Deployment Guide

IPoE インターフェースを利用した FortiGate SD-WAN 設定ガイド

Version 1.0.0 2021 年 2 月

免責事項

目次

1.はじめに

この設定ガイドは FortiGate を使い、日本ネットワークイネーブラー（JPNE）株式会社や NTT コミュニケーションズ株式会社がそれぞれ提供する“IPoE 方式による固定 IP インターネット接続サービス”で SD-WAN を実現するための基本的な設定方法を 2 つご紹介します。

1．　インターネット・ブレイクアウト（2 章）

　　Office365 など、回線負荷が大きい特定のトラフィックを IPv6 回線にルーティングします。

2．　ハイブリッド WAN（3 章）

　　用途によって PPPoE／IPoE 回線を使い分けます。

これらをお客様の要件に合わせて適用することで、柔軟なネットワーク運用が可能になります。

各社の IPoE サービスに関しては事業者の公式情報をご参照下さい。

JPNE「v6 プラス」固定サービス

　　https://www.jpne.co.jp/service/v6plus-static/

NTT コミュニケーションズ　IPoE サービス

　　https://www.ntt.com/business/services/network/internet-connect/ocn-business/ftth/know.html

FortiGate の IPoE の設定には以下のリンクをご参照下さい。

JPNE「v6 プラス」固定サービス

　　https://www.fortinet.com/content/dam/fortinet/assets/deployment-guides/ja_jp/fg-jpne-v6plus.pdf

NTT コミュニケーションズ　IPoE サービス

　　https://www.fortinet.com/content/dam/fortinet/assets/deployment-guides/ja_jp/fg-ocn-ipoe-fixip.pdf

1-1. 利用機器と OS バージョン

利用機器	バージョン
FortiGate-60F	FortiOS 6.4.4

インターフェース名など機器に依存する箇所に関してはお使いの FortiGate に合わせて設定して下さい。

また、一部 GUI の表示部分に関しては見易さの都合上分割して記載しております。

1-2. 参考資料

本設定ガイドで紹介している設定は公式な設定ガイドに基づいています。より詳細な情報が必要な場合は以下も合わせてご参照ください。

https://docs.fortinet.com/document/fortigate/6.4.4/administration-guide/954635/getting-started

2.インターネット・ブレイクアウト

2-1. 想定トポロジー

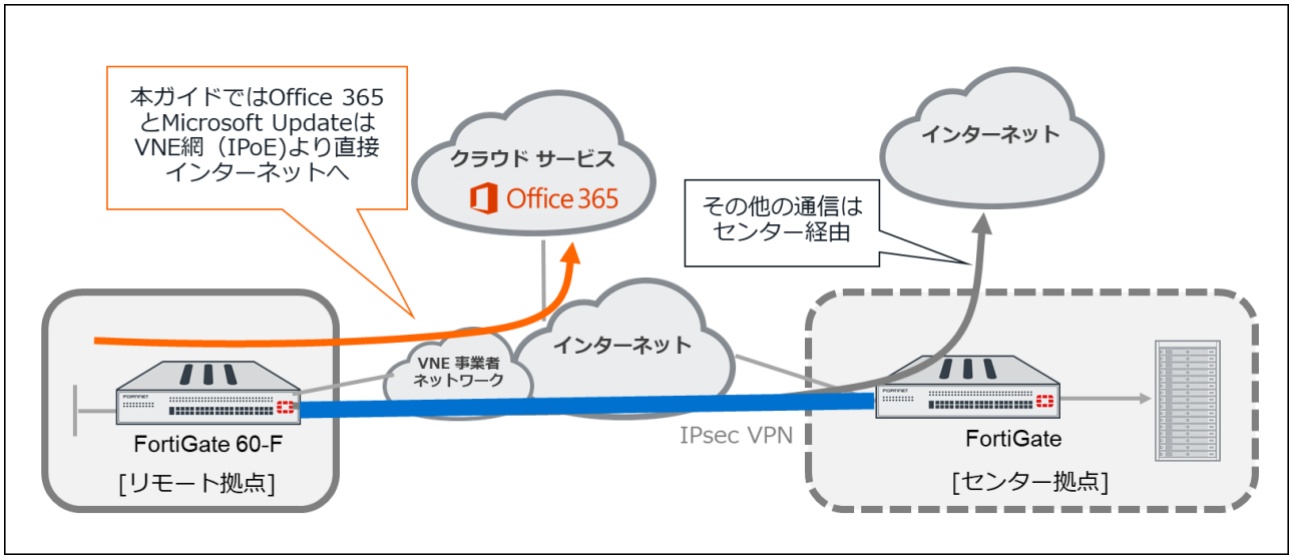

図 2-1. 想定構成図

2-2. 前提条件

- リモート拠点側は【IPoE 回線】を 1 本使用しインターネット接続していること。
- リモート拠点とセンター拠点は【IPsec VPN】で接続されていること。
  （拠点側 IPsec の設定例は APPENDIX #1 も併せてご参照ください）
- FortiGate の基本的な設定および IPoE 接続設定、適切なケーブル結線が完了していること。
- IPoE と IPsec インターフェースにそれぞれデフォルトルートを設定、かつ IPsec インターフェースが優先されるように IPoE 側のインターフェースにプライオリティが設定されていること。

