

OS5.2 SSL-VPN 設定手順書

Ver. 1.1

承認	確認	担当

2015 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
3.3.2	SSL-VPN 詳細設定	10
3.4	ファイアウォールポリシーの作成	11
4	VPN 接続、接続確認	12
4.1	Web ポータルログイン	12
4.2	トンネルモード接続	12
4.3	SSL-VPN トンネルモード接続確認	13

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	2015/02/28	1.0		o	新規作成	NWL	NWL
2	2015/11/10	1.1		r	OS5.2.4 へ内容を修正	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

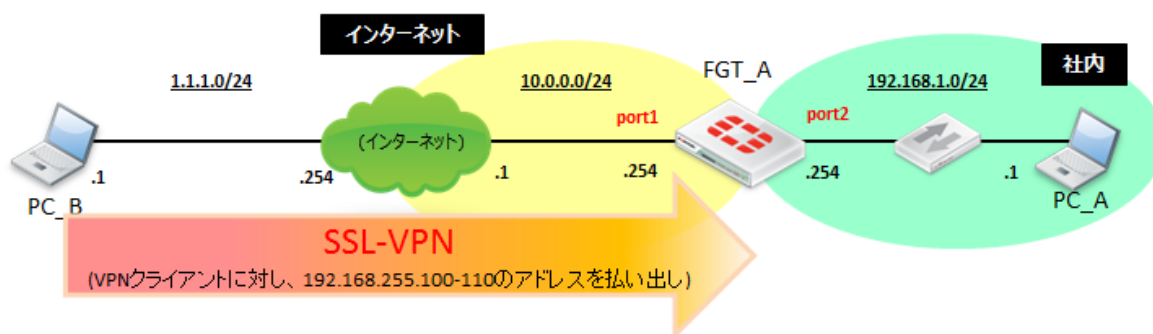
■はじめに

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 5.2.4

PC_A: Windows 7 Professional

PC_B: Windows 7 Professional

■設定内容説明

本手順書は、インターネット上にある PC_B から SSL-VPN 経路を介して、PC_A へアクセスするための設定手順について説明しております。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て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
2	SSL-VPN_Client	192.168.255.100-192.168.255.110

⑤SSL-VPNポータル

項番	名前	トンネルモード	スプリットトンネル	ルーティングアドレス	IPプール	Webモード
1	TEST-full_access	有効	有効	Syanai_Network	SSL-VPN_Client	有効

⑥SSL-VPN設定

項番	Listenするインタフェース	Listenするポート	アクセスを制限	アドレス範囲	IP範囲
1	TEST-full_access	10443	任意のホストからアクセス許可	カスタムIP範囲を指定	SSL-VPN_Client

ユーザ/グループ	ポータル	ユーザ/グループ	ポータル
test-group	TEST-full_access	すべてのその他のユーザ/グループ	web-access

⑦Firewallポリシー

項番	入力インターフェース名	送信元アドレス	送信元ユーザ	出力インターフェース名	出力アドレス	スケジュール	サービス	アクション	NAT
1	port2	all	all	port1	all	always	ALL	ACCEPT	有効
2	ssl.root	all	test-group	port2	Syanai_Network	always	ALL	ACCEPT	有効

