SuitePRO V4 / IndigoPro UTM オプション
FortiGate 設定手順書

株式会社 NTTPC コミュニケーションズ
更新日：2024 年 11 月 06 日

目次

1. はじめに

本手順書では FortiGate バージョン 7.4 の基本的な設定方法について解説します。
本手順で使用している IP アドレスは、RFC で定義されている例示用の IP アドレスとなりますので、設定の際はお客さまの環境に応じて指定してください。

2. UTM 管理サイトへのログイン

コントロールパネル SuitePRO V4（https://pro4.arena.ne.jp）または IndigoPro（https://compas.arena.ne.jp）にログインし、「セキュリティ」>「UTM/NIC4」>「基本情報」を開き、UTM 情報内の「UTM 管理サイト」の URL をクリックします。

UTM 管理サイトのログイン画面が表示されますので、ユーザ名、パスワードを入力し、ログインをクリックします。
※初期状態では、証明書がインポートされていないため、証明書エラーの画面が表示されます。
必要に応じて、お客さまにてドメインとそのドメインの証明書を取得してください。

※ログインできない場合
コントロールパネルの UTM 管理サイトへのアクセス許可から、アクセス元の IP アドレスが許可されているか確認してください。
SuitePRO V4（https://pro4.arena.ne.jp）
IndigoPro（https://compas.arena.ne.jp）

SuitePRO V4「UTM 管理サイトへのアクセス制限」
https://help.arena.ne.jp/hc/ja/articles/360039329673#chapter2

IndigoPro「UTM 管理サイトへのアクセス制限」
https://help.arena.ne.jp/hc/ja/articles/4408148218775#chapter2

UTM 管理サイト用のドメインを準備する場合、以下の作業を実施
① ドメイン取得（FortiGate で使用するため、サーバーとは別に準備する）
② DNS 登録
A レコードで FG 管理サイトの IP アドレスを指定（例：fvd1111.fg.arena.ne.jp）
③ 取得したドメインの証明書購入
④ FortiGate：証明書インポート ※手順「証明書のインポート」参照
⑤ FortiGate：証明書設定
「システム」>「設定」メニュー
「管理者設定」>「HTTPS サーバー証明書」にて対象の証明書を選択し、適用

3. UTM 管理サイトの管理

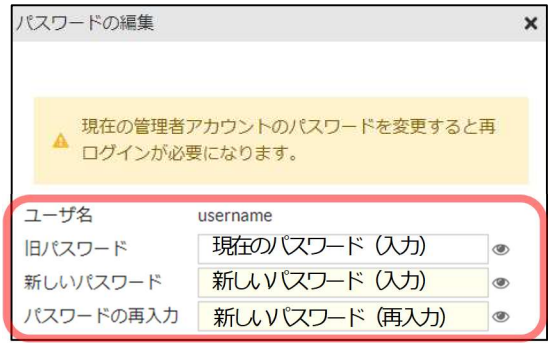
UTM 管理サイト

3-1　UTM 管理サイト のパスワード変更

(1)　ログイン後、UTM 管理サイト右上のユーザ名をクリックします。

「パスワードの変更」をクリックします。

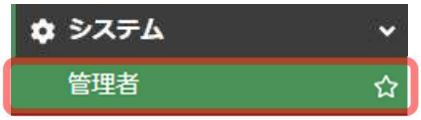
(2)　現在のパスワード、新しいパスワードを 2 回入力し、「OK」をクリックします。



3-2　UTM 管理サイト 接続元 IP アドレスの追加

接続元アドレスの追加を行う方法です。管理サイトにログインしたうえでの作業となります。現在のアドレスが追加されていない場合は、アクセスができませんので「18.コンソール」をご確認ください

(1)　システム＞管理者を選択します。



(2)　対象の管理者をクリックします。

admin とは‥弊社管理のサポート用アカウントになります。削除や変更はお控えいただくようお願い致します。削除・変更されますと、お問い合わせの際にお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。

(3)　信頼されるホストにログインを制限の欄に IP アドレスを追加し、「OK」をクリックします。

4. ファイアウォールポリシー

4-1　ファイアウォールポリシー

ファイアウォールポリシーは、FortiGate ユニットを通過するトラフィックを、FortiGate インタフェース間で制御します。

- Incoming（外部から仮想サーバー）の通信
- Outgoing（仮想サーバーから外部）の通信

トラフィックは、ファイアウォールポリシーリストの最上位にあるものから下位の項目へと順番に評価されます。
一致するポリシーが検出されると、そのポリシーで指定された処理が行われ、以降のファイアウォールポリシーは適用されません。
許可ポリシーに一致しなかったトラフィックは拒否されます。（暗黙の拒否）

4-2　　ファイアウォールポリシーの表示

「ポリシー＆オブジェクト」>「ファイアウォールポリシー」をクリックすると、ファイアウォールポリシーが表示されます。

4-3　プリセットされているファイアウォールポリシー

初期のファイアウォールポリシーは下記のように設定しています。

Incoming（外部から仮想サーバー）の通信

① NTTPC：ポート監視サーバーの通信を許可（ポート監視サービスを利用するために必要）

② Preset2～7：サンプルとなるプリセットのファイアウォールポリシー（ステータス：無効）

preset2：オフィス等から SSH（TCP/22）接続を許可する際に使用

preset3：オフィス等からリモートデスクトップ（TCP/3389）接続を許可する際に使用

preset4：DNS（TCP,UDP/53）サーバーを構築した際に使用

preset5：HTTP（TCP/80）サーバーを構築した際に使用

preset6：HTTPS（TCP/443）サーバーを構築した際に使用

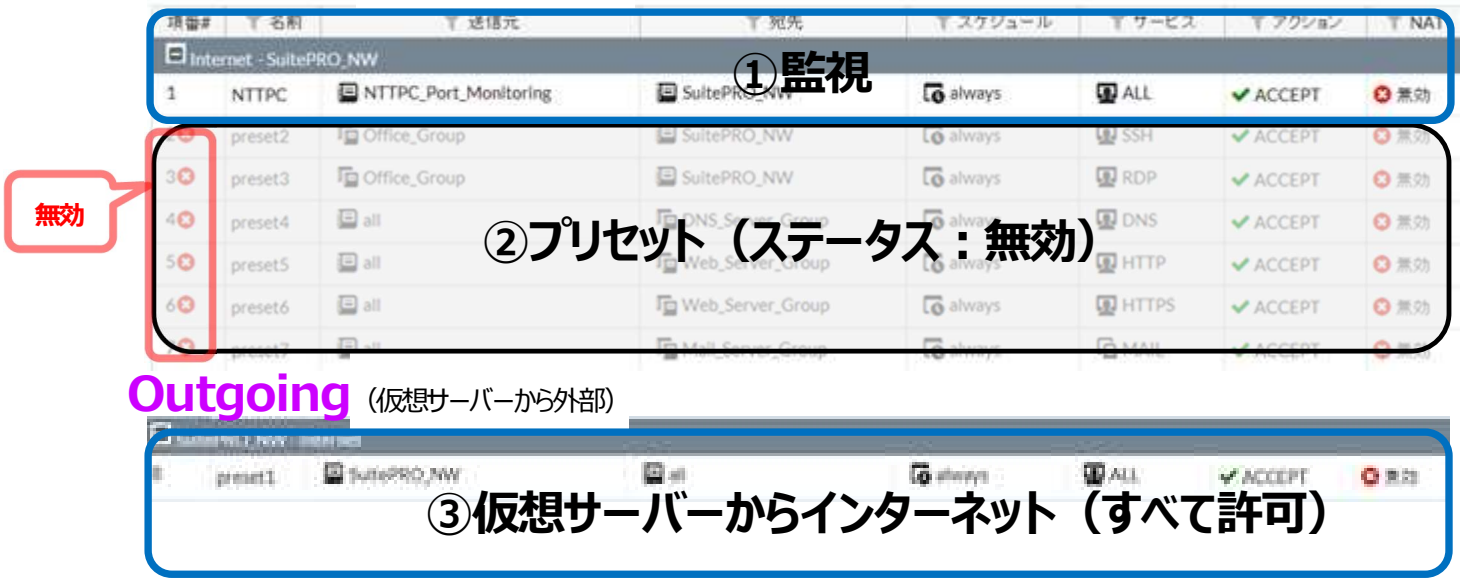
preset7：メールサーバー（※）を構築した際に使用

※POP3（TCP/110），SMTP（TCP/25），SMTP_SUBMISSION（TCP/587），IMAP（TCP/143）

Outgoing（仮想サーバーから外部）の通信

③ preset1：仮想サーバーから外部への通信はすべて許可

Incoming（外部から仮想サーバー）



Outgoing（仮想サーバーから外部）

5. ファイアウォールアドレス

5-1 ファイアウォールアドレス

ファイアウォールポリシーに使用するアドレスです。
初期で登録されているファイアウォールアドレスの一部を紹介します。

NTTPC_Port_Monitoring：NTTPC ポート監視サーバーで使用しているため変更しないでください。
OfficeA：仮想サーバーにアクセスする拠点のアドレスを登録（※）
OfficeB：仮想サーバーにアクセスする上記とは別の拠点があれば登録（※）

※初期で指定している IP アドレスは、RFC で定義されている例示用の IP アドレス（192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24）となりますので、設定の際はお客さまの環境に応じて指定してください。

5-2 ファイアウォールアドレスの変更

ここでは例として、プリセットされているファイアウォールポリシーを使用し、オフィス等、仮想サーバーにアクセスする拠点からのみ SSH（TCP/22）接続を許可します。

本設定の他に、仮想サーバー側での設定も必要となります。詳細はこちらをご確認ください。

- SuitePROV4
  https://help.arena.ne.jp/hc/ja/articles/360039329633
- IndigoPro
  https://help.arena.ne.jp/hc/ja/articles/4408133780375

(1) ファイアウォールアドレス設定画面表示

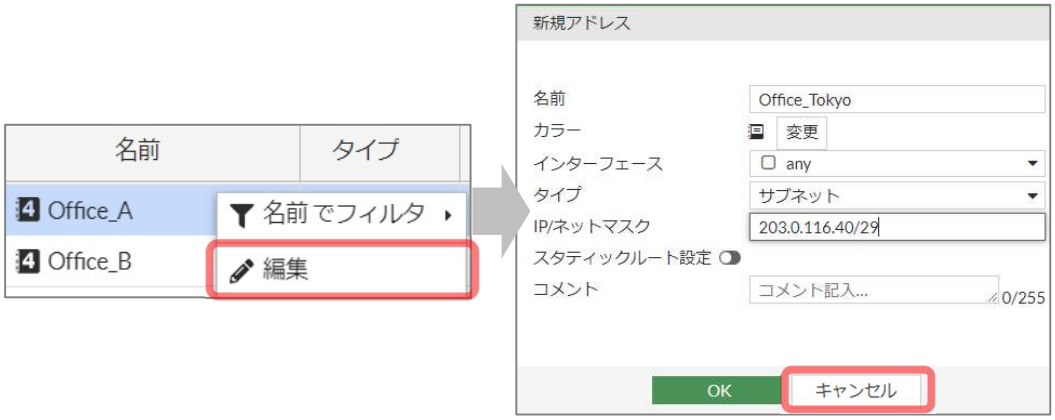
「ポリシー＆オブジェクト」>「アドレス」をクリックします

(2)　プリセットのアドレス変更

プリセットのアドレス「Office_A」を右クリックし「編集」を選択し、名前とアドレスを変更します。

（例）名前：「Office_A」から「Office_Tokyo」と変更 ※お客さまのオフィス拠点名等分かりやすい名前を指定してください。

アドレス：203.0.113.40/29 と変更



内容を確認し、「OK」をクリックします。

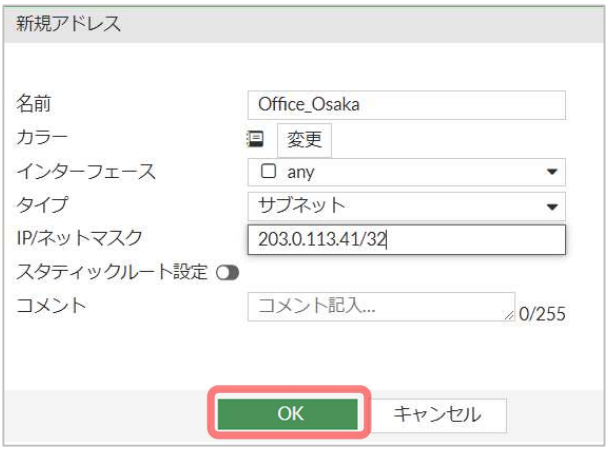
5-3　ファイアウォールアドレスの登録

IP アドレスを新しく登録する場合は「アドレス」を新規作成します。「新規作成」をクリックし、「アドレス」を選択します。

（例）

名前：「Office_Osaka」と入力 ※お客さまのオフィス拠点名等分かりやすい名前を指定してください。

アドレス：203.0.113.41/32 と入力



内容を確認し、「OK」をクリックします。

6. ファイアウォールアドレスグループ

6-1 ファイアウォールアドレスグループ

ファイアウォールポリシーに使用するアドレスグループです。ファイアウォールアドレスをグループでまとめることができます。
初期で登録しているファイアウォールアドレスグループを使用して変更してみます。