2-3. ブレイクアウト用ポリシーの作成

左メニューの「ポリシー＆オブジェクト」＞「ファイアウォールポリシー」を選択し、【＋新規作成】をクリックします。

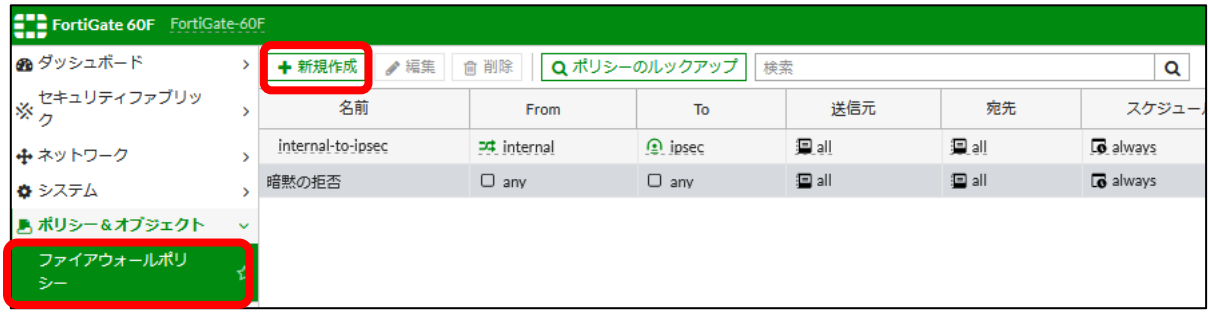

図 2-3-1. ファイアウォールポリシー作成画面

各項目を入力します。

名前：　適当な名前を入力します。（breakout）

発信インターフェース：　vne.root（IPoE）を選択します。

宛先：【+】をクリックし、右側のウィンドウより【インターネットサービス】を選択、ブレイクアウトさせたいアプリケーションを選択します。

トラフィックの確認の為に「ロギングオプション」を以下の通り設定します。

ログ：　有効、【すべてのセッション】を選択します。

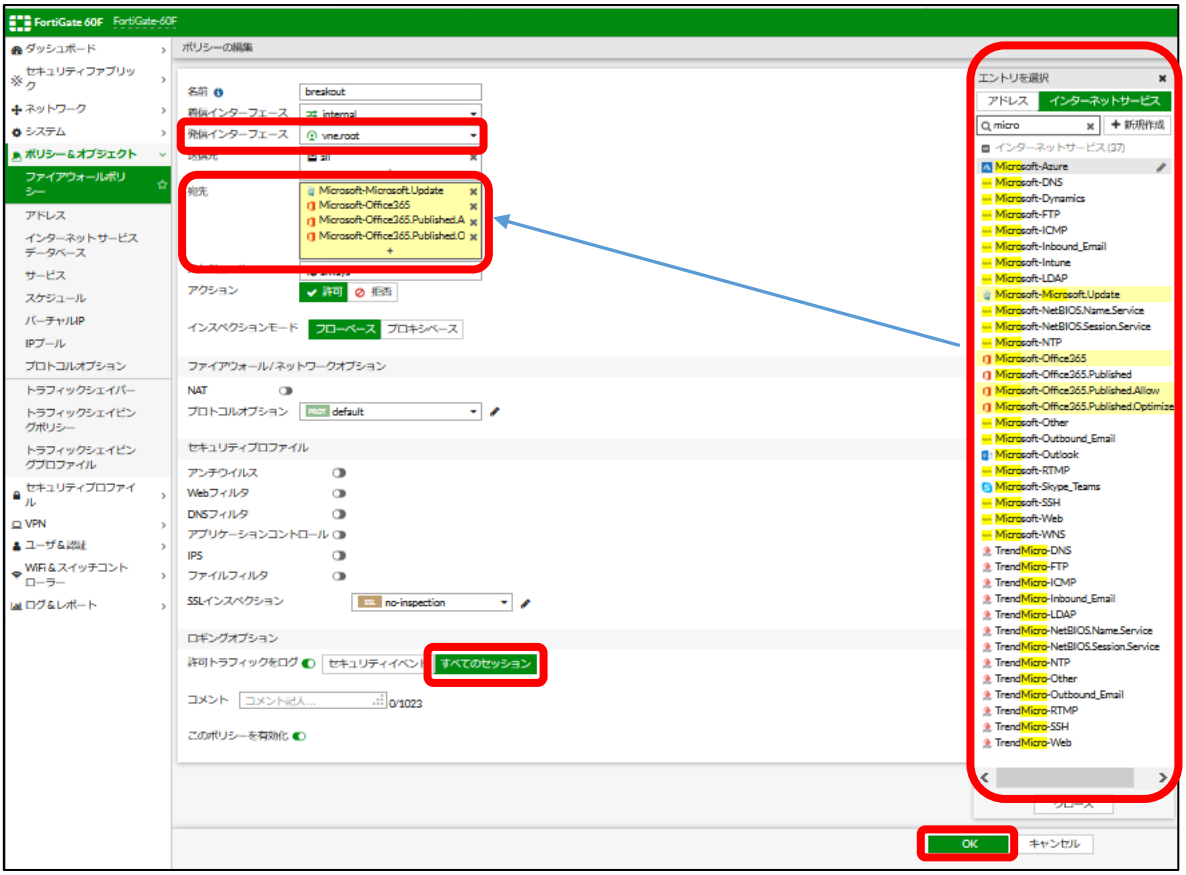

図 2-3-2. ポリシー編集画面

OK をクリックしポリシーを作成します。

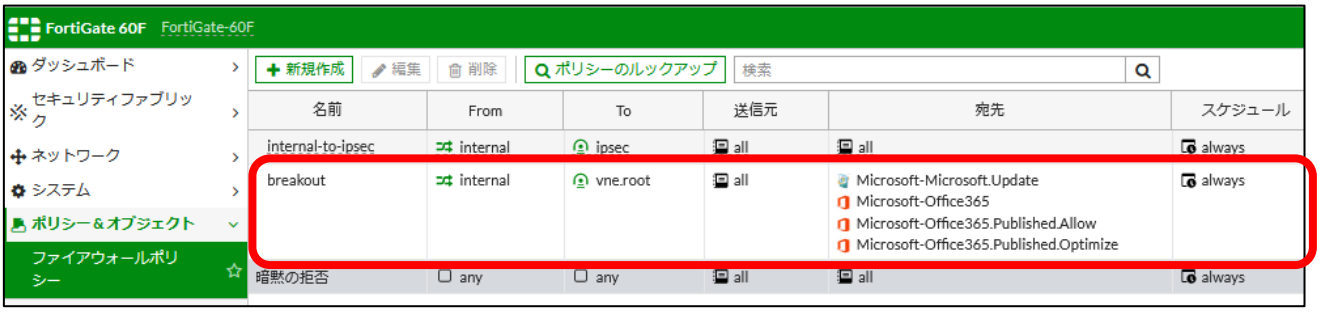

図 2-3-3. 作成済みファイアウォールポリシー（左）

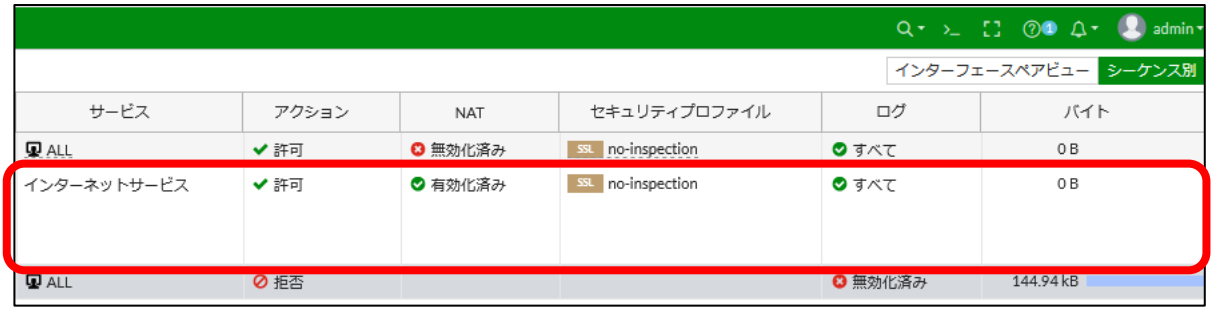

図 2-3-3（続き）. 作成済みファイアウォールポリシー（右）

ポリシー【breakout】を他のポリシーより先に選択させたいので、【breakout】をドラック＆ドロップし上位に移動します。

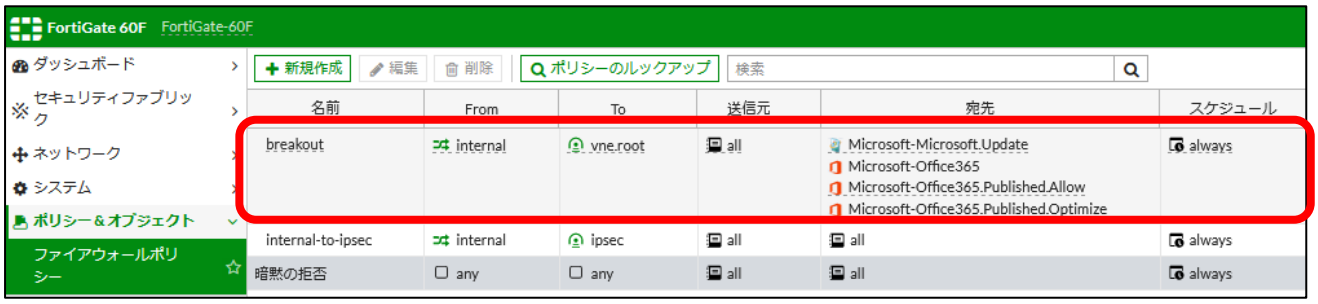

図 2-3-4. 順序を変更したファイアウォールポリシー（左）

図 2-3-4（続き）. 順序を変更したファイアウォールポリシー（右）

本設定により Office 365 と Microsoft update の通信に【breakout】ポリシーが適用されます。

2-4. ブレイクアウト用のルーティングの設定

左メニューの「ネットワーク」 > 「スタティックルート」を選択し、ブレイクアウトさせるアプリケーション毎のスタティックルートを作成します。

インターネットサービス： Microsoft-Microsoft.Update を選択します。

インターフェース： vne.root を選択します。

図 2-4-1. スタティックルート設定画面

【Microsoft-Office365】、【Microsoft-Office365-Allow】、【Microsoft-Office365-Optimize】についても同様にスタティックルートを設定します。

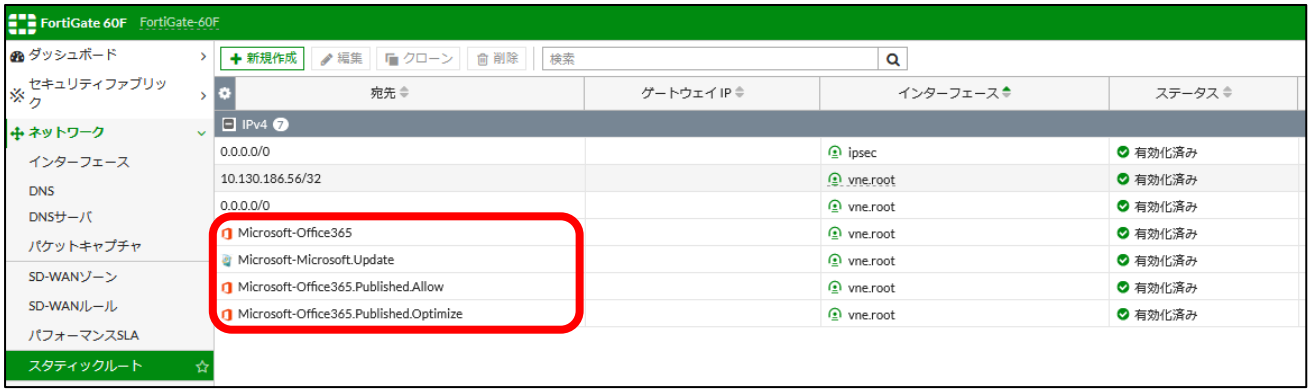

図 2-4-2. スタティックルート表示画面

※本ガイドでは vne.root と ipsec インターフェースにデフォルトルートを設定していますが、お客様の実際の環境に合わせて設定して下さい。

2.5. スタティックルートのプライオリティ変更

IPsec インターフェースが優先されるように IPoE インターフェースのプライオリティを変更します。

左メニューの「ネットワーク」 > 「スタティックルート」 にて vne-root インターフェースのデフォルトルート（0.0.0.0/0 vne.root）を選択し、“編集“をクリックします。