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。

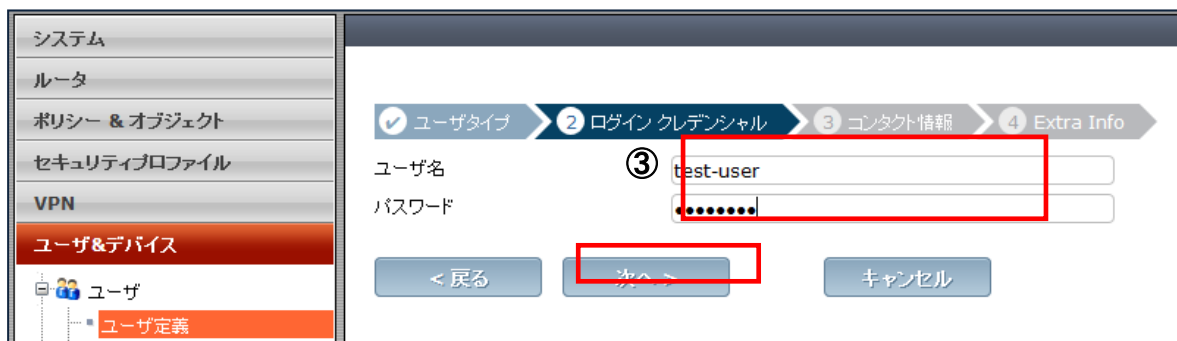
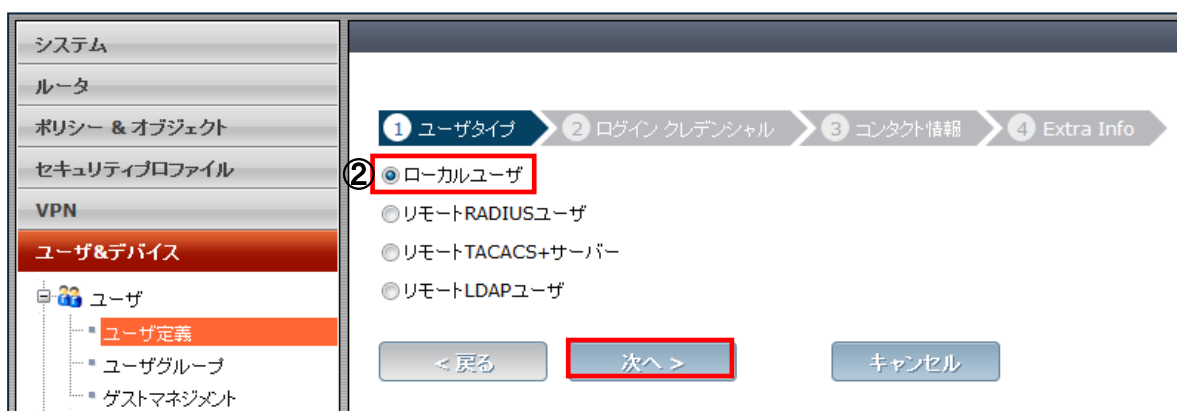
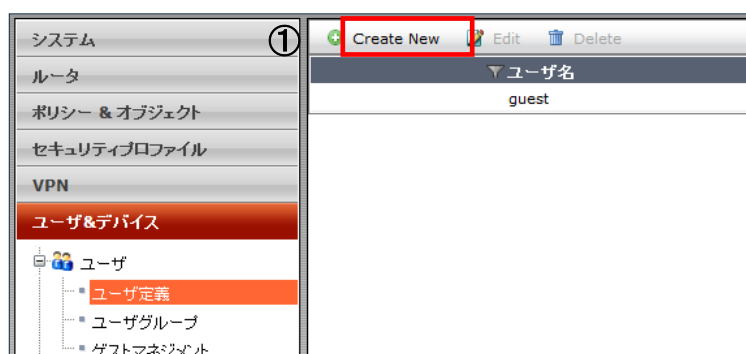
3.1 ユーザ・ユーザグループの作成

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 [Create New]をクリック。
- ② [Local User]を選択し、[次へ]をクリック。
- ③ ユーザ名:『test-user』
パスワード:『password』
[次へ]をクリック。



- ④ [次へ]をクリック。
- ⑤ [有効]:有効
- ⑥ [作成]をクリック。

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 [Create New]をクリック。
- ② [名前]:test-group
- ③ [メンバー]:test-user
- ④ [OK]をクリック。