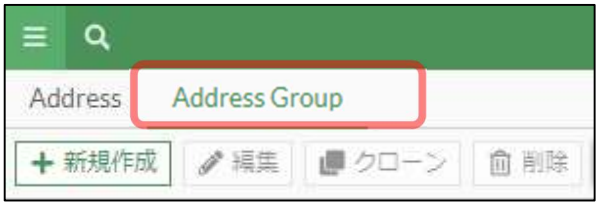
例 Office_Group：Office_A, Office_B

6-2 ファイアウォールアドレスグループの変更

登録した「アドレス」を「ファイアウォールアドレスグループ」でグループ化します。
ここでは例として、プリセットのアドレスグループ「Office_Group」の編集を行います。

(1) アドレスグループ編集

「ポリシー＆オブジェクト」>「アドレス」の上部メニューの「Address Group」を選択します。



「Office_Group」を右クリックし、「編集」をクリックします。

(2) アドレスグループから除外

「メンバ」をクリックすると画面右側にアドレス一覧が表示されます。
「Office_A」のみ使用する場合は、メンバの「Office_B」の右横の×をクリックして削除します。
「OK」をクリックします。

(3)　アドレスグループに追加

新たなアドレスをグループに追加する場合は、「＋」をクリックし、右側のエントリから対象アドレスを選択します。
色が反転し、メンバにが加わったことを確認し、OK をクリックします。

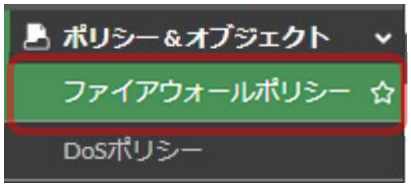
7. ファイアウォールポリシーの有効化・無効化

7-1　ファイアウォールポリシーの有効化

ファイアウォールポリシーを使用するには、ポリシーを有効化する必要があります。
ここでは例として、preset2：オフィス等から SSH（TCP/22）接続を許可するポリシーを有効化し、サーバーへの SSH 通信を許可します。

(1)　IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「ファイアウォールポリシー」をクリックします。



(2)　プリセットのポリシーの確認

プリセットされている「preset 2」を確認します。

送信元：「Office_Group」（お客さまのオフィス）
送信先：「SuitePRO_NW」（お客さまの仮想サーバーが属しているネットワークアドレス）
サービス：「SSH」
アクション：「ACCEPT」

ID	名前	送信元	宛先	スケジュール	サービス	アクション	NAT
Internet (port8) - SuitePRO_NW1812 (port1) (1 - 7)							
1	NTTPC	NTTPC_Port_Monitoring	SuitePRO_NW	always	ALL	ACCEPT	無効
2	preset2	Office_Group	SuitePRO_NW	always	SSH	ACCEPT	無効
3	preset3	Office_Group	SuitePRO_NW	always	RDP	ACCEPT	無効

(3)　ステータスポリシーの変更

対象の ID「2」を選択し、「有効」をクリックします。

(4)　有効化の確認

ID 横の×が消え、ポリシーが有効化されたことを確認してください。

7-2　ファイアウォールポリシーの無効化

有効化したポリシーを無効化する場合はステータスを無効に変更します。

ここでは例として、preset2：オフィス等から SSH（TCP/22）接続を許可するポリシーを無効化し、サーバーへの SSH 通信許可を取り消します。

(1)　ポリシーの無効化

対象の ID を右クリックし、「ステータス」>「無効」をクリックします。

(2) 無効化の確認

ID 横に×が追加され、無効化されたことを確認してください。

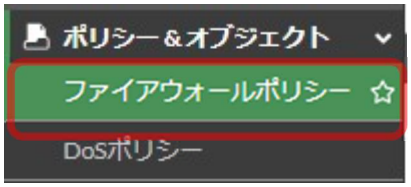
8. セキュリティ　アンチウイルス

アンチウイルスの設定

アンチウイルスとは、サーバーの通信を監視し、不正なウイルスを検知し感染を未然に防ぐシステムです。アンチウイルスは初期状態では OFF になっています。ここでは preset7（MAIL 通信を許可するポリシー）に作成済みアンチウイルスプロファイルの設定を行います。

(1)　IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「IPv4 ポリシー」をクリックします。



(2)　ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

(3)　アンチウイルスの有効化

下記のように設定し、最後に「OK」をクリックします。

アンチウイルス：「ON」に変更し、プルダウンから「AV_MAIL」を選択

SSL インスペクション：任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。

このポリシーを有効：有効になっていない場合は「ON」

（※SSL インスペクションの警告については 12-3「SSL インスペクション警告について」を参照ください。）

(4)　preset7 のセキュリティプロファイルに「AV」が追加されました。

サービス「MAIL」で許可されるサービスは「SMTP」、「Submission」、「POP3」、「IMAP」です。

※ ウイルスが検知された場合の動作

■POP3 / IMAP

受信したメールにウイルスが発見された場合は、ウイルスを含む添付ファイルのみが削除され、添付ファイルは次のメッセージに置き換えられます。送信元へウイルス検知の通知は行われません。

メッセージ

Dangerous Attachment has been Removed.　The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus.　File quarantined as: "."."ウイルス情報 URL"

■SMTP / SMTP_SUBMISSION

メール送信時にウイルスメールが発見された場合は、メールは送信されません。

送信元には、次のメッセージを含むエラーメッセージの表示またはエラーメールが配送されます。

送信メールのログ

Dangerous Attachment has been Removed.　The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus.　File quarantined as: "."."ウイルス情報 URL"

※　ポリシーに「アンチウイルス」と「アンチスパム」両方を設定し、「アンチスパム」の設定で SMTP のアクションに「タグ」を指定している場合

メール送信時にウイルスを検知した場合、ウイルスを含む添付ファイルのみが取り除かれ、メールが送信されます。

取り除かれた添付ファイルは次のメッセージに置き換えられます。

メッセージ

Dangerous Attachment has been Removed.　The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus.　File quarantined as: "."."ウイルス情報 URL"

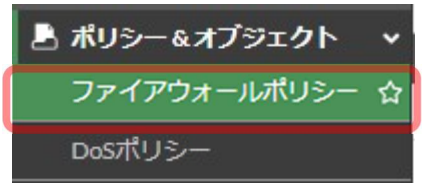
9. セキュリティ　アンチスパム

アンチスパムの設定

アンチスパムとは、サーバーの通信を監視し、迷惑メールを検知するシステムです。アンチスパムは初期状態では OFF になっています。ここでは preset7（MAIL 通信を許可するポリシー）にアンチスパムの設定を行います。

(1)　IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「IPv4 ポリシー」をクリックします。



(2)　ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

(3)　アンチスパムの有効化

下記のように設定し、最後に「OK」をクリックします。

アンチスパム：「ON」に変更し、プルダウンから任意のプロファイルを選択。例では「ANTISPAM」を選択

SSL インスペクション：任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。

このポリシーを有効：有効になっていない場合は「ON」

(4)　preset7 のセキュリティプロファイルに「EMAIL(アンチスパム)」が追加されました。

※ 迷惑メールが検知された場合の動作

■POP3 / IMAP*

受信したメールに迷惑メールが発見された場合は、該当メールの件名に[SPAM] と追記されます。

※IMAP はご利用のメールソフトによって挙動が異なることがあります

メールヘッダ

X-SpamInfo: FortiGuard - AntiSpam ase, X-ASE-REPORT:　(略)

■SMTP / SMTP_SUBMISSION

メール送信時に迷惑メールと判定された場合は、メールは送信されません。

送信元には、次のメッセージを含むエラーメッセージの表示またはエラーメールが配送されます。

送信メールのログ

554 5.7.1 This message has been blocked because ASE reports it as spam.　(in reply to end of DATA command))

メール送信時に迷惑メールと判断された場合は、該当メールの件名に[SPAM] と追記されます。

メールヘッダ

X-SpamInfo: FortiGuard - AntiSpam ase, X-ASE-REPORT:　(略)

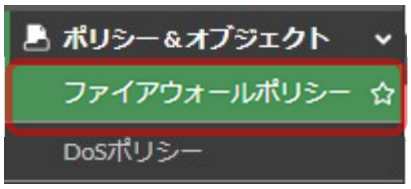
10. セキュリティ IPS

IPS の設定

IPS（侵入防止システム）とは、サーバーの通信を監視し、不正なアクセスを検知して攻撃を未然に防ぐシステムです。IPS は初期状態では OFF になっています。ここでは preset5（HTTP 通信を許可するポリシー）に IPS の設定を行います。

(1) IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「IPv4 ポリシー」をクリックします。



(2) ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

(3) IPS の選択

下記のように設定し、最後に「OK」をクリックします。

IPS：「ON」に変更し、プルダウンから「IPS_HTTP」を選択

SSL インスペクション：任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。

このポリシーを有効：有効になっていない場合は「ON」

Preset7 のセキュリティプロファイルに「IPS」が追加されました。

※HTTPS などの SSL 通信を監視する場合は別途「証明書インポート」、「SSL/SSH インスペクション」の設定が必要です。

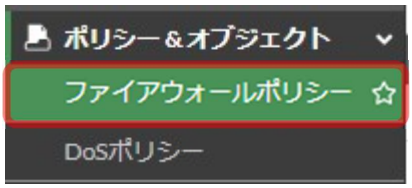
11.セキュリティ　WAF（Web アプリケーションファイアウォール）

WAF の設定

WAF とは、サーバーの通信を監視し、Web アプリケーションの脆弱性を悪用した攻撃を検知するシステムです。WAF は初期状態では OFF になっています。ここでは preset5（HTTP 通信を許可するポリシー）に WAF の設定を行います。

(1)　IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「ファイアウォールポリシー」をクリックします。



(2)　ポリシーの編集

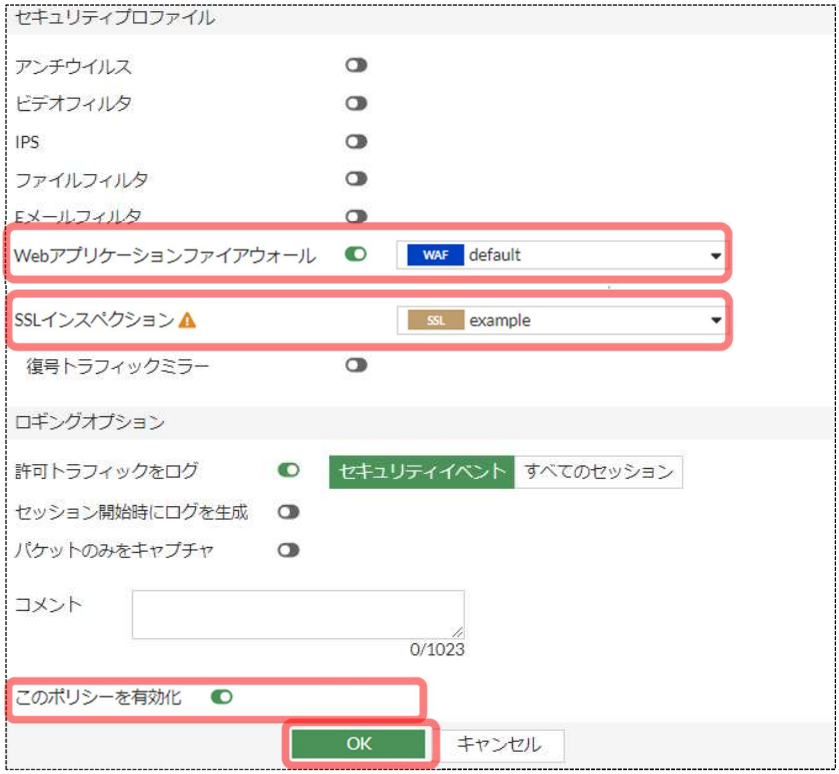
プリセットされている「preset 6」を選択し、「編集」をクリックします。

(3)　インスペクションモード：「プロキシ」を選択

Web アプリケーションファイアウォール：「ON」に変更

SSL インスペクション：任意のプロファイルを指定します。例では作成した SSL インスペクションプロファイルを指定しています。

このポリシーを有効：有効になっていない場合は「ON」



(4) preset5 のセキュリティプロファイルに「WAF」が追加されました。

※HTTPS などの SSL 通信を監視する場合は別途「証明書インポート」、「SSL/SSH インスペクション」の設定が必要です。

※ Web アプリケーションの脆弱性を悪用した攻撃が検知された場合の動作

ブラウザに以下のメッセージが表示され、アクセスがブロックされます。

Web Application Firewall This transfer is blocked by a Web Application Firewall. This transfer is blocked.