図 2-5-1. スタティックルートのプライオリティ変更

「高度な設定」をクリックし、プライオリティ値を変更します。

プライオリティ値に【１】を入力します。なお、デフォルト値は【０】で、プライオリティ値が小さいルートが優先されます。

【OK】をクリックして設定を完了します。

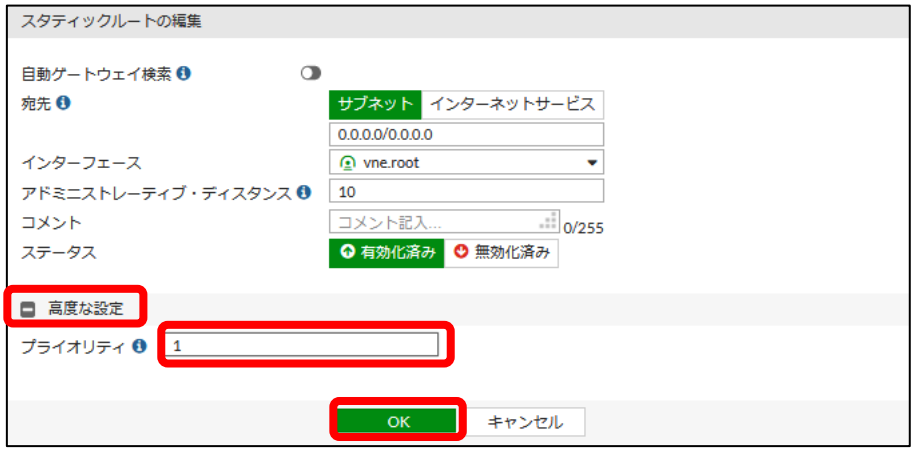

図 2-5-2. スタティックルートのプライオリティ編集

2-6. 確認方法

左メニューの「ログ＆レポート」 ＞ 「転送トラフィック」でブレイクアウトの動作を確認できます。
Office 365 関連トラフィックについてポリシーID が【breakout】、 宛先インターフェースが【vne.root】となっていれば正常に動作しています。

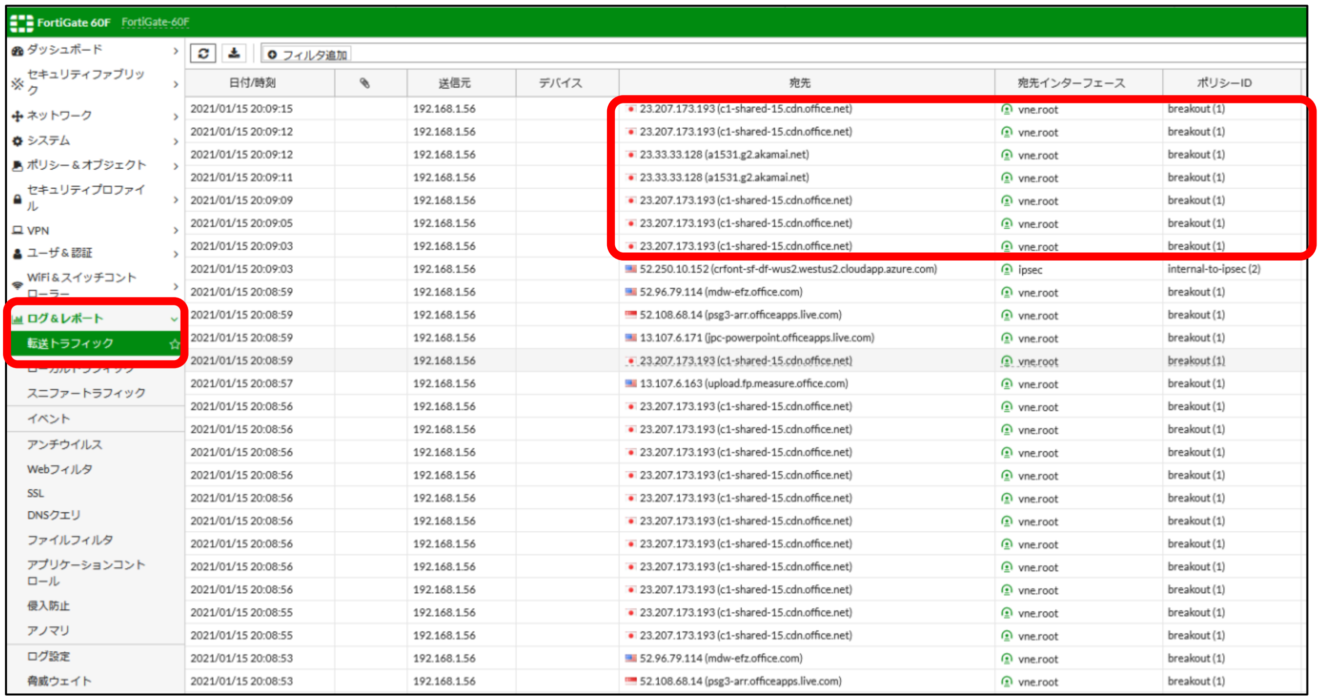

図 2-6. 転送トラフィックログ確認画面

3. SD-WAN ハイブリッド WAN

3-1. 想定トポロジー

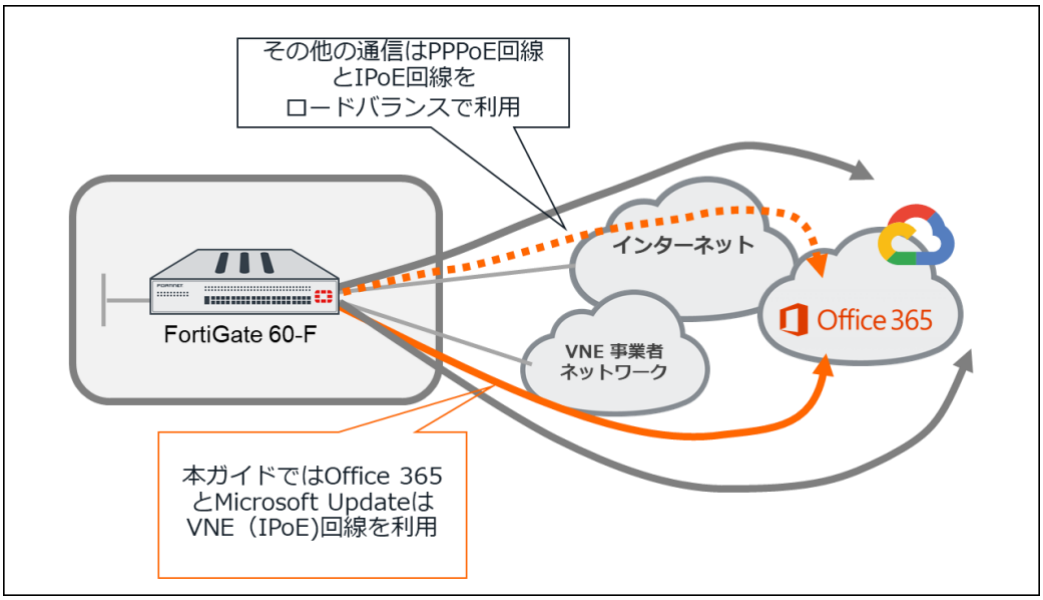

図 3-1. PPPoE、IPoE によるロードバランス構成

3-2. 前提条件

- 設定機器は FortiGate-60F を使用し【IPoE 回線】と【PPPoE 回線】の 2 回線を収容しインターネットに接続されていること。
- FortiGate の基本的な設定、IPoE、PPPoE 接続設定、適切なケーブル結線が完了していること。
- Microsoft Update、Office 365 関連のトラフィックは主に IPoE 回線を利用し、その他のトラフィックは IPoE、PPPoE の両方の回線を利用される設定がされていること。
- PPPoE のインターフェース名は pppoe としています。

3-3. 参考資料

SD-WAN quick start

https://docs.fortinet.com/document/fortigate/6.4.4/administration-guide/889544/sd-wan-quick-start

Config system pppoe-interface

https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/98620/system-pppoe-interface

