

OS5.6 SSL-VPN 設定手順書

Ver. 1.0

承認	確認	担当

2018 年 07 月 26 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	8
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	9
3.3	SSL-VPN ポータル作成	10
3.3.1	SSL-VPN ポータル作成	10
3.3.2	SSL-VPN 詳細設定	11
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	13
4.1	Web ポータルログイン	13
4.2	トンネルモード接続	13
4.3	SSL-VPN トンネルモード接続確認	15

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	2018/07/26	1.0		o	新規作成	NWL	NWL
2							
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://tec-world.networld.co.jp/login>

- ・Fortinet FAQ

Fortinet製品に関するよくある問い合わせ

<https://tec-world.networld.co.jp/>

■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

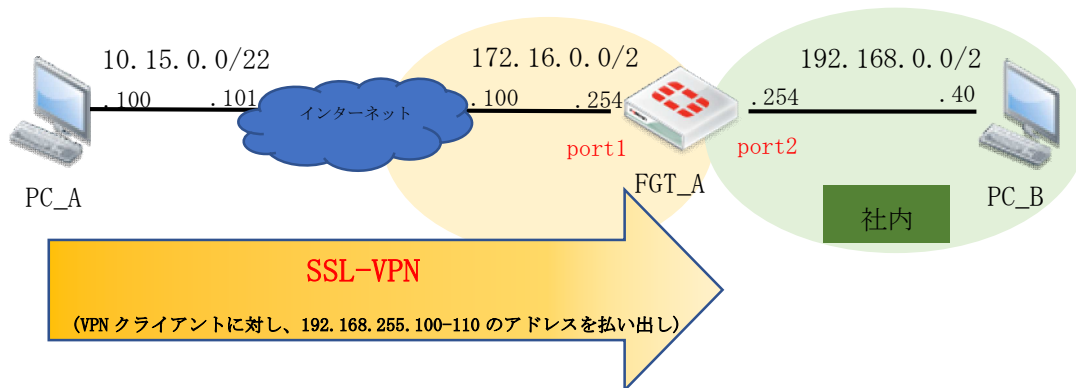
■はじめに

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://tec-world.networld.co.jp/faq/show/2526>

■構成図



■機器情報・ファームウェア

FGT_A: FortiGate-VM00

FortiOS 5.6.5

PC_A: Windows 10 Professional

PC_B: Windows 10 Professional

■設定内容説明

本手順書は、インターネット上にある PC_A から SSL-VPN 経路を介して、PC_B 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

FGT_A

①インターフェース

項番	インターフェース	IPアドレス	サブネットマスク	アクセス
1	port1	172.16.0.254	255.255.255.0	-
2	port2	192.168.0.254	255.255.255.0	ping,https,ssh

②ルーティング

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	172.16.0.100

③ユーザ

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	SyanaiNetwork	192.168.0.0/255.255.255.0
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	full-access	有効	有効	SyanaiNetwork	SSL-VPN_Client	有効

⑥SSL-VPN設定

項番	Listenするインターフェース	Listenするポート	アクセスを制限	アドレス範囲	IP範囲
1	port1	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
すべてのその他のユーザ/グループ	full-access

⑦Firewallポリシー

項番	名前	入力インターフェース	出力インターフェース	送信元アドレス	送信元ユーザ	宛先
1	test-policy	SSL-VPNトンネルインターフェース	port2	all	test-group	SyanaiNetwork

スケジュール	サービス	アクション	NAT
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 > ユーザ定義 にて、ユーザを作成します。