12. セキュリティ SSL/SSH インスペクション

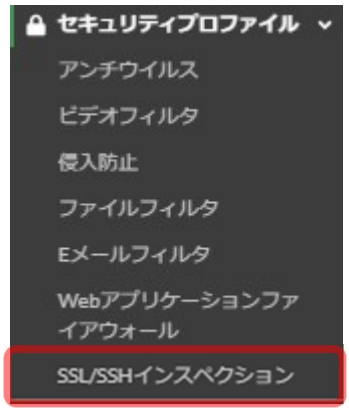
SSL/SSH インスペクション

暗号化された通信において UTM 機能を利用するための設定です。SSL/SSH インスペクションは初期状態では検査しない「no-inspection」が指定されています。ここでは preset6（HTTPS 通信を許可するポリシー）に SSL/SSH インスペクションの設定を行います。事前に「16.証明書のインポート」を実施ください。

12-1 SSL/SSH インスペクション設定

(1) SSL/SSH インスペクションの新規作成

「セキュリティプロファイル」>「SSL/SSH インスペクション」をクリックします。



(2) SSL/SSH インスペクションプロファイルの作成

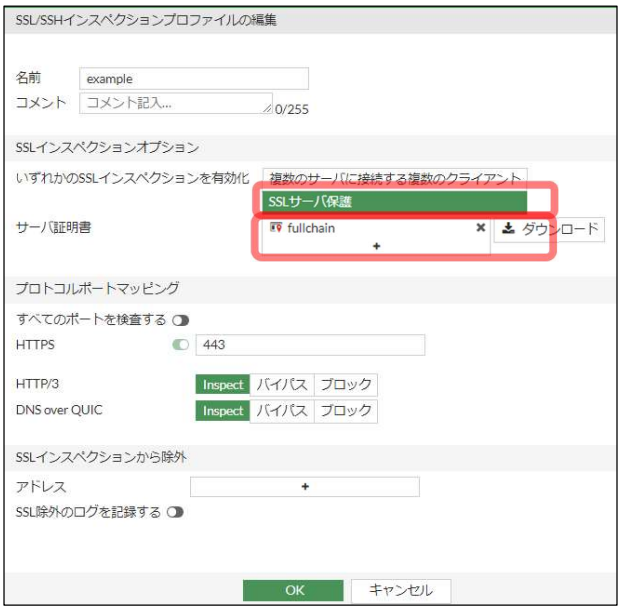
画面上の「新規作成」をクリックし、新しいプロファイルを作成します。

下記のように設定し、最後に「OK」をクリックします。

名前：任意の名前を入力

SSL インスペクションの有効：SSL サーバー保護

サーバー証明書：「16.証明書のインポート」でインポートした証明書を選択



12-2 ポリシーの設定

(1) IPv4 ポリシーの選択

「ポリシー＆オブジェクト」>「ファイアウォールポリシー」をクリックします。

(2) ポリシーの編集

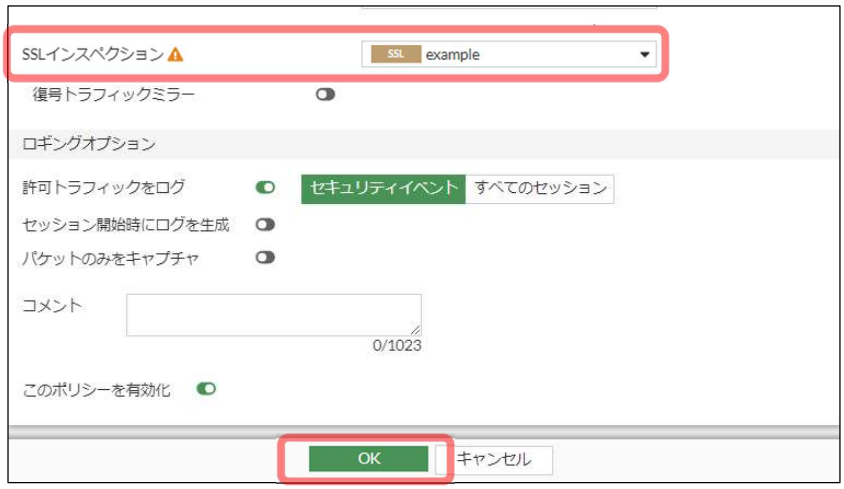
プリセットされている「preset 6」を選択し、「編集」をクリックします。

(3) SSL インスペクションの有効化

下記のように設定し、最後に「OK」をクリックします。

SSL インスペクション：プルダウンから「先ほど作成したプロファイル」を選択

このポリシーを有効：有効になっていない場合は「ON」



・SSL inspection フルインスペクションの注意アイコンについて

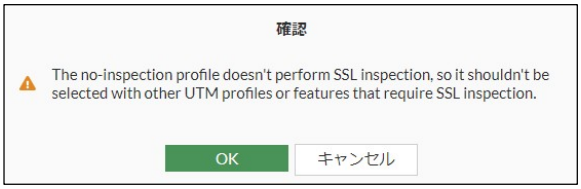
以下は FortiGate に設定した証明書はユーザのブラウザにインストールが必要という注意です。

証明書がパブリックな証明書発行期間から入手した CA 証明書をご利用であれば、問題ありません。自己証明書などをご利用の場合はエンドユーザーのブラウザに証明書のインストールが必要です。

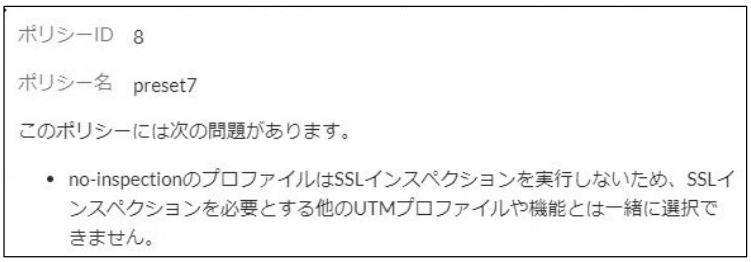
12-3 SSL inspection 警告について

SSL インスペクションは初期状態で「no-inspection(※SSL を監査しない)」セキュリティプロファイルが指定されています。
セキュリティプロファイルを設定して「no-inspection」が選択されている場合以下の警告が表示されます。

証明書をご利用の場合は、「16.証明書のインポート」、「12.SSL/SSH インスペクション」の設定を行うか
その他プリセットされている「certificate-inspection」等のプロファイルを選択してください。
手順例では「certificate-inspection」を選択し、SNI のチェックを行っています。
SSL を使用しない場合は、このまま OK を押して問題ありません。



「no-inspection」を選択した場合、次のようにファイアウォール一覧で注意アイコンが表示されます



このエラーメッセージに関する詳細は次をご参照ください
https://community.fortinet.com/t5/Customer-Service/Technical-Tip-How-to-resolve-the-warning-message-The-no/ta-p/244152

13. ロードバランサー

ロードバランサーの設定

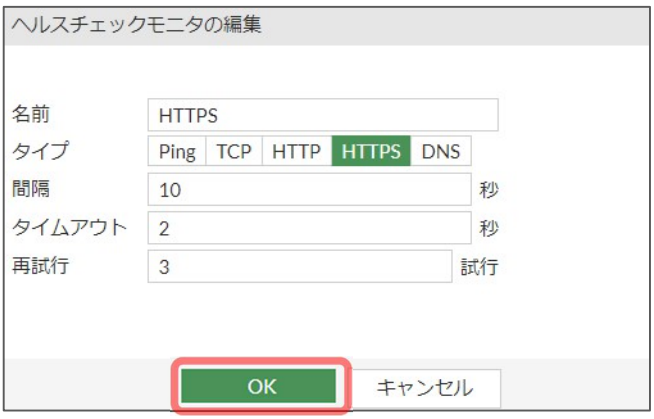
FortiGate は L4 レベルで負荷分散を行うことができます。ここでは HTTP サーバー2 台をラウンドロビン方式で負荷分散する設定を行います。ロードバランサーではバーチャル IP の設定が必要です。

13-1 ヘルスチェックモニタの作成

「ポリシー＆オブジェクト」>「ヘルスチェック」をクリックします。「新規作成」をクリックし、「ヘルスチェックモニタ」を編集します。

ヘルスチェックモニタの設定を行います。

名前	ヘルスチェック名を指定（例は、「HTTPS」と指定）
タイプ	タイプを指定（例は、「HTTPS」を指定）
間隔	チェック間隔を指定
タイムアウト	タイムアウトになるまでの時間を指定
再試行	再試行の回数を指定



内容を確認し、「OK」をクリックします。

13-2 バーチャルサーバの作成

「ポリシー＆オブジェクト」>「バーチャルサーバ」をクリックします。「新規作成」をクリックし、「バーチャルサーバ」を編集します。

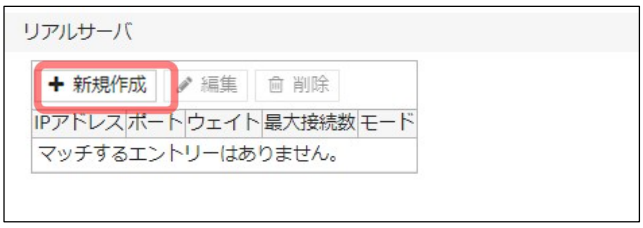
バーチャルサーバの設定を行います。

名前	バーチャルサーバ名を指定（例は、「WebServer_VIP」）
タイプ	タイプを指定（例は、「HTTPS」）
バーチャルサーバ IP	NIC4 の NW 帯からサーバーで使用していないものを指定 ※コントロールパネルにログインし、「セキュリティ」>「UTM/NIC4」>「基本情報」のゲートウェイを確認します。 （SuitePRO V4 https://pro4.arena.ne.jp または IndigoPro https://compas.arena.ne.jp/） 仮にゲートウェイが 203.0.113.1 の場合、203.0.113.2 から 203.0.113.6 の 5 個の範囲でアドレスを選択できます。例えば、サーバーで 203.0.113.2 と 203.0.113.3 を使用している場合、バーチャルサーバ IP に最後の 203.0.113.6 を指定します。
バーチャルサーバポート	ポート番号を指定（例は、「443」）
ロードバランス方法	ロードバランスの方法を選択（例は、「ラウンドロビン」）
ヘルスチェック	ヘルスチェック方法を選択。ヘルスチェック選択可の中から選択し、⇒をクリックして右側に移動させる。（例は、「HTTPS」を指定）
クライアント IP の保持	必要に応じて ON/OFF してください。 「クライアント IP の保持」を ON にすると、クライアント IP アドレスは **X-Forwarded-For** ヘッダーに記録されます。（X-Forwarded-For のロギングは別途 Web サーバーなどの設定が必要です。）
モード	SSL オフロードの範囲を選択します。例では「フル」を選択します。
証明書	Web サーバーの証明書を指定します「 証明書のインポート」でアップロードします

（例）NIC4 の NW 帯からサーバーで使用していないものを指定

13-3 リアルサーバの作成

そのまま画面の下へ移動し、リアルサーバーの「新規作成」をクリックします。



リアルサーバの設定を行います。

IP アドレス	サーバーの IP アドレスを指定（例は、203.0.113.2 と 203.0.113.3）
ポート	ポート番号を指定（例は、「80」を指定 HTTPS の場合は「443」を指定）
モード	対象サーバーの状態を指定（例は、「アクティブ」を指定）

内容を確認し、「OK」をクリックします。

同様に、もう 1 台リアルサーバを作成します。（例：203.0.113.3）

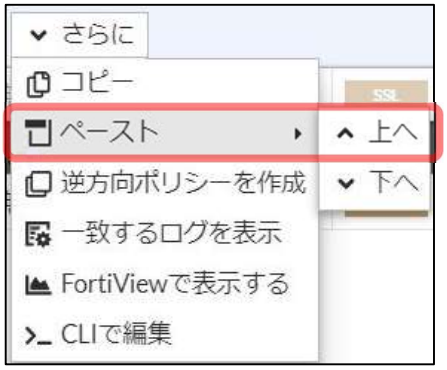
追加したリアルサーバを確認して「OK」をクリックします

13-4 ファイアウォールポリシーの作成

「ポリシー＆オブジェクト」>「IPv4 ポリシー」をクリックし、「preset6」を選択した状態で右クリックし、「コピー」をクリックします。

（HTTPS の場合は「preset6」）

次に「ペースト」を選択し、「上へ」をクリックします。「preset6」の上に新しいポリシーが作成されます。



新しいポリシーを選択した状態で「編集」をクリックします。

ファイアウォールポリシーを編集します。

名前	ポリシーの名前を入力（例は、LB-HTTPS）
送信元	送信元を指定します。（例は、all）
宛先アドレス	送信先を指定します。（例は、WebServer_VIP）
サービス	対象のサービスを選択（例は、HTTP）リアルサーバに設定したプロトコルに合わせて設定します。