3-4. SD-WAN インターフェースの作成

左メニューより「ネットワーク」 > 「SD-WAN ゾーン」を選択し、【virtual-wan-link】をクリックします。

図 3-4-1. SD-WAN ゾーン設定画面

【新規作成】をクリックし、SD-WAN メンバーを選択します。

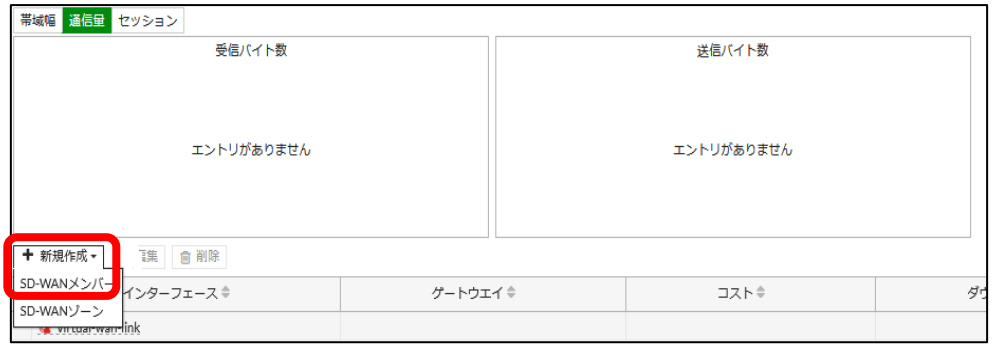

図 3-4-2. SD-WAN メンバー設定画面

SD-WAN メンバーの編集にて、インターフェースで【vne-root】を選択し【OK】をクリックします。

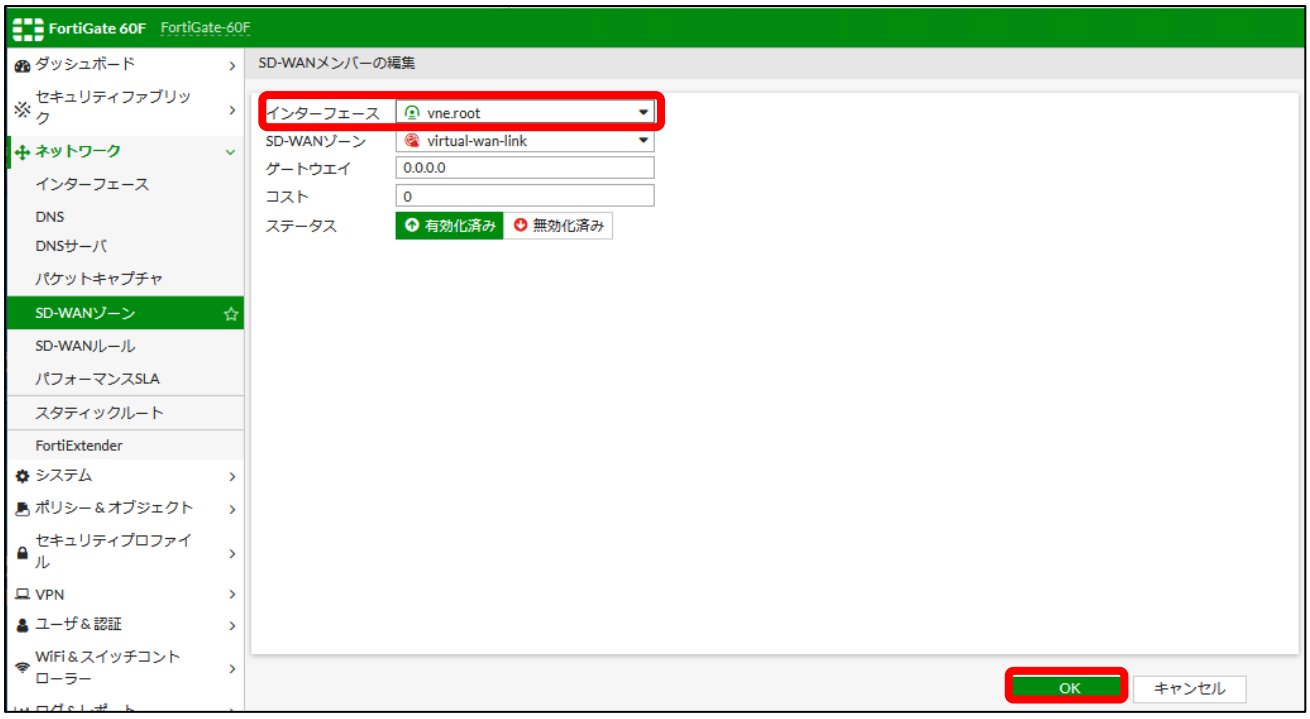

図 3-4-3. SD-WAN メンバー編集画面

同様にメンバーの新規作成を行い、PPPoE インターフェース(pppoe)をメンバーに追加します。
作成されると virtual-wan-link(SD-WAN)インターフェースに vne.root と pppoe のインターフェースが SD-WAN インターフェースのメンバーとして以下のように表示されます。

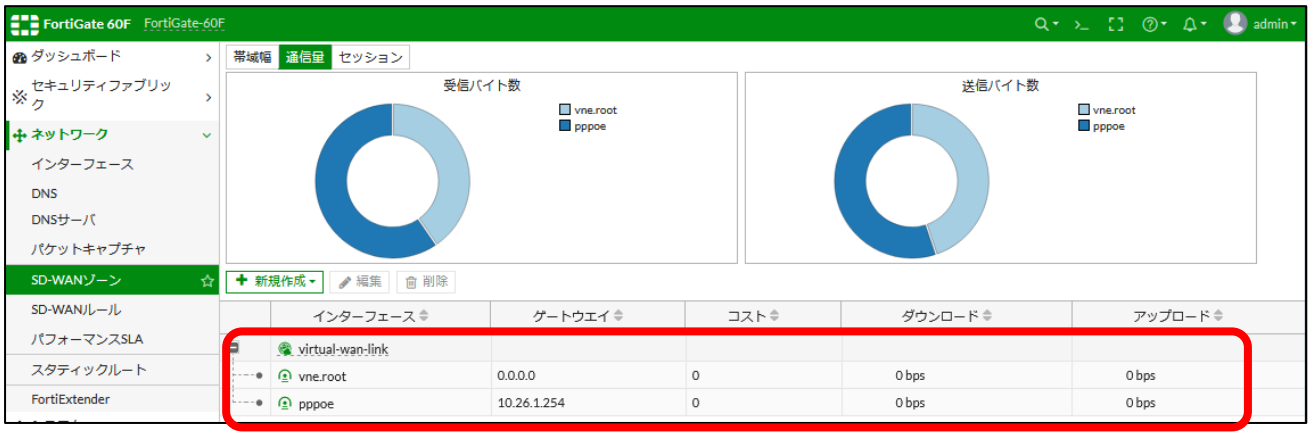

図 3-4-4. SD-WAN ゾーン確認画面

3-5. 特定アプリケーションの優先インターフェース作成

ISDB で特定されるアプリケーショントラフィックが優先的に使用するインターフェースを作成します。本ガイドでは Office 365 と Microsoft update のトラフィックを優先するインターフェースとして vne-root インターフェースを使用します。
左メニューの「ネットワーク」 > 「SD-WAN ルール」 を選択し、 【+新規作成】 をクリックします。

図 3-5-1. SD-WAN ルール新規作成画面

名前：　任意の名前（o365）

送信元アドレス：　【all】を選択します。（本ガイドではすべてのユーザを対象とします）

インターネットサービス：　【Microsoft-Microsoft_Update】、【Microsoft-Office365】、【Microsoft-Office365-Allow】、【Microsoft-Office365-Optimize】を選択します。

