

SSL-VPN 設定手順書

Ver. 1.1

承認	確認	担当

2014 年 02 月 28 日
株式会社 ネットワールド
S I 技 術 本 部
インフラソリューション 技術 部

目次

1	改訂履歴	3
2	はじめに	4
3	SSL-VPN 設定	6
3.1	ユーザ・ユーザグループの作成	6
3.1.1	ユーザの作成	6
3.1.2	ユーザグループの作成	7
3.2	ファイアウォールオブジェクトの作成	8
3.2.1	アクセス先ネットワーク指定用アドレスオブジェクトの作成	8
3.2.2	クライアント使用用アドレスオブジェクトの作成	8
3.3	SSL-VPN ポータル作成	9
3.3.1	SSL-VPN ポータル作成	9
3.4	ファイアウォールポリシーの作成	10
4	VPN 接続、接続確認	11
4.1	Web ポータルログイン	11
4.2	トンネルモード接続	11
4.3	SSL-VPN トンネルモード接続確認	12

1 改訂履歴

変更履歴

番号	変更年月日	Version	Page	status	変更内容	作成	承認
1	2014/02/28	1.0		o	新規作成	NWL	NWL
2	2014/07/25	1.1	p.9, p12	r	SSL-VPN ポータル:「IP プール」変更 コマンドプロンプト画面キャプチャ修正	NWL	NWL
3							
4							
5							

status: a(dd), d(elete), r(eplace), o(ther)

■マニュアルの取り扱いについて

- ・本書の記載内容の一部または全部を無断で転載することを禁じます。
- ・本書の記載内容は将来予告無く変更されることがあります。
- ・本書を使用した結果発生した情報の消失等の損失については、責任を負いかねます。
- ・本書の設定内容についてのお問い合わせは、受け付けておりませんのでご了承ください。
- ・本書の記載内容は、動作を保証するものではありません。従いましてお客様への導入時には、必ず事前に検証を実施してください。

■Networldテクニカルサポート

- ・Tech-World

Fortinet製品に関するソフトウェアサポート窓口

<https://hds.networld.co.jp/helpdesk/support/login.jsp>

- ・Fortinet FAQ

Fortinet製品に関するよくある問い合わせ

https://hds.networld.co.jp/helpdesk/support/faq_info.jsp?link_id=tec

■メーカーサイト

- ・Fortinet テクニカルドキュメント

<http://docs.fortinet.com/fgt.html>

- ・Fortinet Knowledge Base

<http://kb.fortinet.com/kb/microsites/microsite.do>

2 はじめに

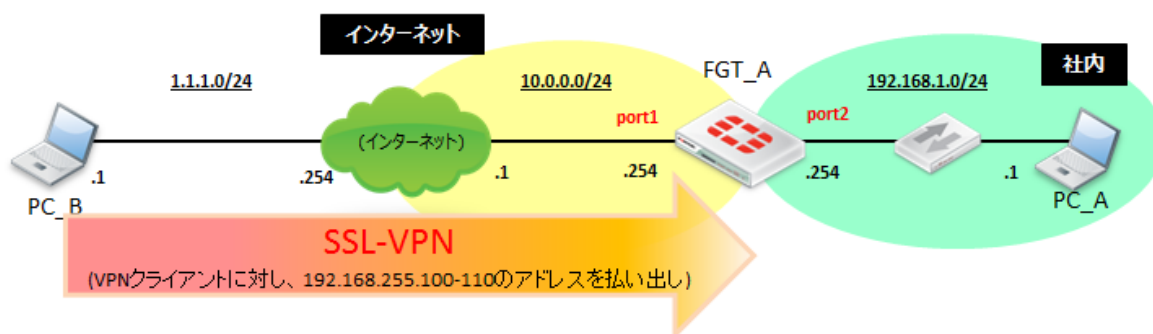
■はじめに

本手順書は SSL-VPN の設定手順を説明しております。

インタフェースなどの初期設定につきましては、別紙 FAQ の『基本設定について』をご確認下さい。

URL: <https://hds.networld.co.jp/faq/fortinet/00002526-1.pdf>

■構成図



■機器情報・ファームウェア

FGT_A: FortiGate-VM00

FortiOS 5.0.7

PC_A: Windows 7 Professional

PC_B: Windows 7 Professional

■設定内容説明

本手順書の設定内容は、インターネット上にある PC_B から SSL-VPN を通じて、PC_A へのアクセスを目的としております。SSL-VPN はトンネルモード、Web モードを両方とも有効にし、社内ネットワーク宛に対しスプリットトンネルを設定しています。