※サービスはバーチャルサーバに指定したプロトコルに合わせる

最後に「このポリシーを有効」を ON にして「OK」をクリックします。

13-5 ロードバランサー接続確認

先ほど、手順「バーチャルサーバの作成」で作成したバーチャル IP に接続できることをブラウザで確認する。

例の場合 https://203.0.113.6

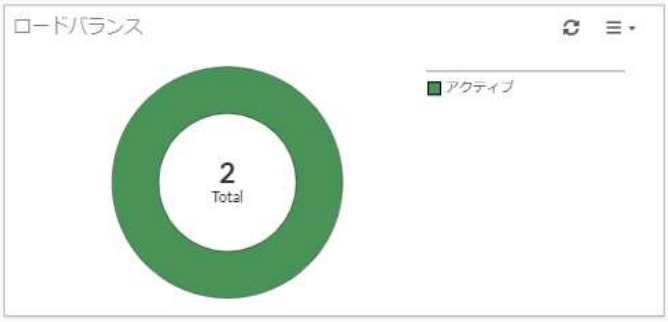
※バーチャルサーバの VIP（もしくはドメイン名）に対してアクセスします。

<ヘルスチェックの状態を確認する>

ヘルスチェックを確認する場合はダッシュボード>ステータスで「ウイジェット追加」します

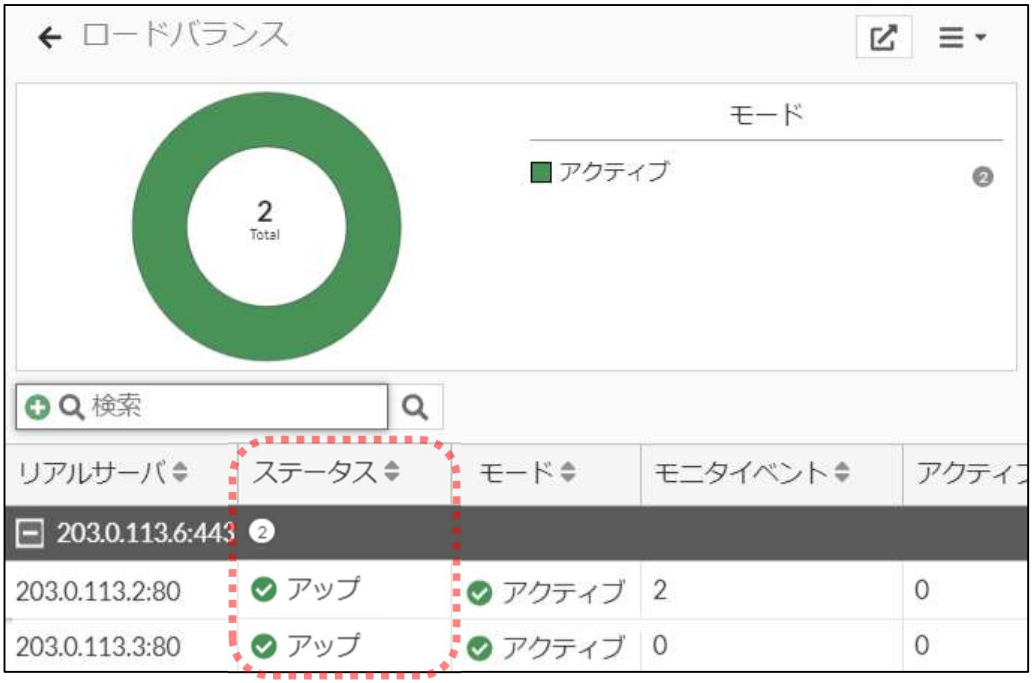
「ロードバランス」を選択します

ダッシュボードに「ロードバランス」が追加されます。ダブルクリックで展開します



リアルサーバのヘルスチェック状況が確認できます

ステータスが「アップ」になっていることを確認してください。（モードが無効の場合、ステータスは常に「ダウン」になります）



14. IPsec（FortiClient リモート接続）

IPSecVPN の設定

FortiClient をインストールしたパソコンから、FortiGate へ IPsec 接続することができます。

14-1 ユーザの作成

(1) ユーザグループを作成します。

「ユーザ＆認証」>「ユーザグループ」をクリックします。「新規作成」をクリックし、「ユーザグループ」を作成します。

ユーザグループ名を入力します。（例：IPsec_group）

タイプは「ファイアウォール」を選択し、「OK」をクリックします。

(2) 次にユーザ定義を作成します。「ユーザ＆デバイス」>「ユーザ定義」を選択し、「新規作成」をクリックします。

(3) ユーザタイプで「ローカルユーザ」を選択し、「次へ」をクリックします。

(4) ログイン クレデンシャルの設定： 認証用のユーザ名（例：ipsec_user）、パスワードを入力して「次へ」をクリックします。

(5) コンタクト情報の設定：必要に応じて二要素認証を有効にし、「次へ」をクリックします。

(6) エキストラ情報：「ユーザグループ」を ON に設定し、ユーザグループに先ほど作成したグループを指定して「作成」をクリックします。

14-2 IPsec の設定

「IPsec」の設定をします。

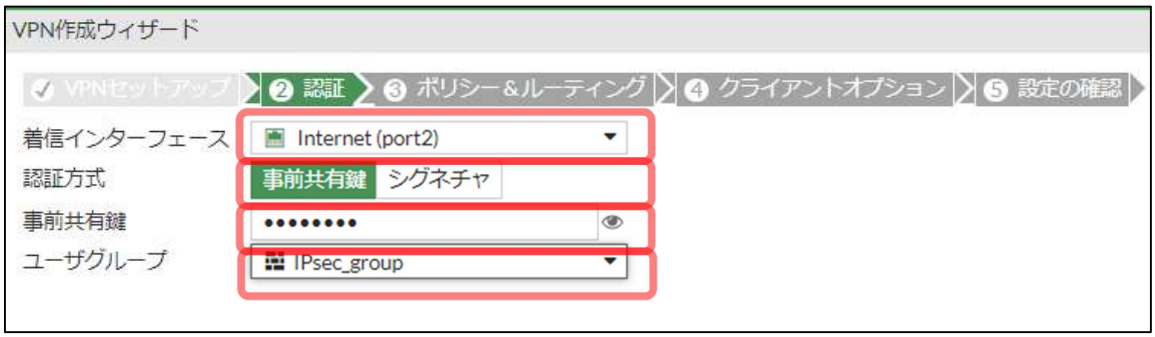
(1) VPN セットアップの設定

「VPN」>「IPsec ウィザード」をクリックします。任意の「名前」を入力、「リモートアクセス」を選択し、「次へ」をクリックします。

(2) 認証 設定

下記のように設定します。本手順では【事前共通鍵】を選択します。

着信インターフェース	「Internet(port2)」を指定
認証方式	選択します。例では事前共通鍵を指定
事前共通鍵	（任意の文字列）※**FortiClient 設定時に私用します**
ユーザグループ	IPsec の接続を許可するユーザーグループを指定します。 ※ここでは手順「14-1」で作成した「IPsec_group」を指定



(3) ポリシー＆ルーティング

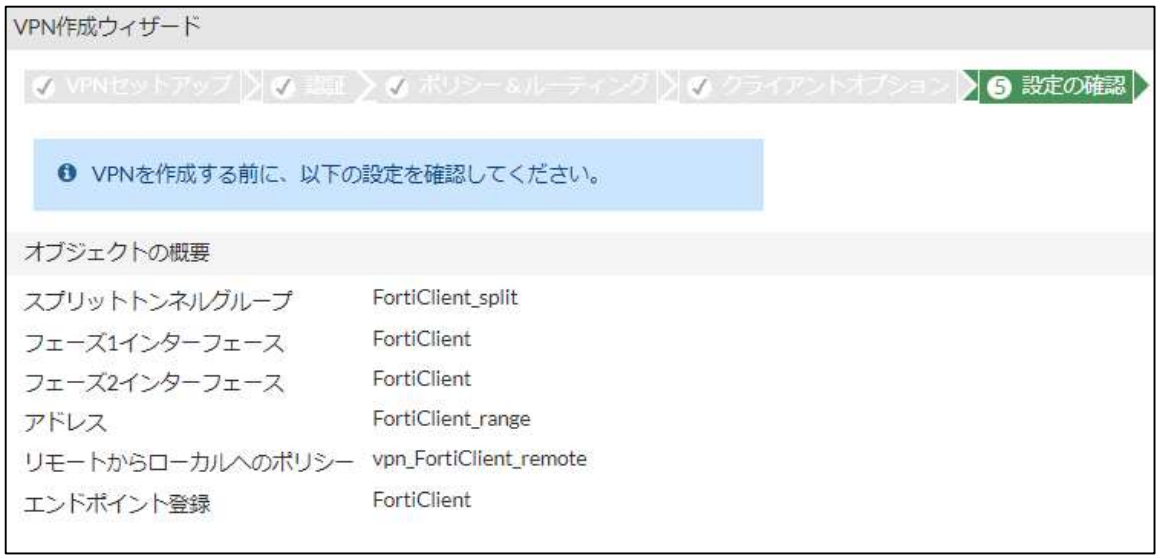
「VPN」>「SSL-VPN 設定」をクリックします。ポリシーの作成画面に移り、設定します。

ローカルインターフェース	「SuitePRO_NW(port1)」を指定
ローカルアドレス	IPsec 接続を許可する**接続先**を選択。例は「SuitePRO_NW」
クイアントアドレス範囲	クライアントに割り当てるアドレス帯を指定します。 例は「192.168.100.10-192.168.100.20」
サブネットマスク	クライアントに割り当てるサブネットマスクを指定します 例は「255.255.255.255」

※DNS サーバー　：システム DNS を使うを選択すると Fortinet の DNS が設定されます。
指定の DNS がある場合は「指定」を選択してアドレスを入力してください。
※IPv4 スプリットトンネル：
ON にした場合「ローカルアドレス」で指定した宛先の通信のみが IPsecVPN 経由になります。OFF にした場合、接続元クライアントの通信はすべて IPsecVPN 経由となります。接続元のネットワーク環境が大きく変わりますのでご注意ください。

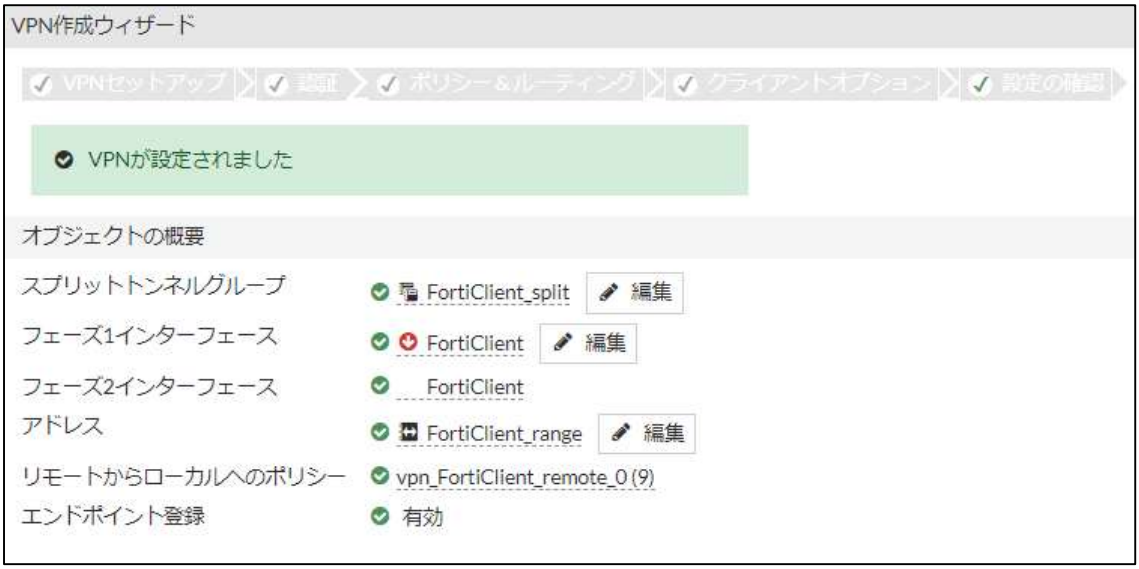
(4)　クライアントオプション
設定を選択し、「次へ」をクリックします。

(5)　設定の確認
設定の一覧が表示されますので確認します。



(6)　結果確認

結果が示されます。



14-3　　ファイアウォールポリシーの設定

IPsec 用のポリシーが新たに作成されていますので内容を確認します

「ポリシー&オブジェクト」>「ファイアウォールポリシー」を選択します。対象の IPsec トンネル名のポリシーを選択します。

NAT 設定は最初「ON」になっております。ON になっていると、IPsec を経由するすべての接続元のアドレスが FortiGate のインスタフェースになります。接続元アドレスをクライアントアドレスにする場合は「NAT」の設定を「OFF」にしてください。

