スプリットトンネリングを許可）

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

5. Windows での Per-App VPN の実行

5.1. WS1 UEMへの加入

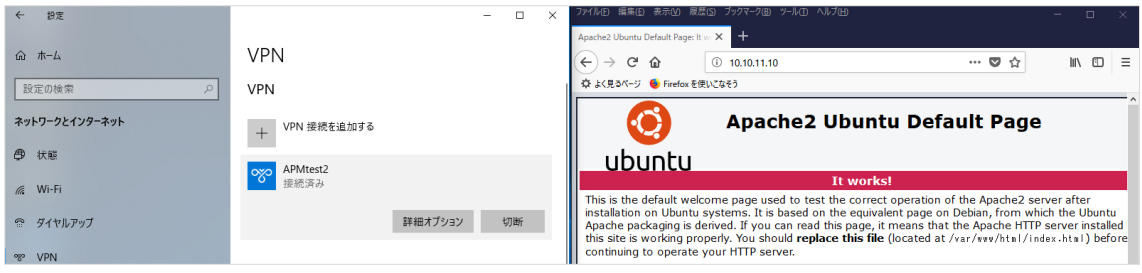
Windows で WS1 UEM に加入すると、WS1 UEM と Gléas との間で証明書発行がおこなわれ、少しの時間が経つと SSL-VPN 設定やクライアント証明書が自動インストールされます。

追加された VPN 設定は、Windows の[設定] > [ネットワークとインターネット] > [VPN]（ms-settings:network-vpn）と進むと確認できます。

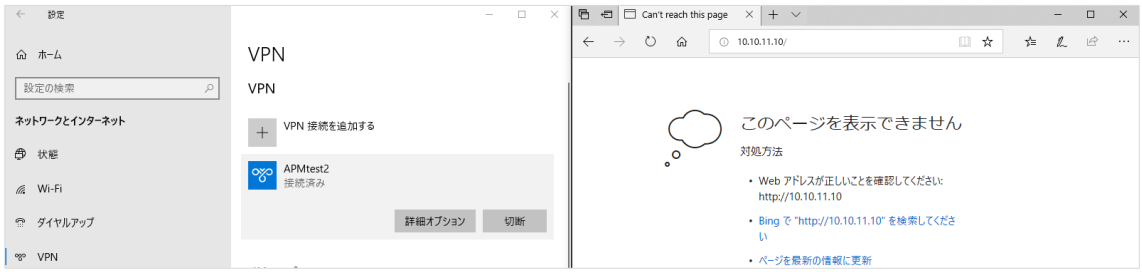
また、インストールされたクライアント証明書は、インターネットオプション（inetcpl.cpl）の[コンテンツ]タブ > [証明書(C)] > [個人]タブの中で確認できます。

5.2. Per-App VPNの動作確認

この状態で Firefox を起動すると、自動的に VPN 接続がおこなわれます。
VPN の設定を見ると”接続済み”と表示され、APM の内部セグメントに接続されている Web サーバへアクセス可能となります。



接続された状態で、同じ URL に対して Edge などの他のブラウザでアクセスすると、Web サーバに接続できずエラーとなります。



6. 問い合わせ

■BIG-IP APM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

URL: https://f5.com/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）

■Workspace ONEに関するお問い合わせ先

ヴイエムウェア株式会社

URL：https://www.vmware.com/jp/company/contact.html

■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