■設定値一覧

①インターフェース情報

項番	インターフェース名	IPアドレス	サブネットマスク	アクセス
1	port2	192.168.1.254	255.255.255.0	ping,https,ssh
2	port1	10.0.0.254	255.255.255.0	-

②ルーティング情報

項番	宛先IP/マスク	デバイス	ゲートウェイ
1	0.0.0.0/0.0.0.0	port1	10.0.0.1

③ユーザ情報

項番	ユーザ名	パスワード	ユーザグループ名
1	test-user	password	test-group

④ファイアウォールアドレス

項番	名前	サブネット/IP範囲
1	Syanai_Network	192.168.1.0/24

⑤SSL-VPN

項番	名前	トンネルモード	スプリットトンネル	IPプール	Webモード
1	TEST-full_access	有効	有効	Syanai_Network	有効

⑥Firewallポリシー

項番	ソースインターフェース名	ソースアドレス	デストインターフェース名	デストアドレス	ポリシータイプ	スケジュール	サービス	アクション	NAT
1	port2	all	port1	all	ファイアウォール	always	ALL	ACCEPT	有効
2	port1	all	port2	Syanai_Network	VPN	-	-	ACCEPT	無効

⑦SSL-VPN認証ルール

項番	グループ	スケジュール	スケジュール	SSL-VPNポータル
1	test-group	always	always	TEST-full_access

3 SSL-VPN 設定

本項目では、SSL-VPN 接続をするための設定を行います。

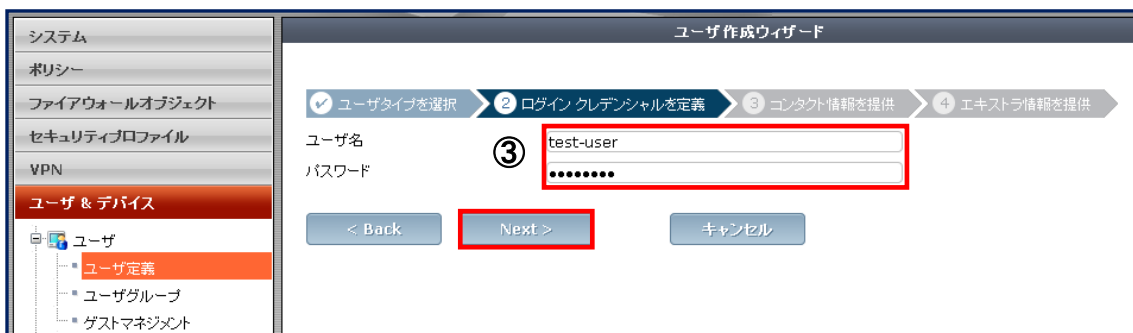
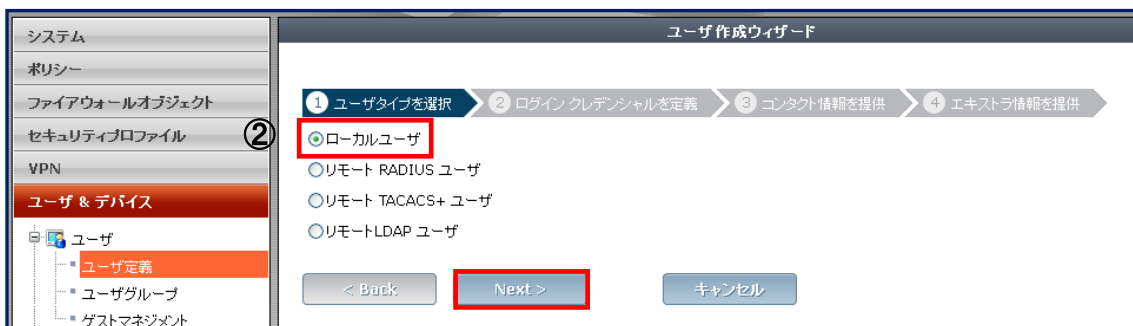
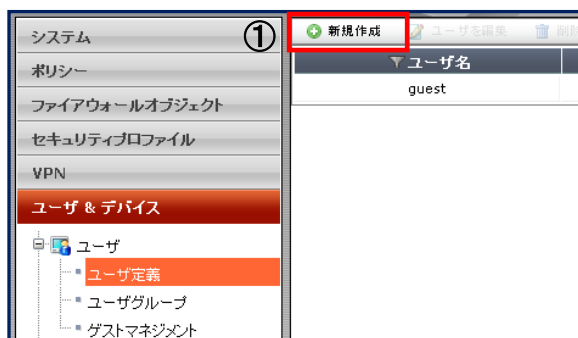
3.1 ユーザ・ユーザグループの作成