- ① [ローカルユーザ]を選択し、[次へ]をクリック。



- ② ユーザ名:『test-user』
パスワード:『password』
[次へ]をクリック。



- ③ [次へ]をクリック。

ダッシュボード > Users/Groups Creation Wizard

1 ユーザタイプ 2 ログインクレデンシャル 3 **コンタクト情報** 4 エキストラ情報

Eメールアドレス

☐ SMS

☐ 二要素認証

< 戻る **次へ** キャンセル

- ④ [ユーザアカウントステータス]: 有効化済み
[サブミット]をクリック。

ダッシュボード > Users/Groups Creation Wizard

1 ユーザタイプ 2 ログインクレデンシャル 3 コンタクト情報 4 **エキストラ情報**

ユーザアカウントステータス **有効化済み** 無効化済み

ユーザグループ

< 戻る **サブミット** キャンセル

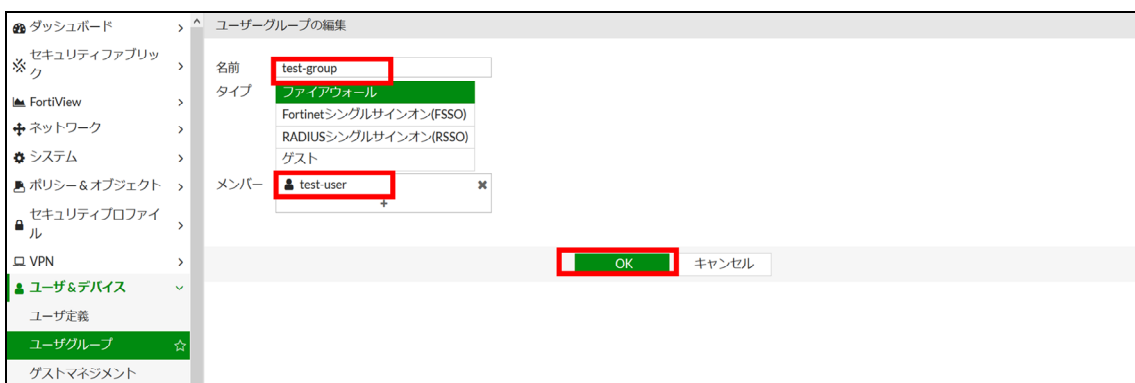
3.1.2 ユーザグループの作成

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
[メンバー]: test-user
[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、ポリシー&オブジェクト > 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]プルダウンメニューから[アドレス]をクリック。



- ② [名前]: Syanai_Network
 [タイプ]: サブネット
 [サブネット/IP 範囲]: 192.168.0.0/255.255.255.0
 [インタフェース]: port2
 [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 [新規作成]プルダウンメニューから[アドレス]をクリック。

- ② [名前]: SSL-VPN_Client
 [タイプ]: IP 範囲
 [サブネット/IP 範囲]: 192.168.255.100-192.168.255.110
 [インタフェース]: any
 [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。