14-4 クライアント設定

クライアント端末に FortiClient のインストールを行います。

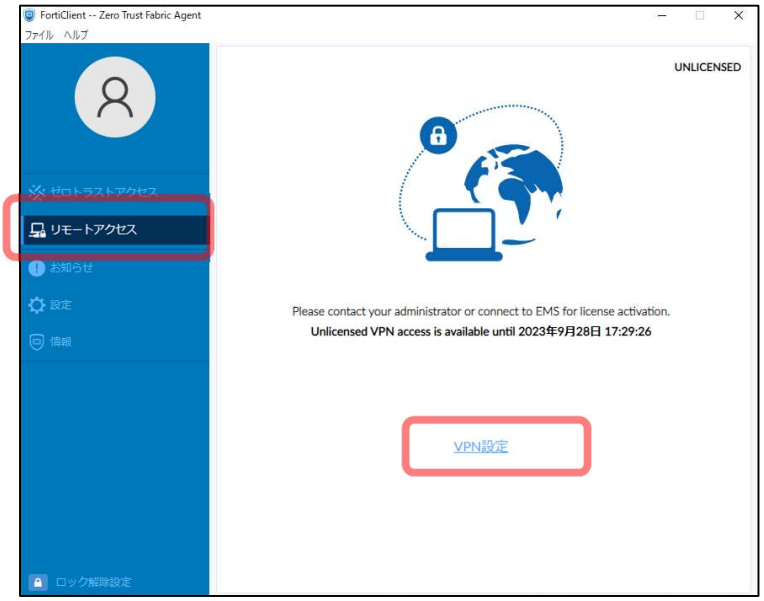
(1) ダウンロード

https://www.forticlient.com/downloads にアクセスします。

「**FortiClient VPN**」をダウンロードし、クライアント端末にインストールします。

(2) FortiClient の設定

インストールした FortiClient を起動し、リモートアクセス＞IPsec VPN を選択します。

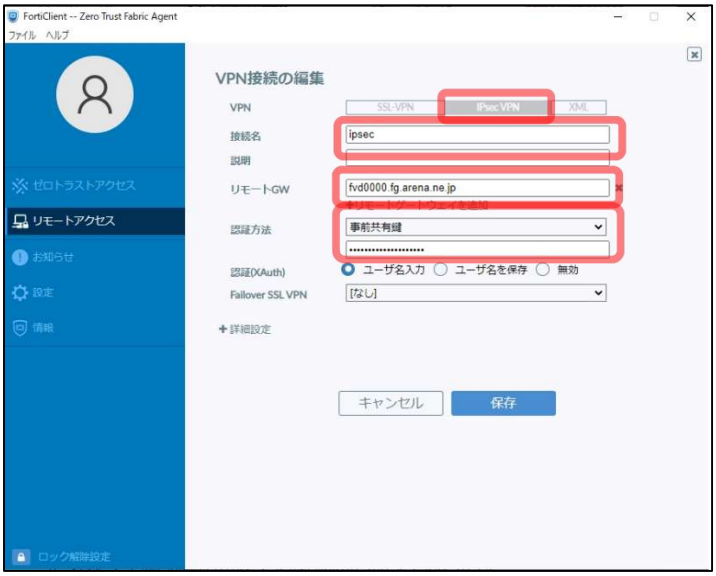


(3) FortiClient の設定

インストールした FortiClient を起動し、リモートアクセス＞IPsec VPN を選択します。

以下の情報を入力し「適用」をクリックします。

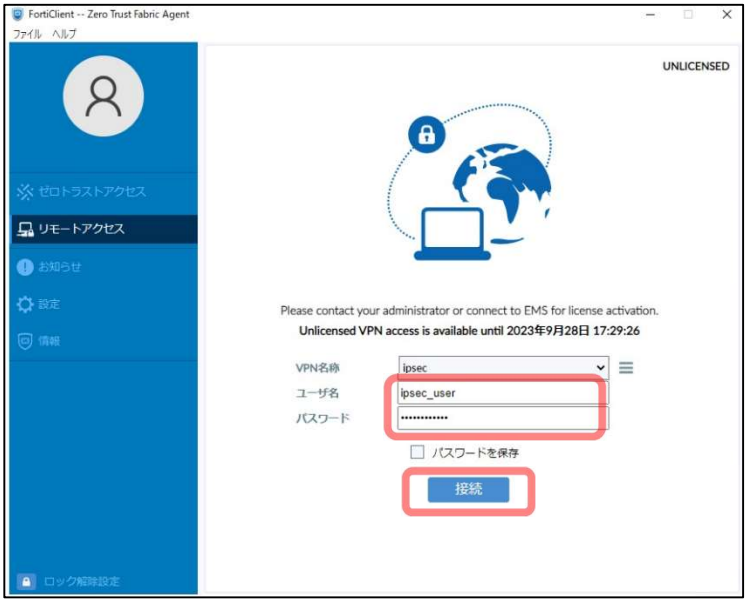
接続名	任意の名前を入力（例は、「ipsec vpn」）
リモート GW	FG 管理サイトのホスト名（例は、fvd0000.fg.arena.ne.jp） ※お客さまにて、FG 管理サイト用のドメインを別途取得している場合はそちらを指定する
認証方法	指定した認証方法を設定します。(例 事前共通鍵の場合：事前共通鍵を指定し、「14-2(2)認証 設定」で設定したパスワード 設定したパスワードを入力します)



(4)　接続

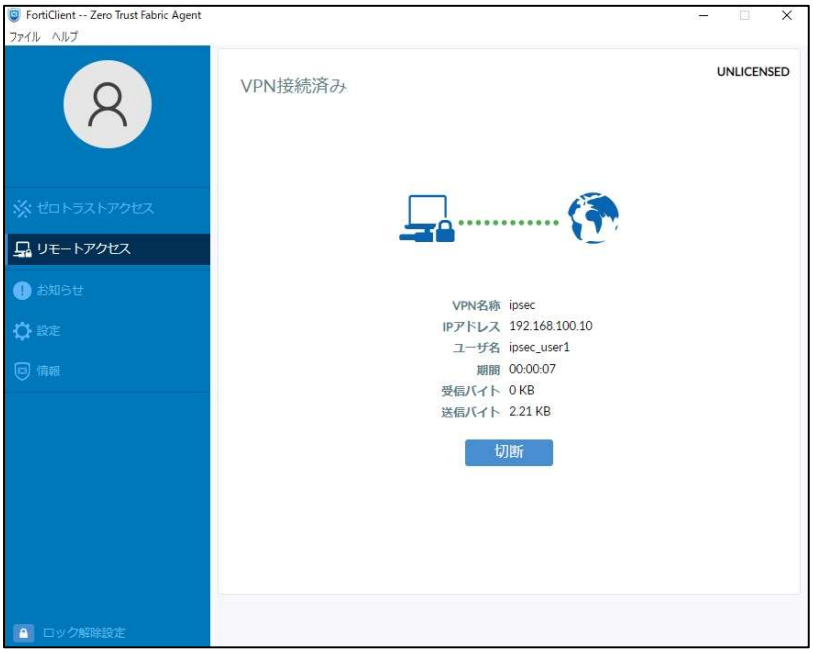
ユーザ名、パスワードを入力し「接続」をクリックし、接続します。

※14-1 ログイン　(4) クレデンシャルの設定で作成したユーザ



(5) 接続状態確認

VPN 接続済みになったことが確認できます。



代表的なエラー

エラー表示	対処
不正なクレデンシャル	ユーザ ID とパスワードを再度確認します。
VPN connection failed. Please check your configuration and network connection, then try your connection. If the problem persists, contact your network administrator for help	FortiClient のポリシーGW に指定したホストと通信ができません。もしくは事前共通鍵などに誤りがあります。FortiClient の設定を確認してください。
トンネルゲートウエイ/ポリシーサーバーと疎通できません。	FortiClient のポリシーGW に指定したホストと通信ができません。FortiClient の設定を確認してください。

15. IPsec（サイト間接続）

IPsec の設定

FortiGate や Cisco などの機器から IPsec トンネルを使用した VPN 接続をすることができます。
ここでは、例として FortiGate を使用したリモート拠点との接続について説明します。
また、拠点側 FortGgate に固定の WAN 側 IP アドレスが設定されている場合について解説します。

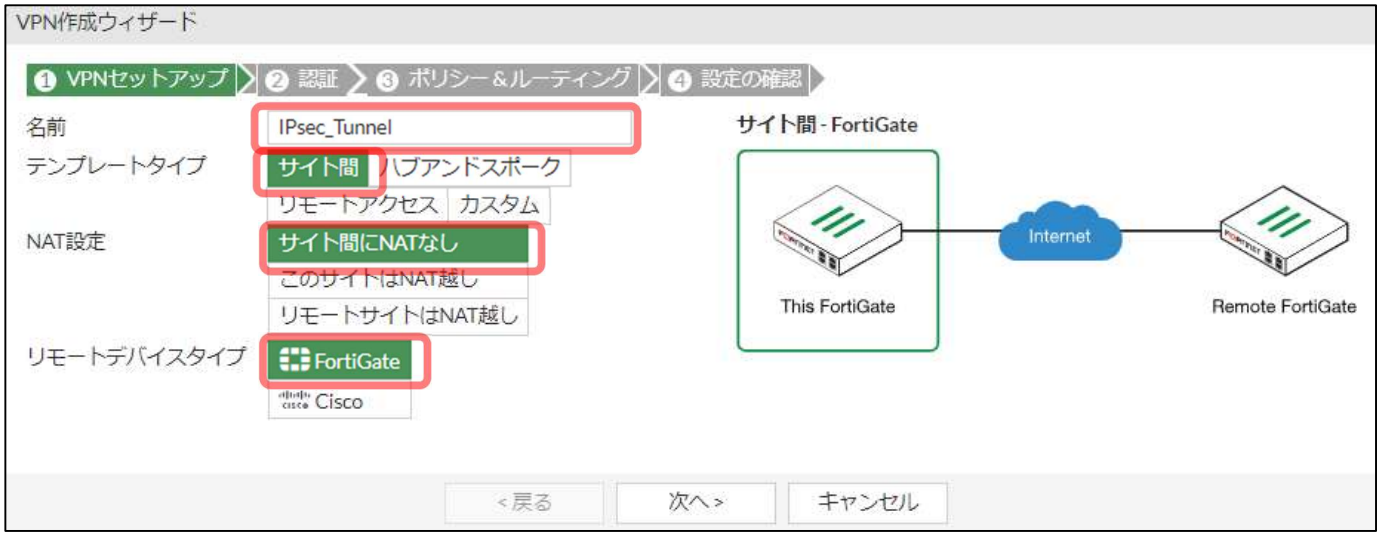
15-1 IPsec トンネルの作成

(1) IPsec トンネルの作成

[VPN]>[IPsec ウィザード]をクリックします。

以下のように設定します。

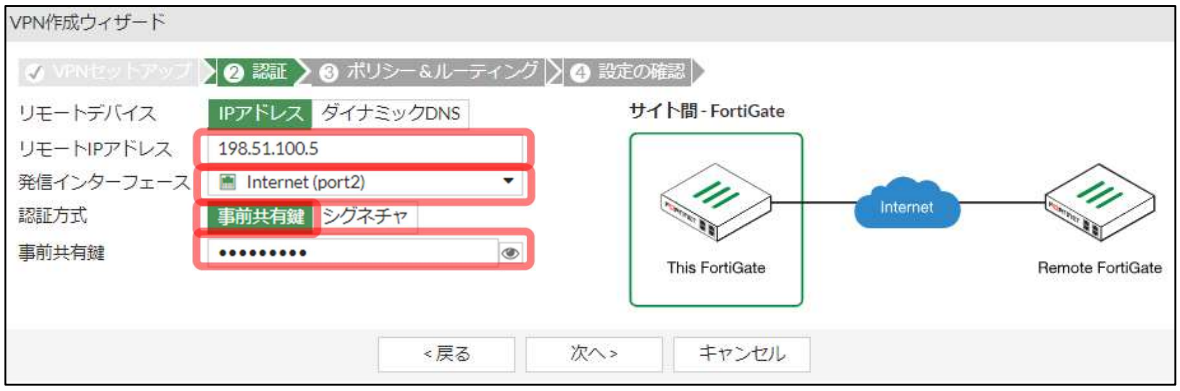
名前	任意の名前を設定します（例は「IPsec_Tunnel」）
テンプレートタイプ	サイト間
NAT 設定	サイト間に NAT なし
リモートデバイスタイプ	FortiGate