下記の手順でユーザとユーザグループを作成します。

3.1.1 ユーザの作成

GUI より、ユーザ&デバイス>ユーザ>ユーザ定義にて、ユーザを作成します。

- ① [新規作成]をクリック。
- ② [ローカルユーザ]を選択し、[Next]をクリック。
- ③ ユーザ名:『test-user』
パスワード:『password』
[Next]をクリック。
- ④ [Next]をクリック。
- ⑤ [有効]:有効
- ⑥ [Done]をクリック。



システム
ポリシー
ファイアウォールオブジェクト
セキュリティプロファイル
VPN
ユーザ & デバイス
ユーザ
ユーザ定義
ユーザグループ
ゲストマネジメント

ユーザ作成ウィザード

1 ユーザタイプを選択 2 ログイン クレデンシャルを定義 3 コンタクト情報を提供 4 エキストラ情報を提供

Emailアドレス

☐ SMS

4 Next >

< Back キャンセル

システム
ルータ
ポリシー
ファイアウォールオブジェクト
セキュリティプロファイル
VPN
ユーザ & デバイス
ユーザ
ユーザ定義
ユーザグループ
ゲストマネジメント

ユーザ作成ウィザード

1 ユーザタイプを選択 2 ログイン クレデンシャルを定義 3 コンタクト情報を提供 4 エキストラ情報を提供

5 ☒ 有効

☐ 二要素認証

☐ ユーザグループ

設定をクリック...

6 Done

< Back キャンセル

3.1.2 ユーザグループの作成

GUI より、ユーザ&デバイス>ユーザ>ユーザグループにて、ユーザグループを作成します。

- ① [新規作成]をクリック。
- ② [名前]:test-group
- ③ [メンバー]:test-user
- ④ [OK]をクリック。

システム
ルータ
ポリシー
ファイアウォールオブジェクト
セキュリティプロファイル
VPN
ユーザ & デバイス
ユーザ
ユーザ定義
ユーザグループ

① 新規作成

グループ名

FSSO_Guest_Users

Guest-group

システム
ポリシー
ファイアウォールオブジェクト
セキュリティプロファイル
VPN
ユーザ & デバイス
ユーザ
ユーザ定義
ユーザグループ
ゲストマネジメント

New User Group

名前 ② test-group

タイプ (RSSO) ③ ☒ ファイアウォール ☐ Fortinet シングルサインオン(FSSO) ☐ ゲスト ☐ RADIUSシングルサインオン

メンバー

リモート認証サーバー

選択してください

guest

test-user

一致するエントリが見つかりません。

④ OK

キャンセル

3.2 ファイアウォールオブジェクトの作成

アクセス先アドレスオブジェクトと、VPN クライアントへ払い出すアドレスオブジェクトを作成します。

3.2.1 アクセス先ネットワーク指定用アドレスオブジェクトの作成

GUI より、ダイアウォールオブジェクト>アドレス>アドレスにて、アドレスオブジェクトを作成します。

- ① [新規作成]をクリック。
- ② [名前]: Syanai_Network
- ③ [サブネット/IP 範囲]: 192.168.1.0/255.255.255.0
- ④ [インターフェース]: port2
- ⑤ [OK]をクリック。