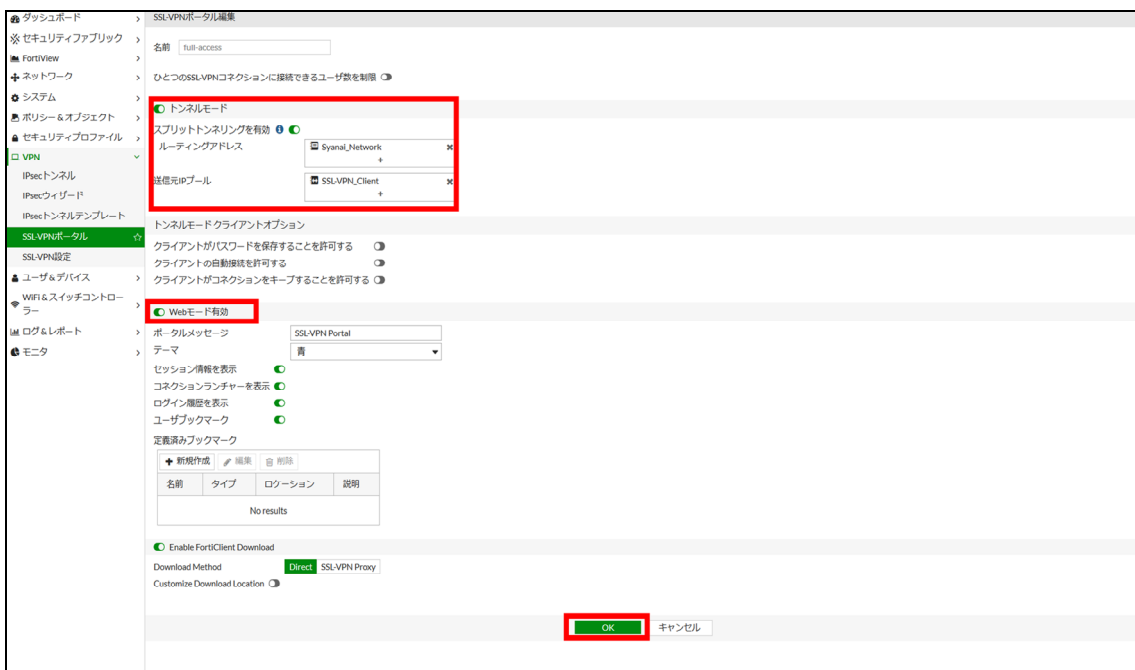
3.3.1 SSL-VPN ポータル作成

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

- ① [full-access]をダブルクリック。



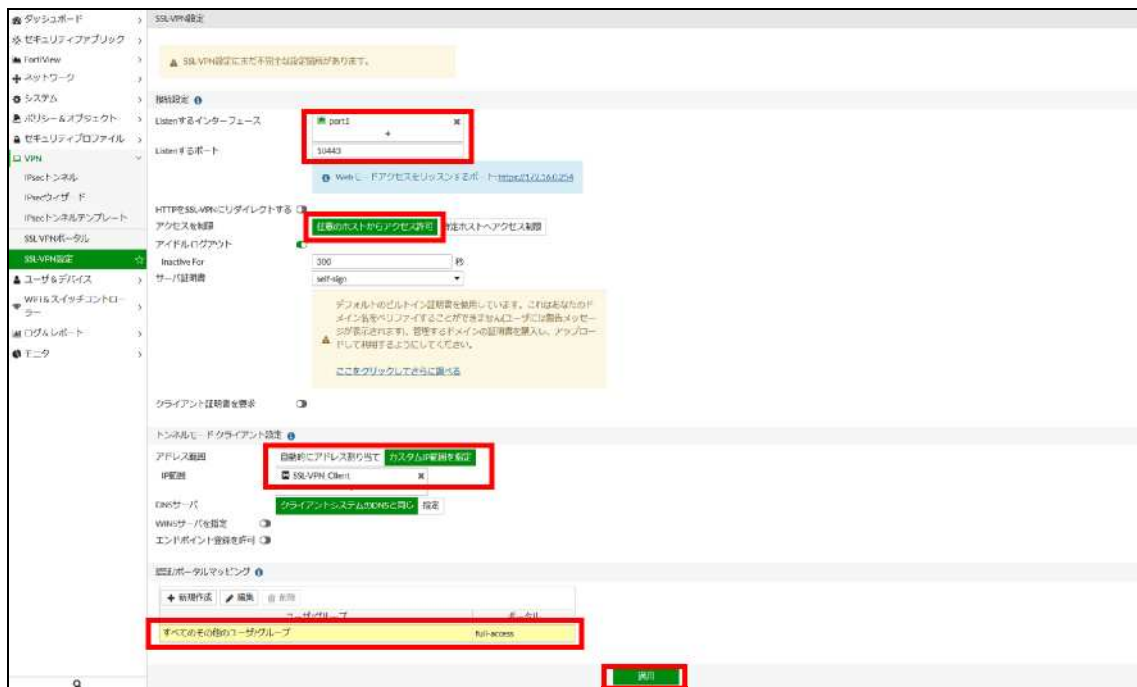
- ② [トンネルモード有効]: 有効
 [スプリットトンネリングを有効]: 有効
 [ルーティングアドレス]: Syanai-Network
 [送信元 IP プール]: SSL-VPN_Client
 [Web モード有効]: 有効
 [OK]をクリック。