発信インターフェース：　【マニュアル】を選択します。

優先するインターフェース：　【vne-root】を選択します。

【OK】をクリックし、SD-WAN ルールを作成します。

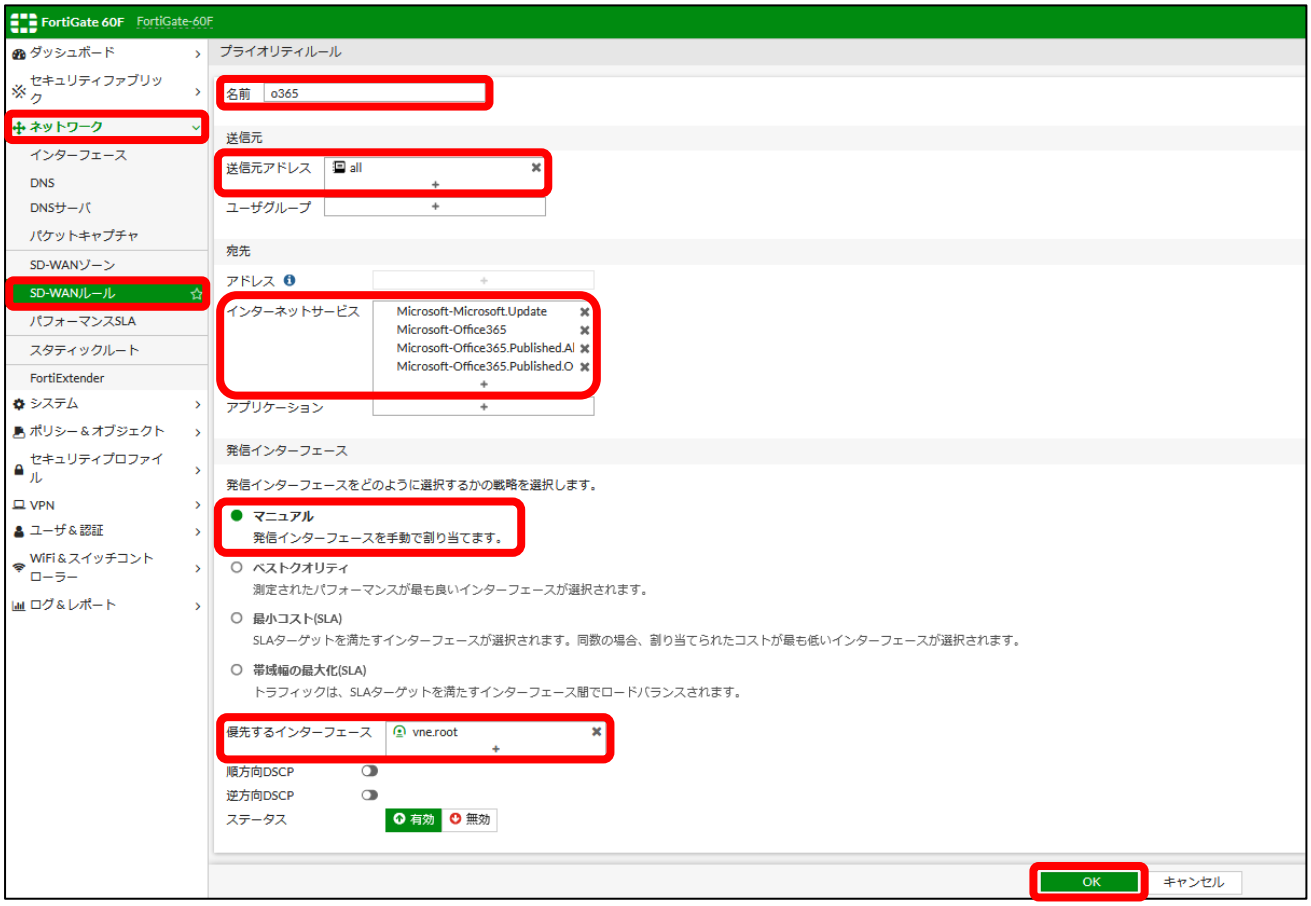

図 3-5-2. プライオリティルール設定画面

上記で作成したルールに該当しないトラフィックは暗黙のルールが適用されます。

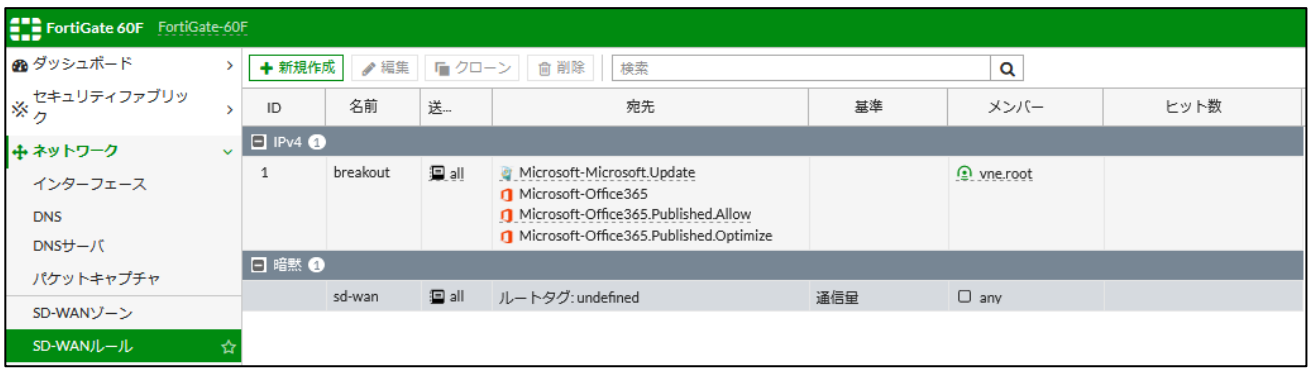

図 3-5-3. SD-WAN ルール画面

3-6. デフォルトルートの作成

デフォルトルートを SD-WAN インターフェースとするスタティックルートを作成します。

左メニューのネットワーク ＞ スタティックルートを選択し、【+新規作成”】をクリックします。

図 3-6-1. スタティックルート作成画面

インターフェースで【SD-WAN】を選択し、【OK】をクリックします。

図 3-6-2. 新規スタティックルート設定画面

3-7. ポリシーの作成

左メニューの「ポリシー＆オブジェクト」 ＞ 「ファイアウォールポリシー」を選択し、【＋新規作成】 をクリックします。

図 3-7-1. 新規ポリシー作成画面

名前： 任意の名前を入力します。（internal to sd-wan）

着信インターフェース： 【internal】を選択します。

発信インターフェース： 【virtual-wan-link】を選択します。

送信元： 【all】を選択します。

宛先： 【all】を選択します。

サービス： 【ALL】を選択します。

トラフィックの確認の為にロギングオプションを以下の通り設定します。

ログ： 有効、【すべてのセッション】を選択します。

【OK】をクリックして設定を完了します。

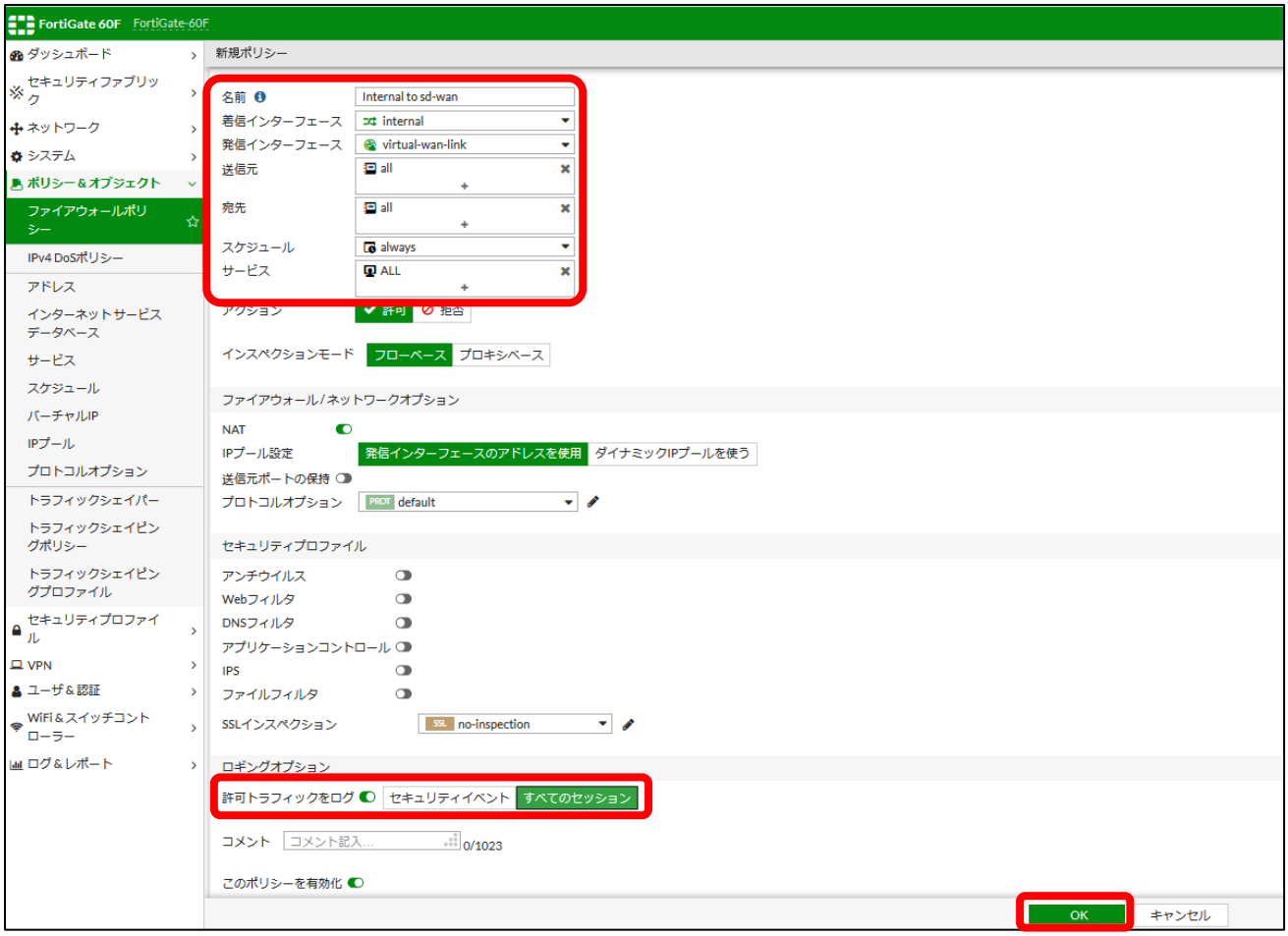

図 3-7-2. 新規ポリシー設定画面

※本ガイドではすべてのトラフィックが【SD-WAN】インターフェースを利用する様に設定していま す。必要に応じて送信元や宛先、セキュリィティプロファイル等を適切に設定して下さい。