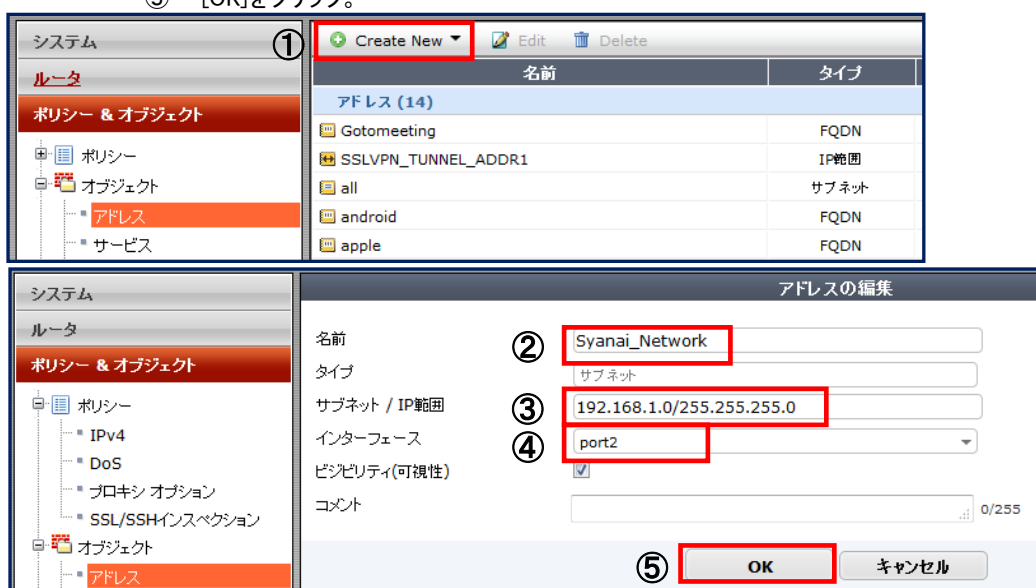
3.2 ファイアウォールオブジェクトの作成

アクセス先の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、ファ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。

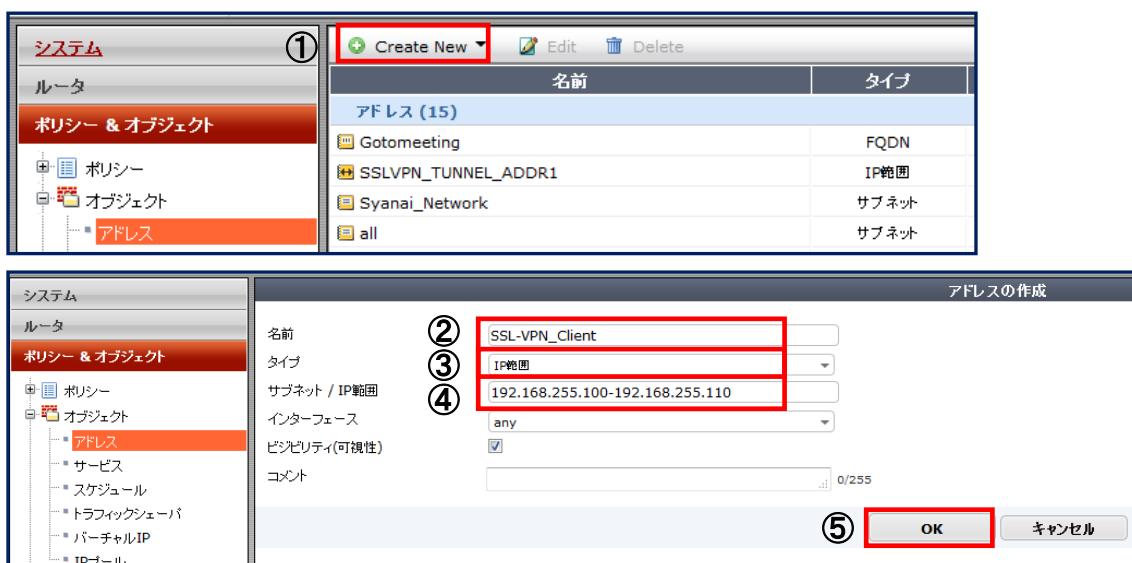
- ① [Create New]をクリック。
- ② [名前]: Syanai_Network
- ③ [サブネット/IP 範囲]: 192.168.1.0/255.255.255.0
- ④ [インターフェース]: port2
- ⑤ [OK]をクリック。



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

3.2.1 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 [Create New]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。