3.3.2 SSL-VPN 詳細設定

GUI より、VPN > SSL-VPN 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
 [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。
 [アクセスを制限]: 任意のホストからアクセス許可
 [アドレス範囲]: カスタム IP 範囲を指定
 [IP 範囲]: SSL-VPN_Client
 [すべてのその他のユーザ/グループ]: full-access
 [適用]をクリック。



3.4 ファイアウォールポリシーの作成

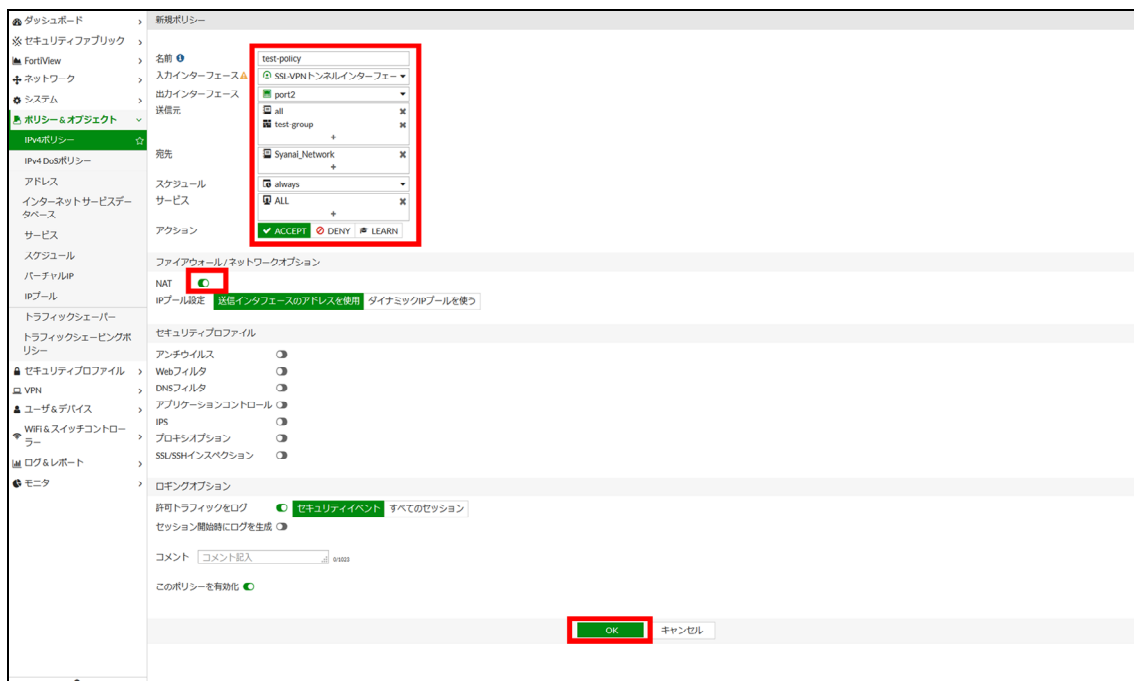
GUI より、ポリシー&オブジェクト > IPv4 ポリシー にて、SSL-VPN 接続用のポリシーを作成します。

- ① [新規作成]をクリック。



- ② [名前]: 任意
 [入力インターフェース]: SSL-VPN トンネルインターフェース
 [出カインターフェース]: port2
 [送信元アドレス]: all
 [送信元ユーザ]: test-group
 [宛先]: Syanai_Network
 [スケジュール]: always
 [サービス]: ALL
 [アクション]: ACCEPT