The screenshot shows the 'ファイアウォールオブジェクト' (Firewall Object) configuration window. On the left, the 'アドレス' (Address) tab is selected. In the center, the '新規作成' (New) button is highlighted with a red box and labeled ①. The right pane shows the '新規アドレス' (New Address) form. The fields are filled as follows: '名前' (Name) is 'Syanai_Network' (labeled ②), 'タイプ' (Type) is 'サブネット' (Subnet), 'サブネット / IP 範囲' (Subnet / IP Range) is '192.168.1.0/255.255.255.0' (labeled ③), 'インターフェース' (Interface) is 'port2' (labeled ④), and 'アドレスリストに表示' (Display in address list) is checked. The 'コメント' (Comment) field is empty. The 'OK' button is highlighted with a red box and labeled ⑤.

3.2.2 クライアント使用用アドレスオブジェクトの作成

3.1.1 と同様に、クライアントへ払い出すアドレスオブジェクトを作成します。

- ① [新規作成]をクリック。
- ② [名前]: SSL-VPN_Client
- ③ [タイプ]: IP 範囲
- ④ [サブネット/IP 範囲]: 192.168.255.100-192.168.255.110
- ⑤ [OK]をクリック。

The screenshot shows the 'ファイアウォールオブジェクト' (Firewall Object) configuration window. On the left, the 'アドレス' (Address) tab is selected. In the center, the '新規作成' (New) button is highlighted with a red box and labeled ①. The right pane shows the '新規アドレス' (New Address) form. The fields are filled as follows: '名前' (Name) is 'SSL-VPN_Client' (labeled ②), 'タイプ' (Type) is 'IP範囲' (IP Range) (labeled ③), 'サブネット / IP 範囲' (Subnet / IP Range) is '192.168.255.100-192.168.255.110' (labeled ④), 'インターフェース' (Interface) is 'Any', and 'アドレスリストに表示' (Display in address list) is checked. The 'コメント' (Comment) field is empty. The 'OK' button is highlighted with a red box and labeled ⑤.

3.3 SSL-VPN ポータル作成

SSL-VPN へ接続するためのポータルを作成します。

3.3.1 SSL-VPN ポータル作成

GUI より、VPN > SSL > ポータル にて、SSL-VPN ポータルを作成します。

- ① [新規作成]をクリック。
- ② [名前]: TEST-full_access
- ③ [トンネルモード有効]: 有効
[スプリットトンネル有効]: 有効
[IP プール]: SSL-VPN_Client
- ④ [Web モード有効]: 有効
- ⑤ [OK]をクリック。

①

SSL-VPN ポータル編集 full-access

名前: full-access
ポータルメッセージ: Welcome to SSL VPN Service
テーマ: ブルー

新規SSL-VPN ポータル

名前: ② TEST-full_access
ポータルメッセージ: Welcome to SSL VPN Service
テーマ: ブルー
ページレイアウト: [Icons]

③ ☒ トンネルモード有効
☒ スプリットトンネル有効
 IPプール: SSL-VPN_Client

クライアントオプション ☐ パスワード保存 ☐ オートコネクト ☐ 常にアップ (Keep Alive)

④ ☒ Webモード有効

アプリケーション
☐ HTTP/HTTPS ☐ FTP ☐ RDP ☐ SMB/CIFS
☐ SSH ☐ TELNET ☐ VNC ☐ PING
☐ CITRIX ☐ RDPネイティブ ☐ ポートフォワード

☒ セッション情報を含む
☒ コネクションツールを含む
☒ FortiClientダウンロードを含む
☒ ログイン履歴を含む
 履歴エントリー数: 5
☒ ブックマークを含む

☒ モバイルユーザにFortiClientアプリケーションをダウンロードするよう促す
☒ 各ユーザに複数のコンカレントセッションを許可する

⑤ OK キャンセル

3.4 ファイアウォールポリシーの作成

GUI より、ポリシー>ポリシー>ポリシーにて、SSL-VPN 接続用のポリシーを作成します。

- ① [新規作成]をクリック。
- ② [ポリシータイプ]:VPN
- ③ [incoming インターフェース]:port1
[リモートアドレス]:all
- ④ [ローカルインターフェース]:port2
[ローカルの保護サブネット]:Syantai_Network
- ⑤ [Create New]をクリック。
- ⑥ [グループ]:test-group
- ⑦ [SSL-VPN ポータル]:TEST-full_access
- ⑧ [OK]をクリック。
- ⑨ [OK]をクリック。

The first screenshot shows the 'システム' (System) menu with 'ポリシー' (Policy) selected. The '新規作成' (Create New) button is highlighted with a red box and circled with ①.