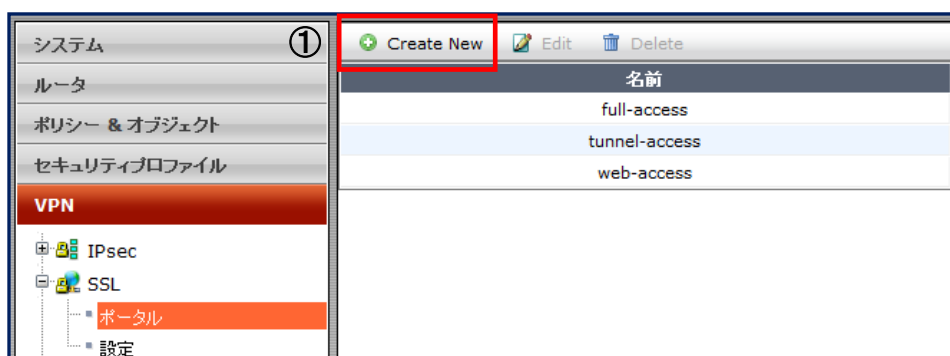
3.3 SSL-VPN ポータル作成

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 [Create New]をクリック。
- ② [名前]: TEST-full_access
- ③ [トンネルモード有効]: 有効
[スプリットトンネリングを有効]: 有効
[ルーティングアドレス]: Syanai-Network
[IP プール]: SSL-VPN_Client
- ④ [Web モード有効]: 有効
- ⑤ [OK]をクリック。



3.3.2 SSL-VPN 詳細設定

GUI より、VPN > SSL > 設定 にて、SSL-VPN の詳細設定を行います。

- ① [Listen するインターフェース]: port1
- ② [Listen するポート]: 10443
※デフォルトでは 443 が指定されておりますが、管理コンソール[HTTPS]のポート番号とバッティングするため、SSL-VPN ログイン用にポート番号を指定します。
- ③ [アクセスを制限]: 任意のホストからアクセス許可
- ④ [アドレス範囲]: カスタム IP 範囲を指定
[IP 範囲]: SSL-VPN_Client

※認証/ポータルマッピングでは、ユーザ情報とポータルの紐付けを行います。

[すべてのその他のユーザ/グループ]と紐付けたポータルはすべてのユーザからアクセスできてしまうため、ご注意ください。

- ⑤ [Create New]をクリック。
- ⑥ [ユーザ/グループ]: test-group
[ポータル]: TEST-full_access
- ⑦ [OK]をクリック。
- ⑧ [未設定]をクリック。
- ⑨ [ポータル]: web-access
- ⑩ [OK]をクリック。
- ⑪ [適用]をクリック。

The screenshot shows the FortiGate SSL-VPN configuration page. The left sidebar has 'VPN' selected, with 'SSL' and '設定' (Settings) highlighted. The main area is titled 'SSL-VPN設定' and contains several sections:

- 接続設定 (Connection Settings):**
 - Listenするインターフェース: ① port1
 - Listenするポート: ② 10443
 - アクセスを制限: ③ 任意のホストからアクセス許可
 - アイドル ログアウト: Inactive For 300 (秒)
 - サーバ証明書: Self-Signed
 - クライアント証明書を要求: []
- トンネルモード クライアント設定 (Tunnel Mode Client Settings):**
 - アドレス範囲: ④ カスタムIP範囲を指定
 - IP範囲: SSL-VPN_Client
 - DNSサーバ: クライアントシステムのDNSと同じ
 - WINSサーバを指定: []
 - エンドポイント登録を許可: []
- 認証/ポータルマッピング (Authentication/Portal Mapping):**
 - ⑤ Create New button
 - Table with columns: ユーザ/グループ, ポータル
 - Row 1: test-group, TEST-full_access
 - Row 2: すべてのその他のユーザ/グループ, ⑧ 未設定

At the bottom, there are two modal windows:

- 新規認証/ポータルマッピング (New Authentication/Portal Mapping):**
 - ⑥ ユーザ/グループ: test-group
 - ⑥ ポータル: TEST-full_access
 - ⑦ OK button
- デフォルトの認証/ポータルマッピングを編集 (Edit Default Authentication/Portal Mapping):**
 - ⑨ ポータル: web-access
 - ⑩ OK button

The '適用' (Apply) button is highlighted with ⑪.

