

NetAttest EPS 設定例

連携機器：

FortiGate 50E

Case : FortiClient を利用した、
証明書とパスワードによるハイブリッド認証

Version 1.0

Sample

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

Copyright © 2020, Soliton Systems K.K. , All rights reserved.

はじめに

本書について

本書は、NetAttest EPS と Fortinet 社製 FortiGate 50E との証明書認証連携について記載した設定例です。

各機器の管理 IP アドレス設定など、基本設定は既に完了しているものとします。設定は管理者アカウントでログインし、設定可能な状態になっていることを前提に記述します。

表記方法

表記方法	説明
ABCDabcd1234 (normal)	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。
ABCDabcd1234 (bold)	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。
<i>ABCDabcd1234</i> (italic)	変数を示します。実際に使用する特定の名前または値で置き換えます。

表記方法	説明
『 』	参照するドキュメントを示します。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[キー]	キーボード上のキーを表します。
[キー-1]+[キー-2]	[キー-1]を押しながら[キー-2]を押すことを表します。

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[] は省略可能な項目を示します。この例では、filename は省略してもよいことを示しています。

アイコンについて

アイコン	説明
	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性がります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び FortiGate 50E の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

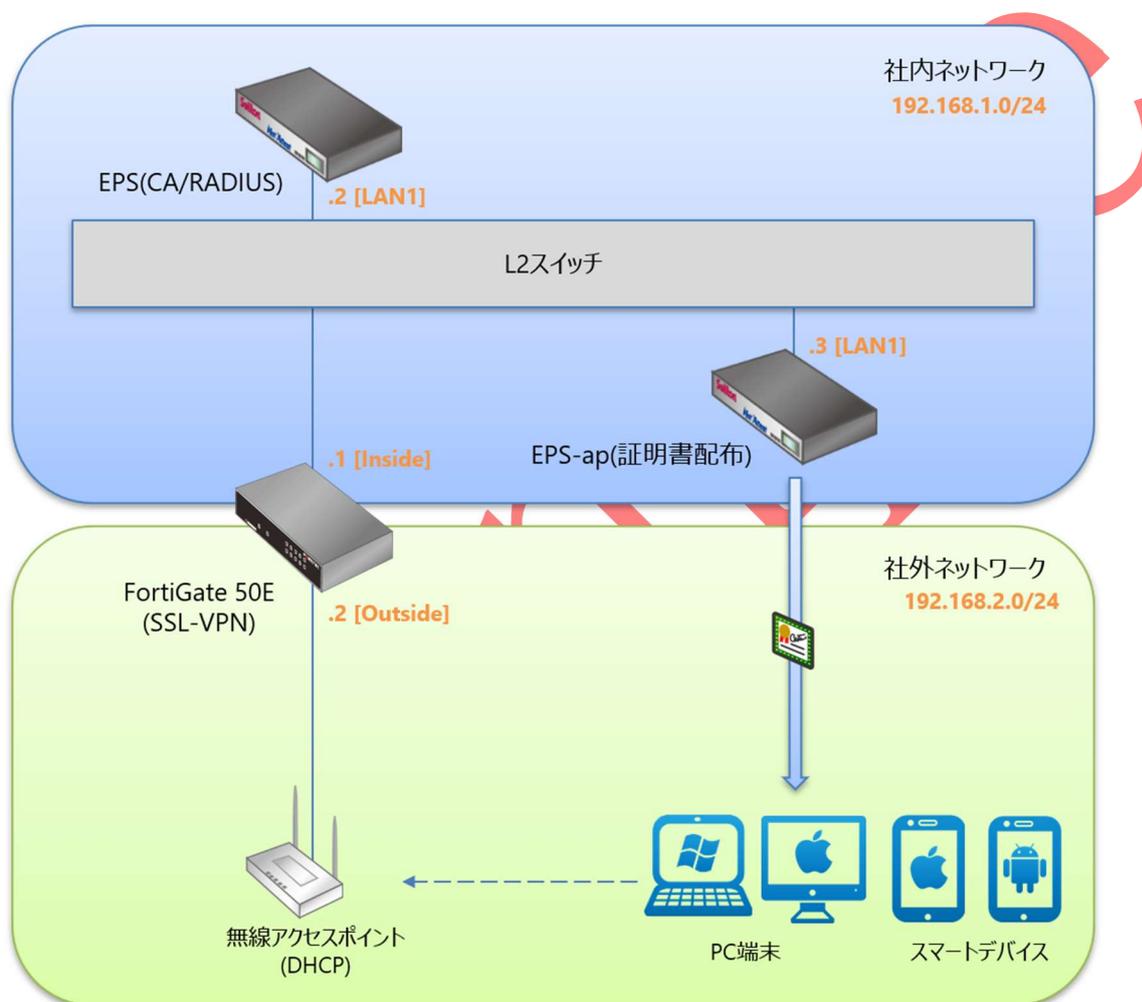
目次

1	構成	7
1-1	構成図	7
2	NetAttest EPS の設定	9
2-1	システム初期設定ウィザードの実行	10
2-2	サービス初期設定ウィザードの実行	11
2-3	認証ユーザーの追加登録	12
2-4	クライアント証明書の発行	13
3	FortiGate の設定準備	14
3-1	インターフェースの設定	15
3-2	システム時刻の設定	16
3-3	証明書設定画面の表示設定	17
4	FortiGate 50E の PKI 関連の設定	18
4-1	CSR の生成 (FortiGate 50E)	19
4-2	サーバー証明書署名要求 (NetAttest EPS)	21
4-3	サーバー証明書の発行 (NetAttest EPS)	22
4-4	サーバー証明書のダウンロード (NetAttest EPS)	23
4-5	CA 証明書の取得 (NetAttest EPS)	24
4-6	CRL の取得 (NetAttest EPS)	24
4-7	サーバー証明書のインポート (FortiGate 50E)	25