[NAT]:有効
画面下部の[OK]をクリック。



以上で、SSL-VPN の設定は完了です。

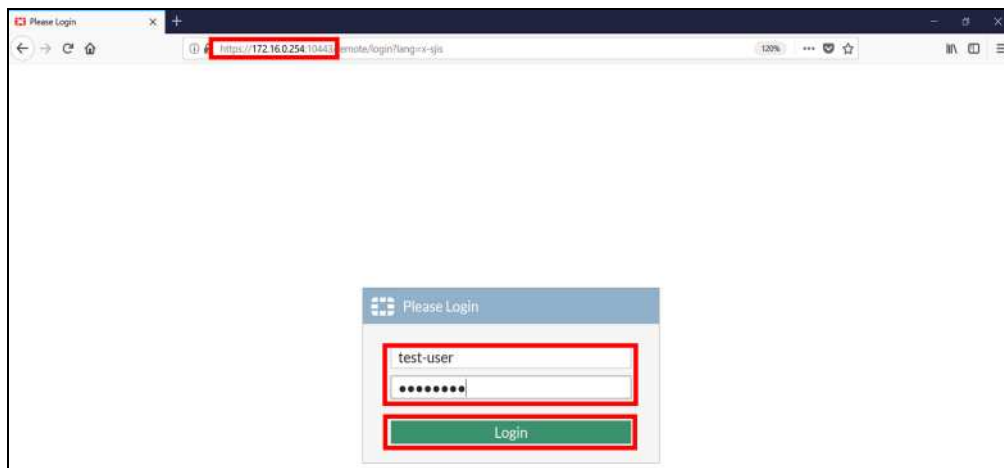
4 VPN 接続、接続確認

PC1 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://172.16.0.254:10443
[Name]: test-user
[Password]: password
[Login]をクリック。