ポリシーが作成されると以下の様に表示されます。

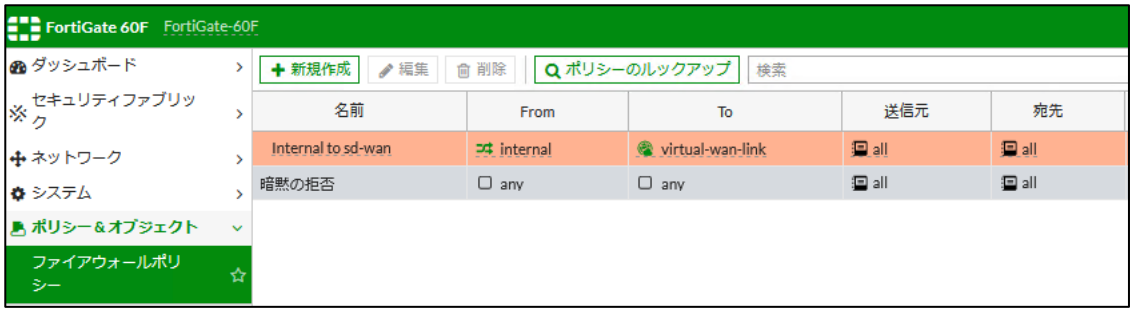

図 3-7-3. ファイアウォールポリシー画面（左）

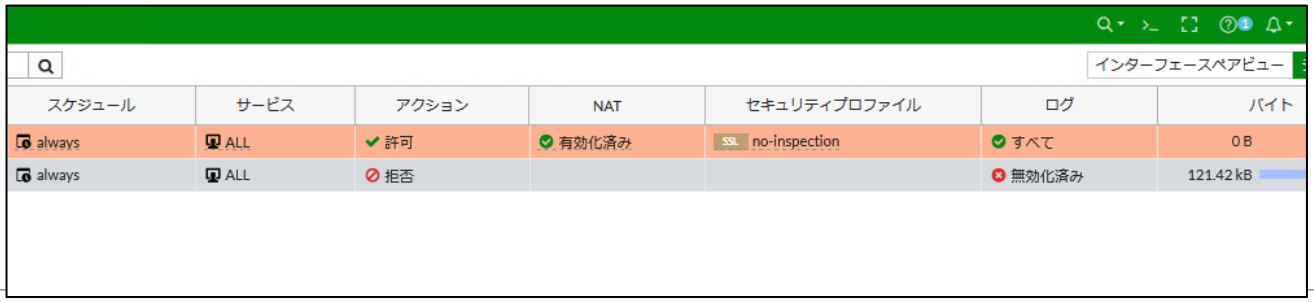

図 3-7-3（続き）．ファイアウォールポリシー画面（右）

3-8. mss 値の変更

IPv6 ヘッダ追加に伴い vne.root を経由するセッションの TCP の MSS（最大セグメントサイズ）の値を変更する必要があります。

ファイアウォールポリシーで TCP MSS 値の設定ができます。

GUI 画面右上部の“>_“より CLI コンソールを開きます。

図 3-8-1. CLI コンソール呼び出しアイコン

CLI コンソールより以下を設定します。

```
config firewall policy
   edit 1
      set tcp-mss-sender 1420
      set tcp-mss-receiver 1420
end
```

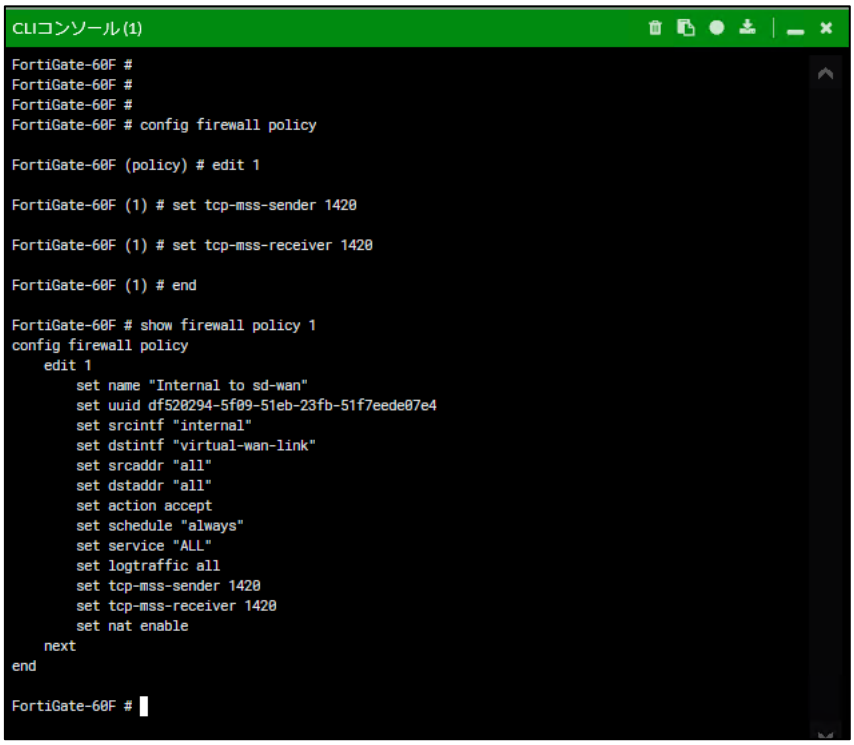

図 3-8-2. CLI コンソール画面

3-9. 確認方法

端末より、対象となるトラフィック（Office 365 やその他トラフィック）を送信します。

左メニューの「ネットワーク」 > 「SD-WAN ゾーン」を選択し、各 SD-WAN メンバーインターフェースのダウンロードやアップロードのトラフィック量がカウントされている事を確認します。