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 [Create New]をクリック。
- ② [入カインタフェース]:ssl.root(SSL VPN interface)
[送信元アドレス]:all
[送信元ユーザ]:test-group
- ③ [出カインタフェース]:port2
[宛先サブネット]:Syanai_Network
- ④ [サービス]:ALL
- ⑤ 画面下部の[OK]をクリック。



以上で、SSL-VPN の設定は完了です。

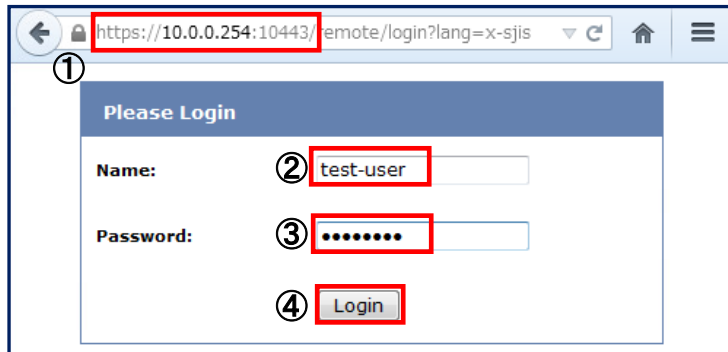
4 VPN 接続、接続確認

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://10.0.0.254:10443
- ② [Name]: test-user
- ③ [Password]: password
- ④ [Login]をクリック。



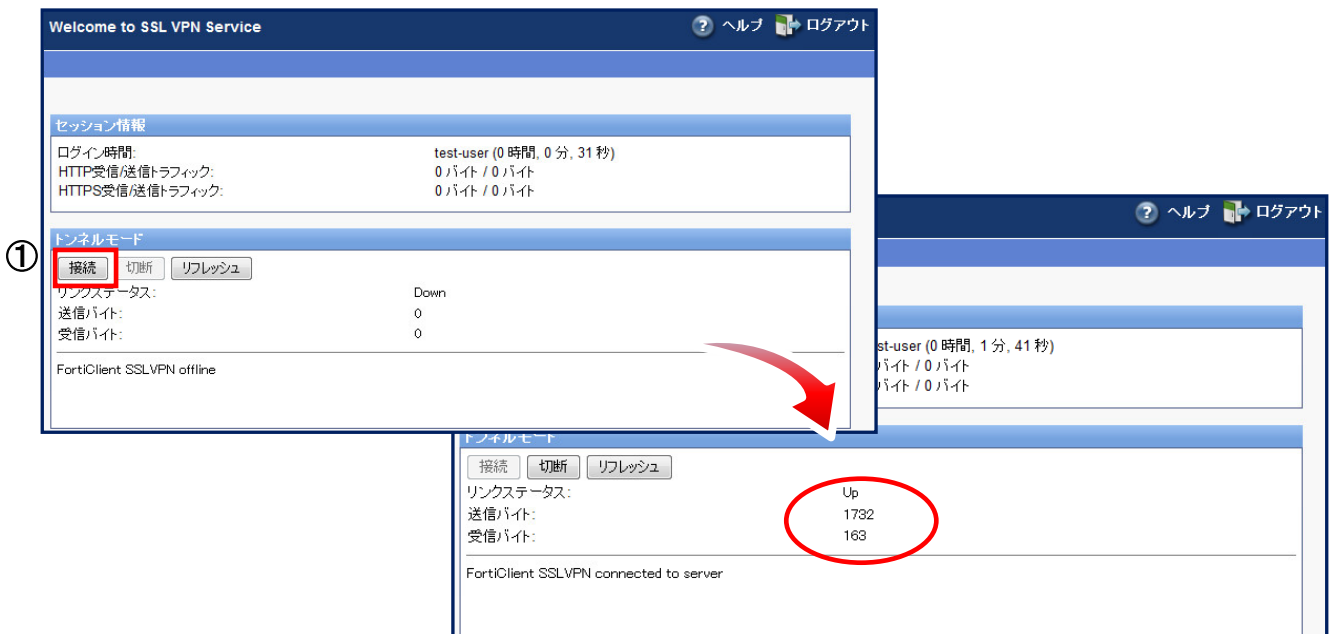
4.2 トンネルモード接続

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

トンネルモードで正しく 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 . . . . : 
  リンクローカル IPv6 アドレス . . . . : fe80::c143:4eda:b2bf:de31%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
```

■route print

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:\Users\admin>tracert -d 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    *      2 ms     9 ms     192.168.1.1

トレースを完了しました。

C:\Users\admin>
```