4-8	CA 証明書のインポート (FortiGate 50E)	26
4-9	CRL のインポート (FortiGate 50E)	27
5	FortiGate 50E の接続設定	28
5-1	RADIUS サーバーの設定	29
5-2	ユーザグループの設定	30
5-3	SSL-VPN ポータルの設定	31
5-4	SSL-VPN 設定	33
5-5	IPv4 ポリシーの設定	35
6	Windows 版 FortiClient の設定	37
6-1	PC へのデジタル証明書のインストール	38

6-2 Windows 版 FortiClient の設定	40
7 Mac 版 FortiClient の設定	43
7-1 PC へのデジタル証明書のインストール	44
7-2 Mac 版 FortiClient の設定	48
8 iOS 版 FortiClientVPN の設定	50
8-1 iPhone への VPN 用デジタル証明書のインストール.....	51
8-2 iOS 版 FortiClientVPN の設定	54
9 Android OS 版 FortiClientVPN の設定	59
9-1 Android 端末への VPN 用デジタル証明書のダウンロード	60
9-2 Android OS 版 FortiClientVPN 設定	61
10 接続の確認	63
10-1 Windows における FortiClient を利用した SSL-VPN 接続	63
10-2 Mac における FortiClient を利用した SSL-VPN 接続.....	65
10-3 iPhone における FortiClientVPN を利用した SSL-VPN 接続.....	67
10-4 Android 端末における FortiClientVPN を利用した SSL-VPN 接続.....	68

1 構成

1-1 構成図



※NetAttest EPS の設定は、設定用の Windows 管理端末 と NetAttest EPS の管理ポート (LAN2) を直結して行います。

環境

1-2-1 機器

役割	メーカー	製品名	SWバージョン
Authentication Server (認証サーバー)	ソリトンシステムズ	NetAttest EPS (EPS-ST05-A)	Ver. 4.10.7
RADIUS クライアント (SSL VPN 機器)	Fortinet	FortiGate 50E	Ver. 6.2.3 build 1066
Client PC	Microsoft	Surface Laptop	Windows 10 64bit
Client PC	Apple	macOS Catalina	Ver. 10.15.7
Client Smart Phone	Apple	iPhone 8	iOS 14.1
Client Smart Phone	Google	Pixel 3a	Android 10

1-2-2 認証方式

デジタル証明書認証+ID・Password 認証

1-2-3 ネットワーク設定

	EPS-ST05-A	FortiGate 50E	Client PC/Smart Phone
IP アドレス	認証用ポート : 192.168.1.2/24 管理用ポート : 192.168.2.1/24	Inside : 192.168.1.1/24 Outside : 192.168.2.2/24	DHCP
RADIUS port (Authentication)	TCP 1812		-
RADIUS port (Accounting)	TCP 1813		-
RADIUS Secret (Key)	Secret		-