[次へ]を押下します。

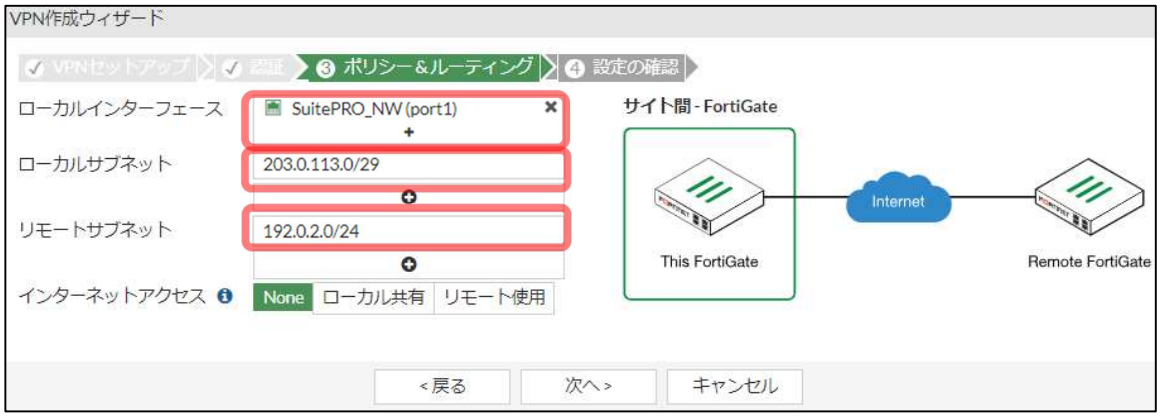
リモートデバイス	IP アドレス
IP アドレス	リモート拠点 FortiGate の wan 側 IP アドレスを指定します。（例では「198.51.100.5」としています）
発信インターフェース	Internet(port2) 自動的に選択されます
認証方式	例では「事前共通鍵」を選択します
事前共通鍵	任意の文字列を入力します **後程リモート拠点側の IPsec 設定でも使用しますので必ず控えておきます。**

[リモートデバイス]を『IP アドレス』とし、[IP アドレス]欄へリモート拠点 FortiGate の wan 側 IP アドレスを[xxx.xxx.xxx.xxx]の形式で入力します。([出力インターフェース]は自動的に選択されます)
[認証方式]を『事前共有鍵』とし、[事前共有鍵]欄に任意の文字列を入力します。
この『事前共有鍵』は後程リモート拠点側の IPsec 設定でも使用しますので必ず控えておきます。



[次へ]を押下します。

[ローカルインターフェース]にて『SuitePRO_NW(port1)』を選択します。
[ローカルサブネット]にはお客様の環境に応じて自動的に入力が行われますので、
[リモートサブネット]欄にリモート拠点側の LAN 側セグメントを[xxx.xxx.xxx.xxx/xx]の形式で入力してください。



[作成]を押下します。

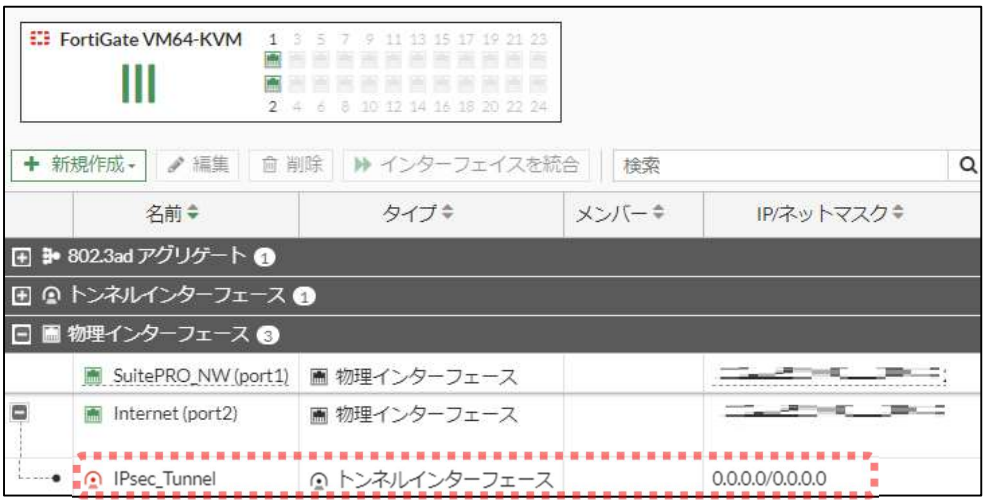
IPsec トンネルが作成されました。

15-2 作成された IPsec トンネルの確認

(1) 自動追加されたリソースの確認

正常に作成されると、以下の項目が自動で追加、設定されます。

[ネットワーク]>[インターフェース]に IPsec トンネルが追加されます。



[ネットワーク]>[スタティックルート]にルールが 2 つ追加されます。

[ポリシー&オブジェクト]>[IPv4 ポリシー]に以下のポリシーが追加されます。

デフォルトでは拠点間の通信は全て許可となりますので、必要に応じてお客様側でポリシーの設定をお願いします。

[ポリシー&オブジェクト]>[アドレス]に以下のアドレスが追加されます。

名前	タイプ	インターフェース	詳細	IP	参照
FABRIC_DEVICE	サブネット			0.0.0.0/0	0
FIREWALL_AUTH_PORTAL_ADDRESS	サブネット			0.0.0.0/0	0
IPsec_Tunnel_local_subnet_1	サブネット			203.0.113.0/29	1
IPsec_Tunnel_remote_subnet_1	サブネット			192.0.2.0/24	1

15-3 (参考)リモート拠点側の設定

参考として、リモート拠点側 FortiGate の設定例を示します。

(1) IPsec トンネルの作成

[VPN]>[IPsec ウィザード]をクリックします。

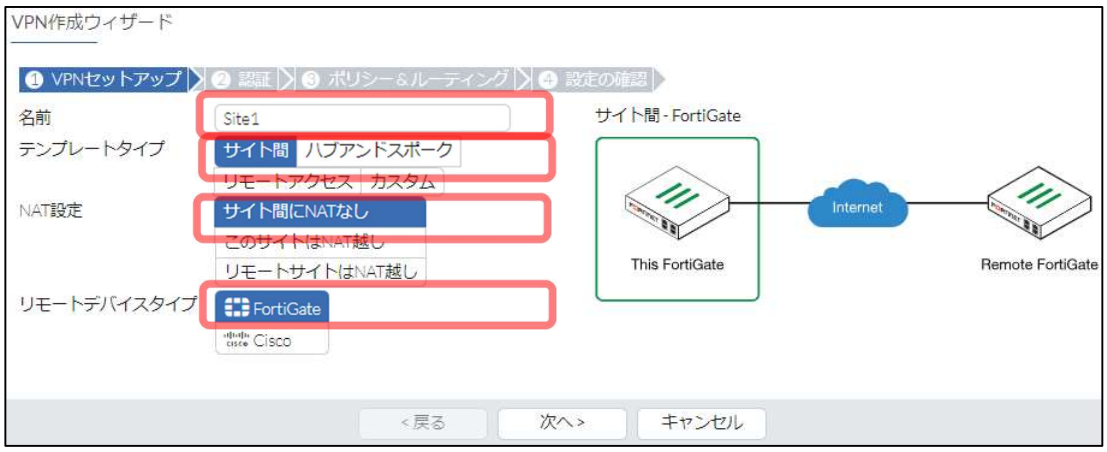
[名前]に任意の名前を入力します(ここで指定する名前は [15-1]で入力したものと同一でなくて構いません)。

例) Site1l

[テンプレートタイプ]を『サイト間』、

[リモートデバイスのタイプ]を『FortiGate』、

[NAT 設定]を『サイト間に NAT なし』とします。



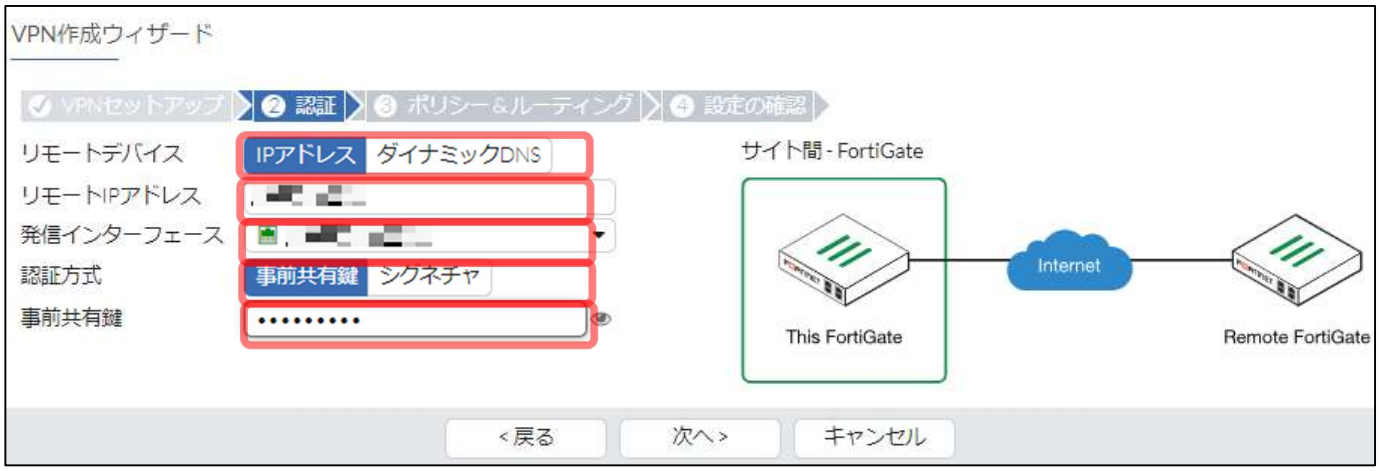
[次へ]を押下します。

[リモートデバイス]を「IP アドレス」

[IP アドレス]へ対象 UTM の wan 側 IP アドレスを入力します。

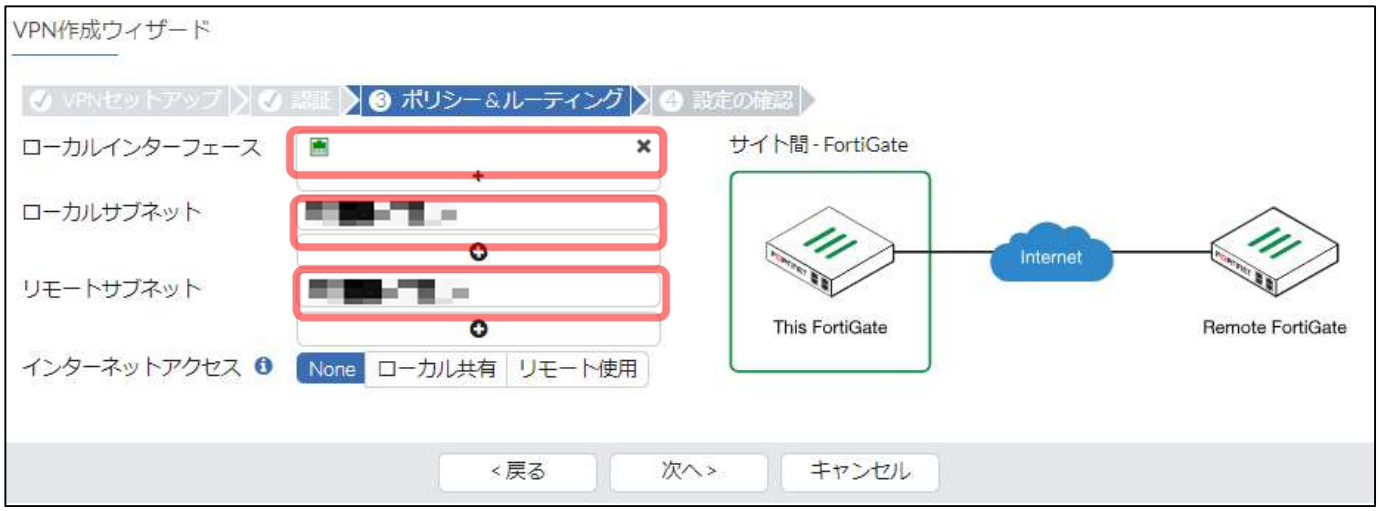
[発信インターフェース]はリモート側のインターネット側インターフェースを指定します。