図 3-9-1. SD-WAN ゾーン セッション表示

左メニューの「ログ＆レポート」 > 「転送トラフィック」を選択し、以下を確認します。

Office 365 トラフィックは vne-root から優先して送信されていること。

その他のトラフィックは vne-root と pppoe のインターフェースから送信されていること。

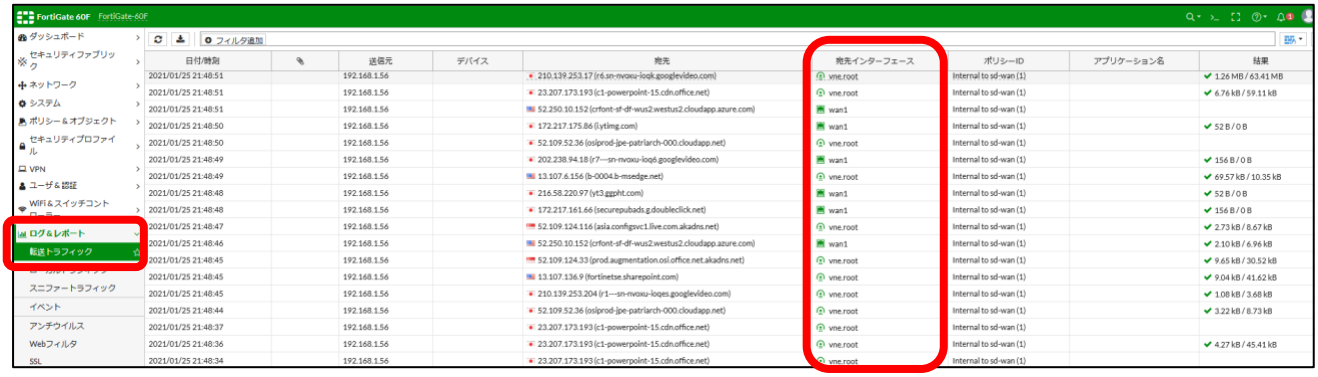

図 3-9-2. 転送トラフィックログ確認画面

APPENDIX　＃１

本ガイドの第２章「インターネット・ブレイクアウト設定」を行う際のリモート/センター拠点における IPsec 設定を説明します。

1. 想定トポロジー

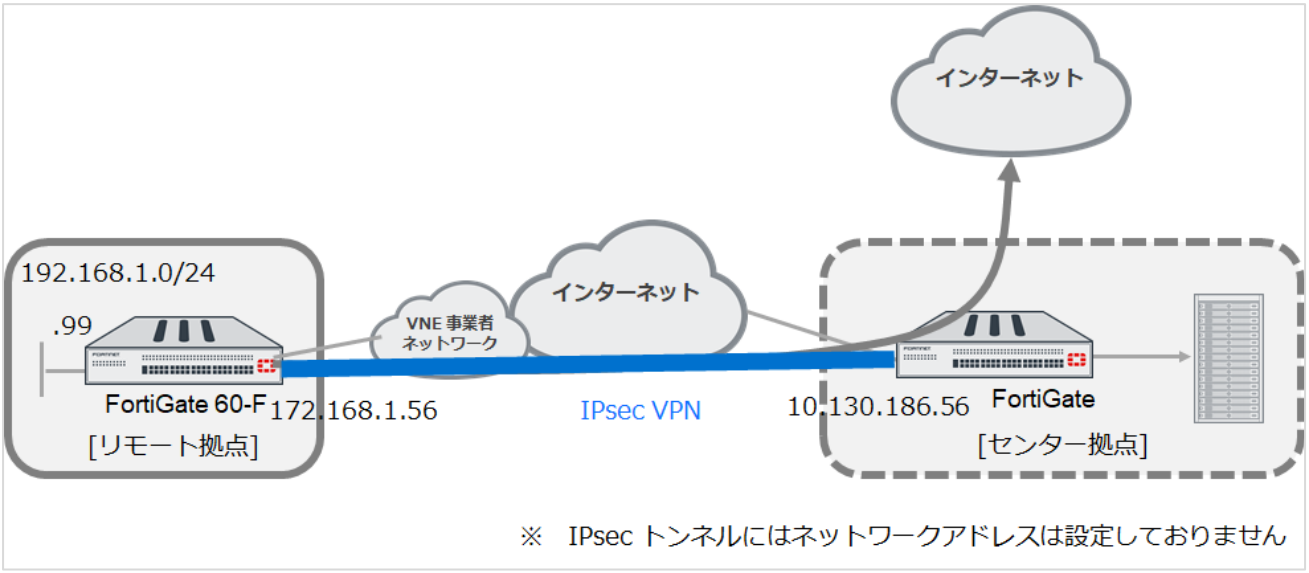

図. IPsec VPN 構成

2. 参考資料

- Basic site-to-site VPN
  https://docs.fortinet.com/document/fortigate/6.4.4/administration-guide/202791/site-to-site-vpn

- VPN IPsec troubleshooting
  https://docs.fortinet.com/document/fortigate/6.4.4/administration-guide/137844/vpn-ipsec-troubleshooting

3. 前提条件

- IPsec トンネルにはネットワークアドレスは設定しない。
- 鍵交換はアグレッシブモードで設定しています。
- 認証方式は事前共有鍵で設定しています。
- VPN ウィザードのカスタムを利用した設定である。
- 特に明示していない設定はデフォルト設定を適用。

4. IPsec VPN の設定

左メニューの「VPN」 > 「IPsec ウィザード」 を選択し、VPN 作成ウィザードを実行します。

名前： 任意の名前を入力します。（ipsec）

テンプレートタイプ： 【カスタム】を選択し、【次へ】をクリックします。

なお、カスタムを選択するとウィザードは終了し、詳細設定する画面に遷移します。

センター側、リモート側でそれぞれ設定が必要です。

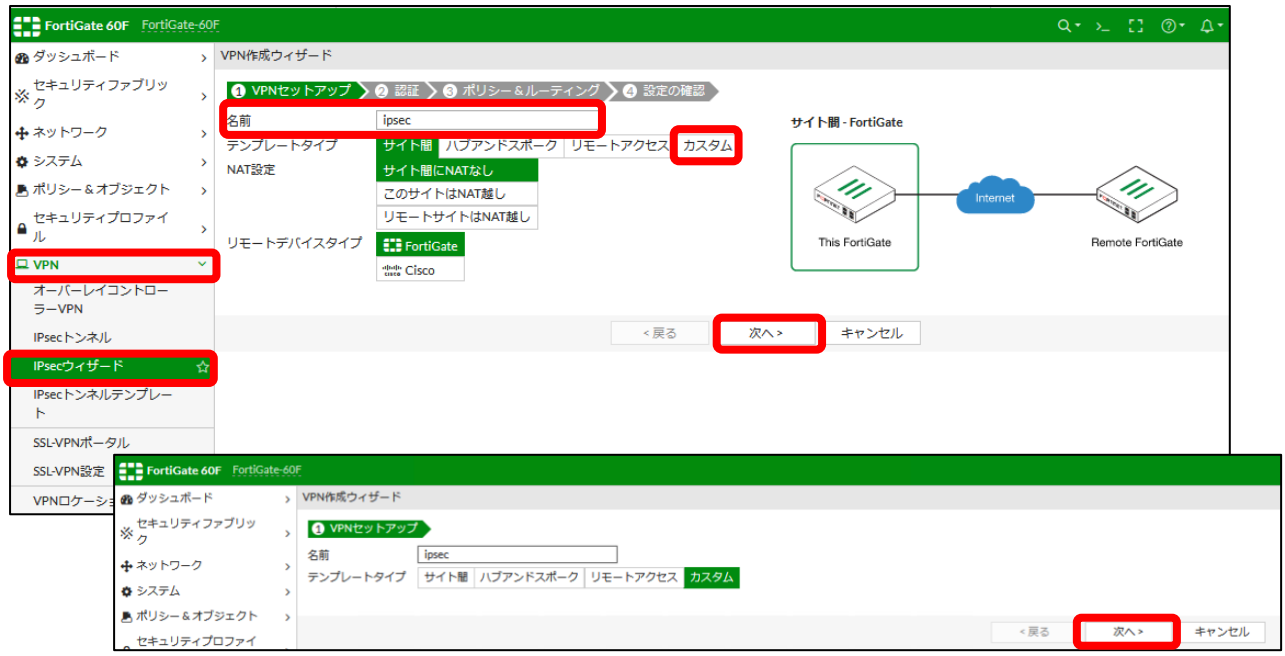

図 4-1. VPN 作成ウィザード画面

IP アドレス：

リモート拠点：センター拠点の WAN IP アドレスを設定（10.130.186.56）

センター拠点：リモート拠点の vne.root の IP アドレスを設定

インターフェース：

リモート拠点：【vne.root】

センター拠点：【WAN1】

をそれぞれ選択

認証：

方式：【事前共有鍵】

事前共有鍵：任意の文字列

IKE：

モード：アグレッシブ

受け入れるタイプ：【任意のピア ID】

フェーズ 2 セレクタ：

ローカルアドレスに 192.168.1.0/255.255.255.0 を入力

図 4-2. 新規 VPN トンネル設定画面

IPsec ルーティング設定

左メニューの「ネットワーク」 ＞ 「スタティックルート」を選択し、IPsec トンネルをデフォルトルート（宛先 0.0.0.0/0.0.0.0）に設定し【OK】をクリックして設定を完了します。

図 4-3. リモート拠点のデフォルトルート設定

同様に、センター拠点の FortiGate 宛（宛先 10.130.186.56/255.255.255.255）の通信は vne.root 経由になるスタティックルートを設定します。