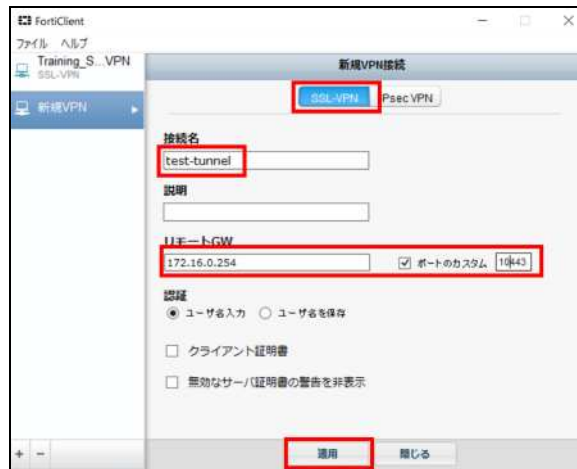
接続が成功するとポータル画面が表示されます。



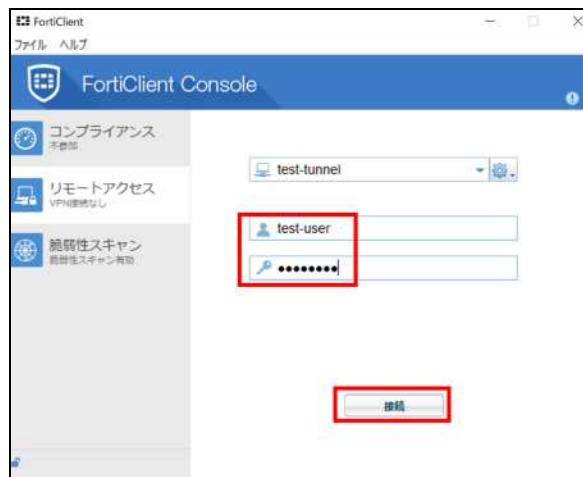
4.2 トンネルモード接続

FortiClient からトンネルモードへ接続します。
※事前にインストールする必要があります。

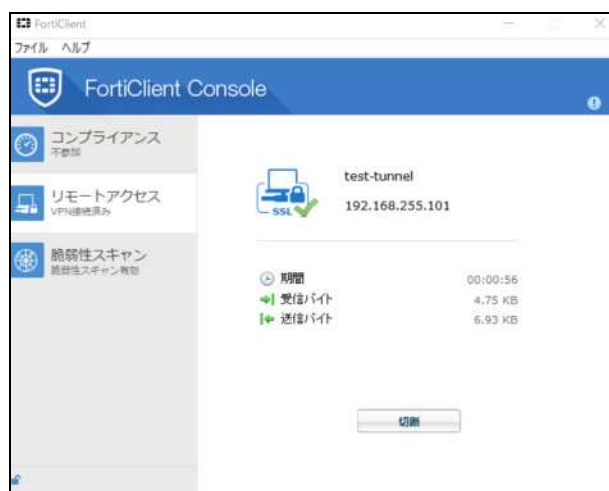
- ① [新規 VPN]をクリック。
[SSL-VPN]を選択
[接続名]: test-tunnel
[リモート GW]: 172.16.0.254
[ポートのカスタム]: 10443
[適用]をクリック。



② トンネルモードへ接続



③ 接続成功例



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。

※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：
[”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。

```
C:\Users\%username>ipconfig

Windows IP 構成

イーサネット アダプター イーサネット 4:
    接続固有の DNS サフィックス . . . . . : 
    IPv4 アドレス . . . . . : 192.168.255.100
    デフォルト ゲートウェイ . . . . . : 255.255.255.255

イーサネット アダプター イーサネット 1:
    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::84c4:7f3e:9bb4:aedd%2
    IPv4 アドレス . . . . . : 10.15.0.100
    サブネット マスク . . . . . : 255.255.252.0
    デフォルト ゲートウェイ . . . . . : fe80::5:73ff:fea0:73%2

Wireless LAN adapter ローカル エリア接続* 2:
    メディアの状態 . . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :
```

■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。

```
C:\Users\%username>route print

インターフェイス一覧
6...00 09 0f aa 00 01 ..... Fortinet SSL VPN Virtual Ethernet Adapter
2...60 45 bd 7b e7 af ..... Surface Ethernet Adapter
7...52 1a c5 e4 f2 66 ..... Microsoft Wi-Fi Direct Virtual Adapter
15...00 09 0f fa 00 01 ..... Fortinet Virtual Ethernet Adapter (NDIS 6.30)
5...50 1a c5 e4 f3 67 ..... Marvell AVASTAR Wireless-AC Network Controller
4...60 02 92 7e ae e4 ..... Bluetooth デバイス (パーソナル エリア ネットワーク)
1... .. Software Loopback Interface 1
21...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface

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
10.15.0.0              255.255.252.0      リンク上          10.15.0.100            281
10.16.0.100            255.255.255.255    リンク上          10.15.0.100            281
10.16.3.255            255.255.255.255    リンク上          10.15.0.100            281
127.0.0.0              255.0.0.0          リンク上          127.0.0.1              331
127.0.0.1              255.255.255.255    リンク上          127.0.0.1              331
127.255.255.255        255.255.255.255    リンク上          127.0.0.1              331
192.168.0.0            255.255.255.255    10.15.0.101       10.15.0.100            26
192.168.0.0            255.255.255.255    192.168.255.101   192.168.255.100        1
192.168.255.100        255.255.255.255    リンク上          192.168.255.100        281
224.0.0.0              240.0.0.0          リンク上          127.0.0.1              331
```

■tracert

```
C:\Users\%username>tracert 192.168.0.40

WIN7PRO [192.168.0.40] へのルートをトレースしています
経路するホップ数は最大 30 です:

 1    2 ms    1 ms    2 ms SF-02669 [192.168.255.100]
 2    3 ms    2 ms    2 ms WIN7PRO [192.168.0.40]

トレースを完了しました。

C:\Users\%username>
```