The second screenshot shows the '新規ポリシー' (New Policy) dialog. The 'ポリシータイプ' (Policy Type) is set to 'VPN' (circled with ②). The 'incoming インターフェース' (Incoming Interface) is 'port1' (circled with ③) and the 'リモートアドレス' (Remote Address) is 'all' (circled with ③). The 'ローカルインターフェース' (Local Interface) is 'port2' (circled with ④) and the 'ローカルの保護サブネット' (Local Protected Subnet) is 'Syantai_Network' (circled with ④). The 'SSL-VPN認証ルールを設定' (Set SSL-VPN Authentication Rules) section has 'Create New' highlighted with a red box and circled with ⑤. The 'ユーザ/グループ' (User/Group) dropdown is 'ANY', 'サービス' (Service) is 'ALL', 'スケジュール' (Schedule) is 'always', 'セキュリティ' (Security) is 'ACCEPT', and 'SSL-VPNポータル' (SSL-VPN Portal) is 'TEST-full_access'. The 'コメント' (Comment) field is empty. The 'OK' button is highlighted with a red box and circled with ⑨.

The third screenshot shows the '新規 SSL VPN認証ルール' (New SSL VPN Authentication Rule) dialog. The 'グループ' (Group) is 'test-group' (circled with ⑥). The 'ユーザ' (User) is 'always' (circled with ⑦). The 'スケジュール' (Schedule) is 'always'. The 'SSL-VPNポータル' (SSL-VPN Portal) is 'TEST-full_access' (circled with ⑦). The 'アクション' (Action) is 'ACCEPT'. The 'ログオプション' (Log Option) is 'セキュリティイベントをログする' (Log security events). The 'セキュリティプロファイル' (Security Profile) section has 'アンチウイルス' (Anti-virus), 'Webフィルタ' (Web filter), 'アプリケーションコントロール' (Application control), and 'IPS' all set to 'default'. The 'OK' button is highlighted with a red box and circled with ⑧.

4 VPN 接続、接続確認

PC2 から FortiGate へ VPN 接続を行います。

4.1 Web ポータルログイン

Web ポータルへ接続します。

- ① ブラウザを立ち上げ、https で port1 へアクセス。
URL: https://10.0.0.254
- ② [Name]: test-user
- ③ [Password]: password
- ④ [Login]をクリック。