（センター拠点の FortiGate にも同様に、宛先に vne.root の IP アドレスを設定、インターフェースに【WAN1】を設定します）

図 4-4. リモート拠点のスタティックルート設定

設定後は以下の様になります。

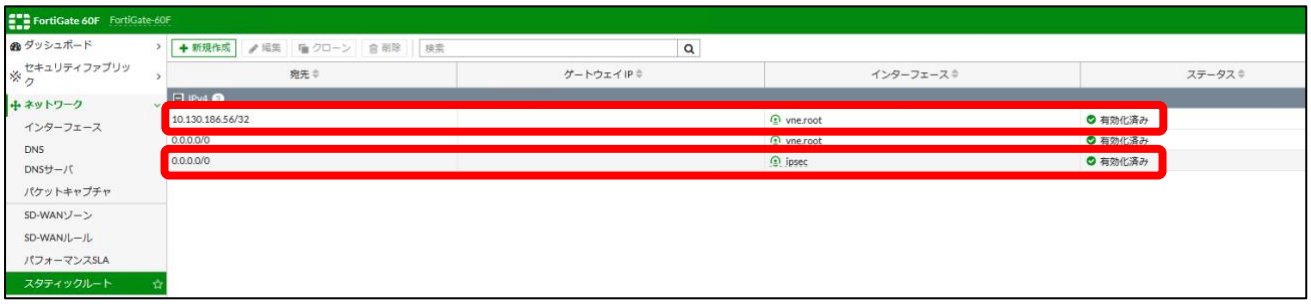

図 4-5. リモート拠点のルーティング設定

5. IPsec ポリシー設定

IPsec ポリシーの作成

左メニューの「ポリシー＆オブジェクト」 ＞ 「ファイアウォールポリシー」を選択し、【+新規作成】をクリックし IPsec ポリシーを作成します。

図 5-1. IPsec ポリシー作成画面

IPsec ポリシーの編集

名前： 任意の名前を入力します。（internal-to-ipsec）

着信インターフェース： 【internal】を選択します。

発信インターフェース： 【ipsec】を選択します。

NAT： 【無効】に設定します。

【OK】をクリックして設定を完了します。

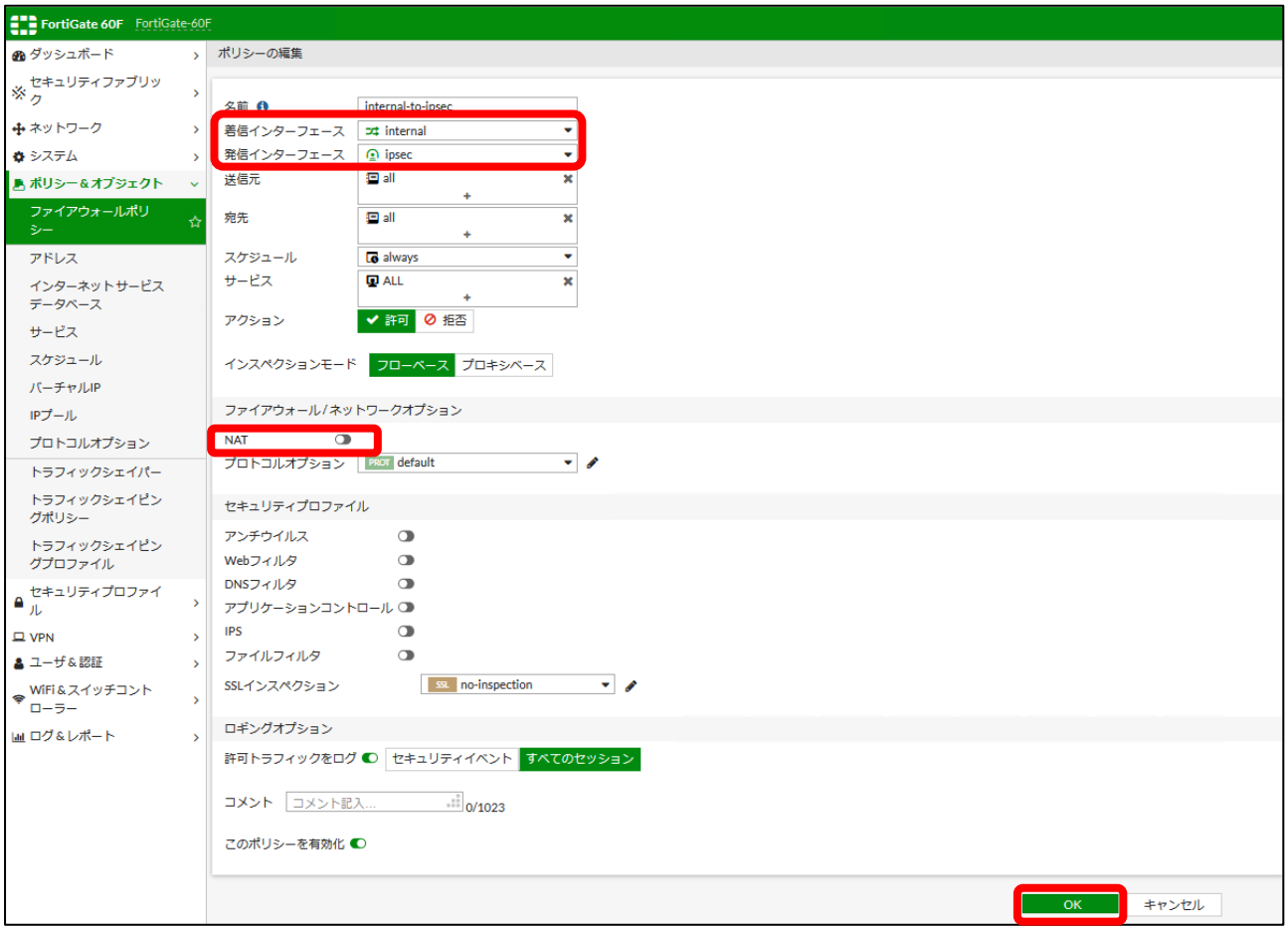

図 5-2. IPsec ポリシー編集画面

6. 確認方法

リモート側/センター側の設定が終了した後、リモート側の LAN 内の端末からセンター側を経由する通信を発生させる事で IPsec のステータスがアップする事を確認して下さい。

FortiGate のダッシュボードで IPsec の状態を確認できます。

左メニューの「ダッシュボード」 > 【+】を選択し、モニタの追加画面で【IPsec】をクリックし、【モニタの追加】をクリックします。

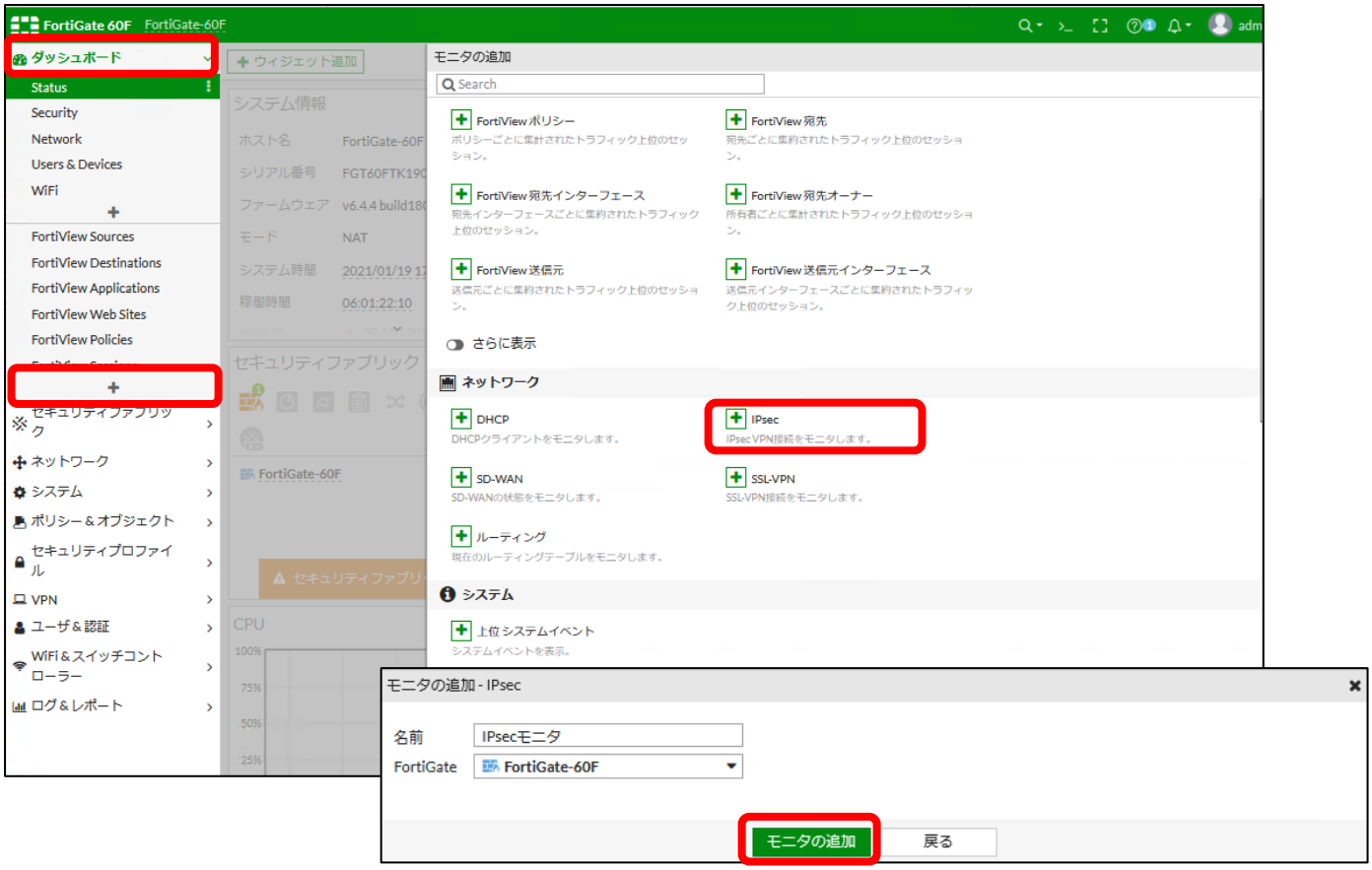

図 6-1. ダッシュボード追加画面

ダッシュボードに新しく追加された【IPsec モニタ】をクリックすると IPsec インターフェースの状況を確認する事ができます。

図 6-2. IPsec モニタ画面

改定履歴

バージョン	リリース日	改定履歴
1.00	2021.2	初版発行