[認証方式]を『事前共有鍵』とし、[事前共有鍵]欄に**[15-1]で UTM 側作業時に設定したものと同一の事前共有鍵**を入力します。



[次へ]を押下します。

[ローカルインターフェース]にて IPsec 接続をするお客様環境の LAN 側インターフェースを選択します。
[ローカルサブネット]が IPsec 接続をするお客様環境の LAN 側セグメントになっていることを確認の上、
[リモートサブネット]欄にサーバー側セグメント(SuitePRO_NW(port1)のセグメント)
を[xxx.xxx.xxx.xxx/xx]の形式で入力してください。



[作成]を押下します。

IPsec トンネルが作成されました。

作成後は、[15-2]を参考に適宜設定内容の確認を行ってください。

16. 証明書のインポート

証明書のインポート

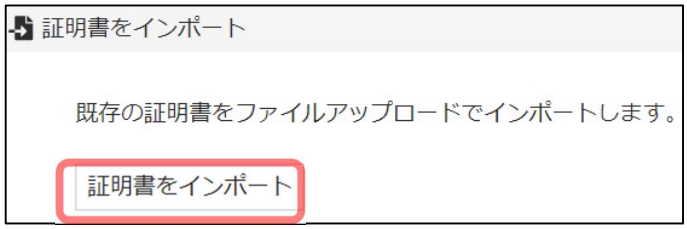
FortiGate で利用する証明書をインポートします。

(1) 証明書の選択

「システム」>「証明書」をクリックします。

(2) 「インポート」>「ローカル証明書」をクリックします。

「証明書をインポート」をクリックします。



(3) 証明書・キーファイルの選択

下記のように指定し、最後に「OK」をクリックします。

タイプ：証明書

証明書ファイル：証明書ファイルを選択

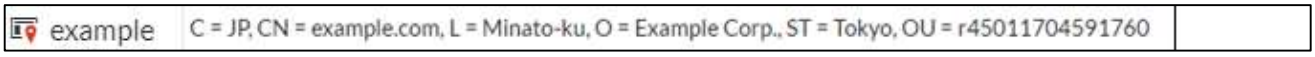
キーファイル：秘密鍵ファイルを選択

パスワード：鍵ファイルにパスワードを設定している場合のみ入力

証明書名：ファイル名に合わせて自動的に設定されます。書き換えることもできます。

(4) 証明書インポート確認

証明書の一覧に新しく証明書が追加されたことを確認します。



ステータスも「OK」になっていることを確認します。

17.コンソール

コントロールパネルからコンソールに接続し、FortiGate にログインすることができます。

17-1 コンソールからログイン

(1) コントロールパネルにログインして「セキュリティ」メニューをクリックし、プルダウンから「UTM/NIC4」を選択します。

SuitePRO V4（https://pro4.arena.ne.jp）
IndigoPro（https://compas.arena.ne.jp）

(2) 「基本情報」タブの「UTM 情報」 > 仮想 UTM サーバー管理」にある、「仮想 UTM サーバー」をクリックします。

(3) 右側のコンソール「開く」をクリックするとコンソール画面が開きます。

(4) ログインアカウントとパスワードを入力し、ログインします。

```
fvd0000 login : username
Password:
Welcome!
```

コマンドの詳細は Fortinet 社の CLI reference を参照ください。（使用中のバージョンを選択してください）
Fortinet Document Library https://docs.fortinet.com/product/fortigate/

17-2 接続元 IP アドレスの許可設定を追加する場合

ここでは FortiGate に接続元のアドレス許可設定を行います。UTM 管理サイトにアクセスするには、接続元のアドレスを許可設定が必要です。接続元のアドレス許可設定は UTM 管理サイトまたはコンソールで行えます。

アカウント名	（例）username
追加するアドレス	（例）203.0.113.41

(1) 「config system admin」と入力し、管理者アカウントの設定に移動します。続いて「get」と入力し、現在のアカウントの一覧を表示し、アカウント名を確認します。

```
fvd0000 # config system admin

fvd0000 (admin) # get
 == [ username]
name: username
```

(2) 「edit アカウント名」で対象のアカウントの設定に移ります。「show」と入力すると現在の設定が表示されます。
「trusthost」が何番まで使われているか確認します。例では"trusthost1"が使われています。

```
fvd0000 (admin) # edit username
fvd0000 (username) # show
config system admin
    edit "username"
        set trusthost1 203.0.113.40 255.255.255.255
        set accprofile "super_admin"
        set vdom "root"
        set password ENC SH2EGMYy5NOQsZ+YqoNFzxROnlY6utMjhQLlOKHB
    next
```

(3) trusthost2 にアドレスを追加します。(例)「set trusthost2 203.0.113.41 255.255.255.255」と入力します。
「trusthost」は 1 から 10 まで使用可です。追加の場合は、元の設定を上書きしないよう使われていない番号を選択してください。
現在の設定を書き換えたい場合は対象と同じ番号を指定します。

```
fvd0000 (username) # set trusthost2 203.0.113.41 255.255.255.255
```

(4)　追加後、「show」コマンドで現在の設定を確認します。trusthost2 に「203.0.113.41」が追加されています。

```
fvd0000 (username) # show
config system admin
    edit "username"
        set trusthost1 203.0.113.40 255.255.255.255
        set trusthost2 203.0.113.41 255.255.255.255        ←追加されている
        set accprofile "prof_admin"
        set vdom "root"
        set password ENC SH2EGMYy5NOQsZ+YqoNFzxROnlY6utMjhQLlO
    next
end
```

(5)　「next」で設定を終了します。ここで設定が保存・反映されます。続いて「end」「exit」で FortiGate からログオフします。

```
fd0000(user name) # next
fvd0000(admin) #end
#exit
```

18. FortiGate 管理-snmp 監視設定

FortiGate 自身を外部の監視サーバーから監視するための設定です。

18-1 インターフェース設定

(1) ネットワーク>インターフェースを開き、port1 (SuitePRO_NW)を選択し、色を反転させ、編集をクリックします。

(2) 管理者アクセスの SNMP を ON にします。

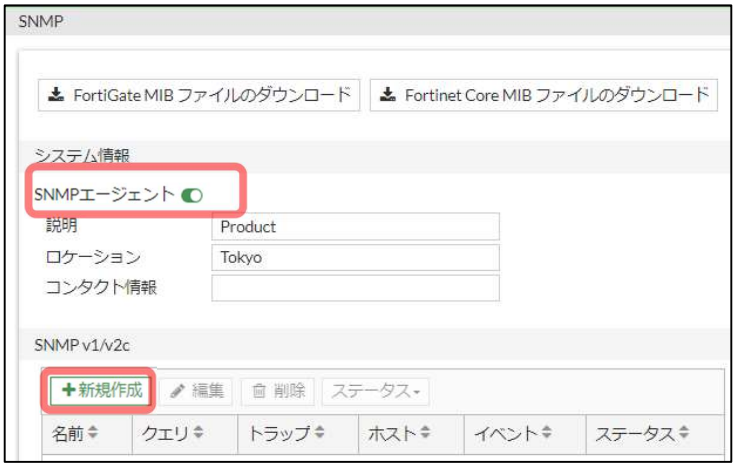
(3) 中央下の「OK」をクリックします。

18-2 snmpd 設定

システム＞snmpd を選択します

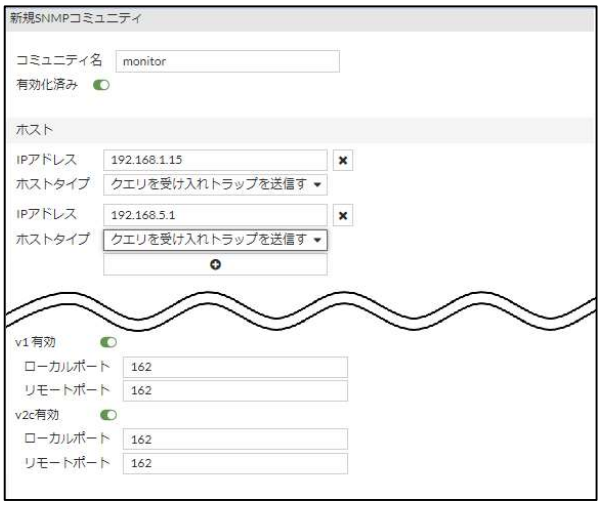
(1) SNMP エージェントの設定を ON にして説明やロケーションなど任意の情報を入力します。コミュニティを作成します。

「新規作成」をクリックします。

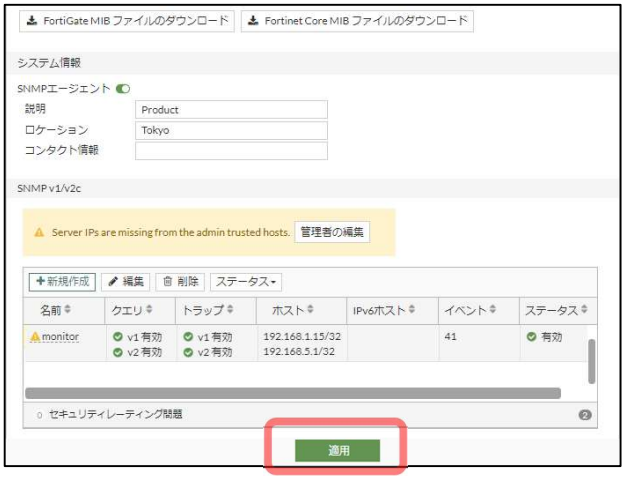


(2)　ホストの項目に監視サーバーの設定を入力します。
コミュニティ名：監視サーバーと同じコミュニティ名を入力します。
IP アドレス：監視サーバーの IP アドレス
ホストタイプ：クエリやトラップ等の種別を選択

他トラップを選択し、「OK」をクリックします

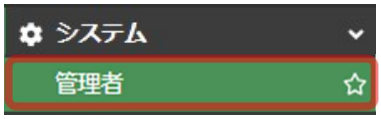


(3)作成されたことを確認し「適用」をクリックします。



18-3 管理アカウント設定

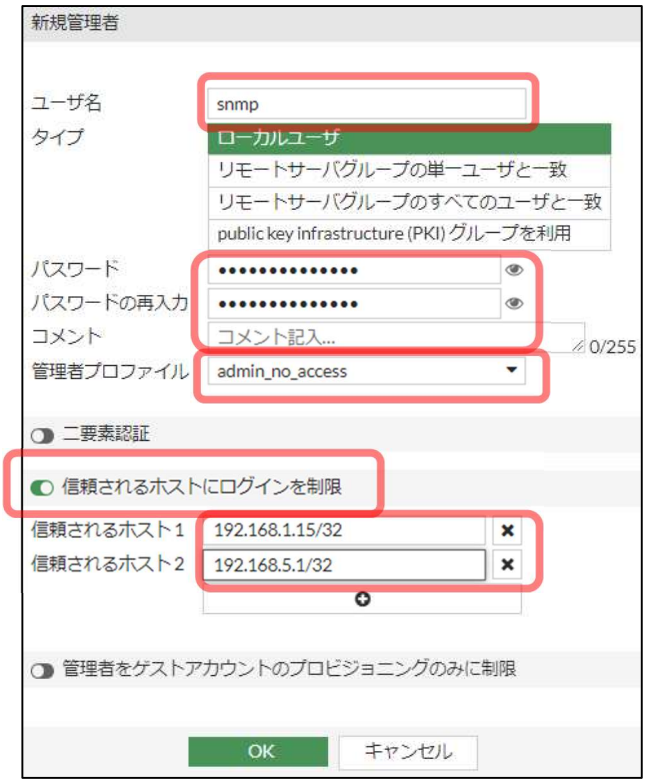
(1) システム>管理者を開きます。



新規作成> 管理者 を選択します

(2)　管理者設定を入力します

項目	値
名前	任意（例では「snmp」）
パスワード	任意
管理者プロファイル	admin_no_access
信頼されるホストにログインを制限	ON
信頼されるホスト	SNMP 監視サーバーのアドレスを入力