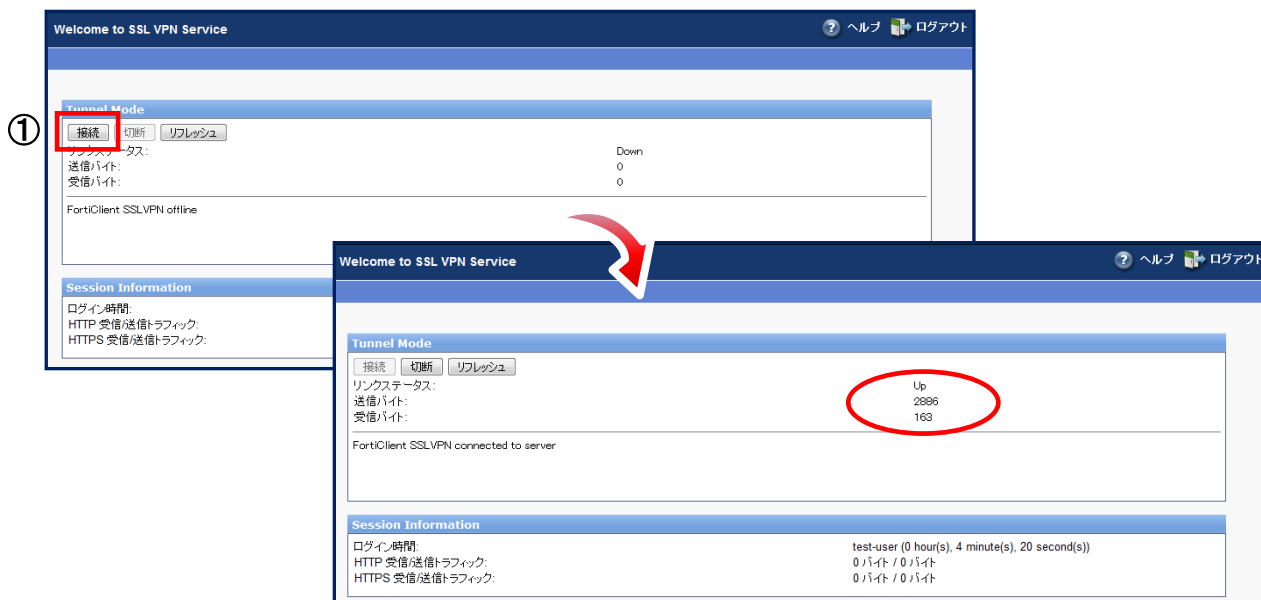
4.2 トンネルモード接続

Web ポータルからトンネルモードへ接続します。

- ① [接続]をクリック。

接続後は、[リンクステータス]: Up となり、トラフィックが流れます。

※事前に SSL-VPN クライアントモジュールをインストールする必要があります。



※FortiClient を使用しての接続、SSL-VPN トンネルモードのご利用について詳しくは:

-FAQ-ID=2626

- [SSL-VPN トンネルモード利用方法について](#)をご覧ください。

4.3 SSL-VPN トンネルモード接続確認

正しく VPN 接続できているか、コマンドプロンプトを使用して確認します。

■ipconfig

VPN 接続用に IP アドレスが割り当てられています。

```
PPP アダプター fortissl:

  接続固有の DNS サフィックス . . . . :
  IPv4 アドレス . . . . . : 192.168.255.100
  サブネット マスク . . . . . : 255.255.255.255
  デフォルト ゲートウェイ . . . . . :

イーサネット アダプター ローカル エリア接続:

  接続固有の DNS サフィックス . . . . : flets-east.jp
  リンクローカル IPv6 アドレス . . . . : fe80::14:6522:2c57:1f02%11
  IPv4 アドレス . . . . . : 1.1.1.1
  サブネット マスク . . . . . : 255.255.255.0
  デフォルト ゲートウェイ . . . . . : 1.1.1.254
```

■routeprint

ルート情報に新たに社内セグメント[192.168.1.0]宛のルートが追加されています。

```
IPv4 ルート テーブル
=====
アクティブ ルート:
ネットワーク宛先      ネットマスク      ゲートウェイ      インターフェイ
ス      メトリック
0.0.0.0      0.0.0.0      1.1.1.254      1.1.1.1      266
1.1.1.0      255.255.255.0      リンク上      1.1.1.1      266
1.1.1.1      255.255.255.255      リンク上      1.1.1.1      266
1.1.1.255      255.255.255.255      リンク上      1.1.1.1      266
10.0.0.254      255.255.255.255      1.1.1.254      1.1.1.1      10
127.0.0.0      255.0.0.0      リンク上      127.0.0.1      306
127.0.0.1      255.255.255.255      リンク上      127.0.0.1      306
127.255.255.255      255.255.255.255      リンク上      127.0.0.1      306
192.168.1.0      255.255.255.0      192.168.255.101      192.168.255.100      20
192.168.255.100      255.255.255.255      リンク上      192.168.255.100      276
224.0.0.0      240.0.0.0      リンク上      127.0.0.1      306
224.0.0.0      240.0.0.0      リンク上      1.1.1.1      266
224.0.0.0      240.0.0.0      リンク上      192.168.255.100      276
255.255.255.255      255.255.255.255      リンク上      127.0.0.1      306
255.255.255.255      255.255.255.255      リンク上      1.1.1.1      266
255.255.255.255      255.255.255.255      リンク上      192.168.255.100      276
=====
```

■tracert

```
C:\Documents and Settings¥Administrator>tracert 192.168.1.1

192.168.1.1 へのルートをトレースしています。経由するホップ数は最大 30 です

 1    1 ms    <1 ms    <1 ms    192.168.255.100
 2    1 ms    1 ms    <1 ms    192.168.1.1
```