19. FortiGate 管理-CPU･メモリ負荷の詳細確認

負荷状況の詳細を確認します

sys top の確認と プロセスの kill

(1) CLI コンソールを開きます。画面右上のメニューをクリックします

CLI コンソール

(2) CLI ウインドウが表示されます

「diagnose sys top」と入力し、実行します。コマンドを入力してソートすることができます。

c ：CPU 使用率の順にソートして表示

m：メモリ使用率の順にソートして表示

q：表示を終了

左から、プロセス名、プロセス ID,現在のステータス、CPU 使用率(%)、メモリ使用率(%)を示します。

例「updated」プロセスはシグネチャ・DB などのアップデートプロセスです。処理中は一時的に CPU を消費します

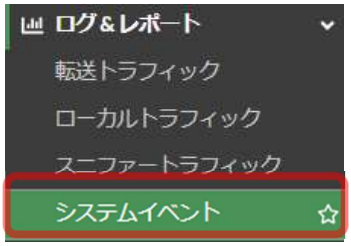
```
Run Time:  0 days, 4 hours and 1 minutes

    9U, 0N, 2S, 85I, 4WA, 0HI, 0SI, 0ST; 1992T, 855F
       updated    32630      R N    92.8     0.2
          node      254      S <     1.9     0.3
        sslvpnd      404      S       0.5     0.1
        slbrpcd      372      S       0.5     0.0

      forticldd      343      S       0.1     0.2

          httpsd    25525      S       0.1     0.1
initXXXXXXXXXX        1      S       0.1     0.0
          newcli    32641      R       0.1     0.0
```

20. FortiGate 管理-システムログの確認

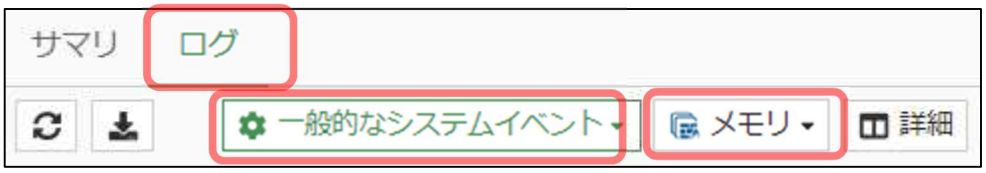
FortiGate のログを確認します

システムログの確認

(1) ログ&レポート>システムイベントを開きます。



(2) ログをクリックし、「一般的なシステムイベント」を選択し、「メモリ」(またはディスク)をそれぞれ選択します。



ログ出力例１： CPU usage statics（CPU 使用量）

Notice	CPU usage reaches: 93	CPU usage statistics

ログ出力例２： FortiGate update succeeded（アップデート完了）

Notice	Fortigate scheduled update fcni=yes fdni=yes ...	FortiGate update succeeded

・ログの保存期間について

メモリ上のログは再起動後残りません。

ディスクログの保存期間は初期設定では 7 日間となっています。期間の変更を行う場合は CLI コンソールで「maximum-log-age」の値を変更してください。0-3650 までの数字が指定できます。

CLI コンソール


```
config log disk setting
        set maximum-log-age 7
end
```

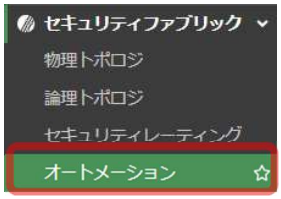
21. FortiGate 管理-オートメーション設定

動作を自動化する機能です。トリガーとアクションの 2 つをまとめたスティッチを作成します。ここでは例として Conserve mode に移行したときに指定のアドレスにメールを送信する設定を行います。

Conserve mode…メモリ使用率が高い時に移行する自己防衛モード

スティッチの作成

(1)　セキュリティファブリック>オートメーションを開きます。



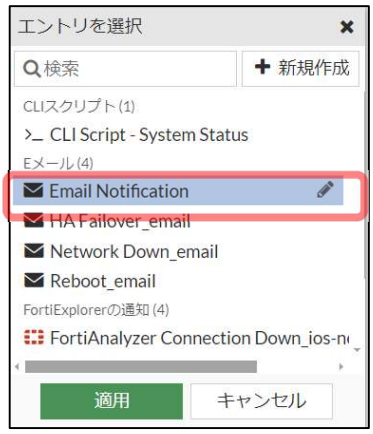
(2)　スティッチを作成します。新規作成を開きます。

(3)　名前を入力し、まずトリガーを追加します

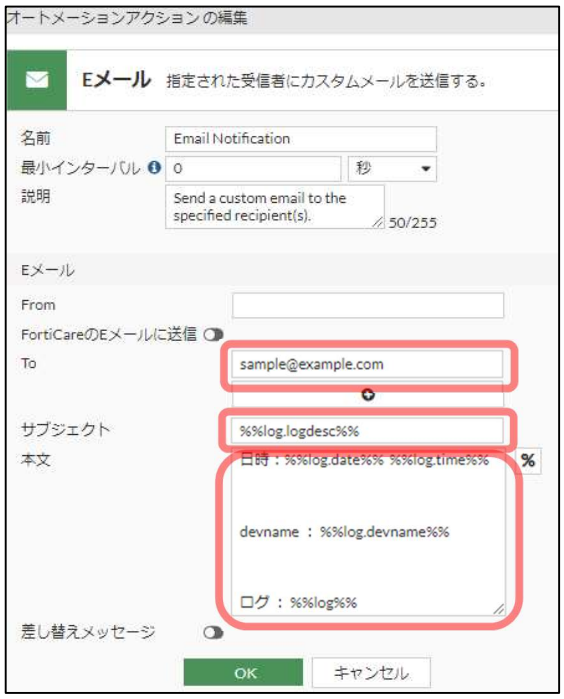
※トリガーを選択します

(3)　その次に「アクションを追加」を選択します

(4)　「Email Nortification」を選択します。



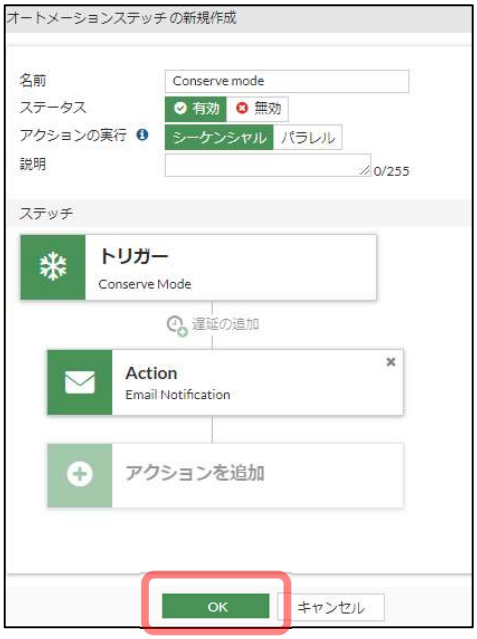
To 宛先、サブジェクト、本文などを指定します。



From は指定が無い場合 DoNotReply@fortinet-notifications.com になります。

※**「FortiCare の E メールに送信」は OFF のままご利用ください。**

(5)完成したら「OK」をクリックします。アクションは複数追加できます。



以上は設定の一例になります。このほかの設定や詳細に関しては Fortinet 社のコミュニティやフォーラム、ドキュメントを参照ください。

22.設定例

ここでは過去にお問い合わせいただいた設定方法についてまとめました。

22-1 設定例 1：国内アドレスのみを許可する

- ファイアウォールポリシーは上から順に評価され、一致したポリシーがあればそのポリシーで通信します。お客様のポリシー構成に応じて、移動が必要な場合はドラッグして順番を変更してください。
- 許可されていない通信は、「暗黙の拒否」ポリシーによって拒否されますので、基本的に拒否ポリシーの作成は必要ありません。（ポリシー構成に応じて拒否ポリシーが必要な場合は設定してください）

許可

（1） 許可ポリシーの作成

国内限定の通信許可設定を行います。事前にプリセットされている「Japan_Segment」（ジオグラフィアドレス）を使用します。

新規ファイアウォールポリシーの作成

「新規作成」>「ファイアウォールポリシー」をクリックすると、ポリシー作成画面が表示されます。

➢ ファイアウォールポリシーの表示

「ポリシー＆オブジェクト」>「ファイアウォールポリシー」をクリックすると、ファイアウォールポリシーが表示されます。

「新規作成」>「ファイアウォールポリシー」をクリックすると、ポリシー作成画面が表示されます。

下記のように設定します。

着信インターフェース	「Internet(port2)」を指定
発信インターフェース	「SuitePRO_NW(port1)」を指定

送信元	「Japan_Segment」
宛先	「SuitePRO_NW」（例）
サービス	RDP
アクション	**許可**
NAT	無効（例）
セキュリティプロファイル	（例 ここでは指定しません。）任意の設定を追加してください

➢ 無効化設定

「このポリシーを有効化」を無効にし、「OK」をクリックして、ポリシー作成を完了します。

➢ ポリシーの確認

ポリシーリストの一番下に「×」が付いた状態（無効化されている）で表示されます。この段階では、まだこのポリシーは反映されていません。

（3）ポリシーの有効化

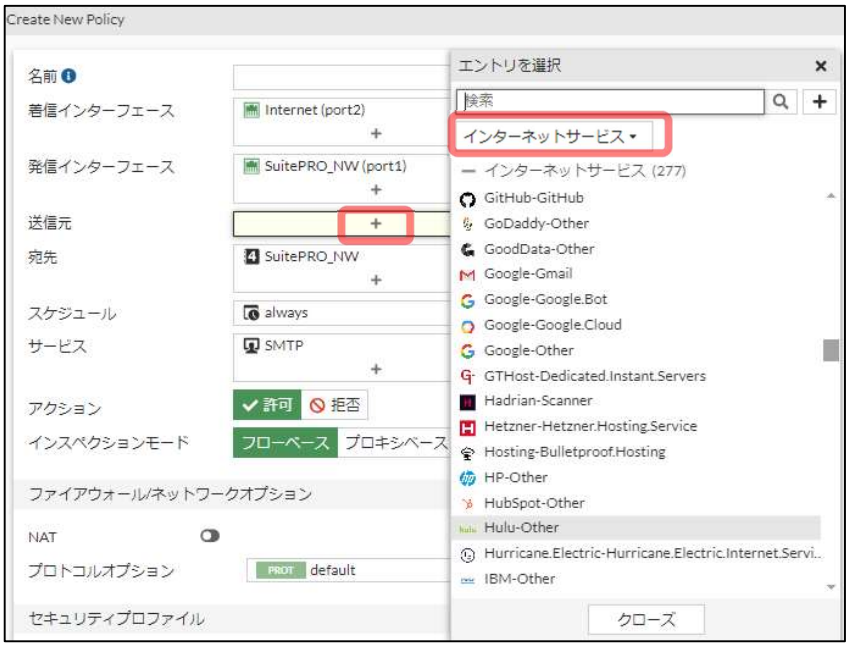
ポリシー位置に問題ないことを確認し、有効化します。

対象ポリシーを選択し、「有効」をクリックし有効化します。ポリシーの設定が反映されます。

22-2 設定例２：インターネット系サービスの許可も追加する場合（ISDB の利用）

日本国内の許可に加えて、インターネット系のサービスも許可したい場合は、インターネットサービスデータベースのを使用します。インターネットサービスの指定はアドレスオブジェクトと一緒に指定できませんので専用にポリシーを作成します。

送信元（もしくは宛先）の選択で「インターネットサービス」を選択し、一覧から追加したいアドレスを選択します。



- インターネットサービスの種類の確認

ポリシー&オブジェクト>インターネットサービスデータベース のメニューを開き、内容を確認してください。宛先。送信元などの方向によって使用できるサービスに違いがあります。

名前	方向	エントリ数	参照
Redhat-Other	両方	970	0
Redhat-Outbound_Email	宛先	970	0
Redhat-RTMP	宛先	970	0
Redhat-SSH	宛先	970	0
Redhat-Web	宛先	970	0
RedShield-RedShield.Cloud	両方	37	0
Restream-Restream.Platform	宛先	1,024	0
RingCentral-RingCentral	宛先	2,353	0
Salesforce-DNS	宛先	10,996	0

23. Q&A

全般

Q:「admin」とは何でしょうか

A: 弊社管理のサポート用アカウントになります。削除や変更はお控えいただくようお願いいたします。削除・変更されますと、お問い合わせの際にお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。

Q: 作業中にブラウザが応答しなくなった。

A: ブラウザをリロードして再読み込みするか、別の種類のブラウザの使用をお試しください。

Q: FortiGate の詳しい仕様を知りたい。

A: 各設定画面の右側に「オンラインガイド」や「コミュニティ」のリンクがあるのでご参照ください。
設定可能な最大値情報は Fortinet の max-values Table でご確認いただけます。
（Model は FortiGate VM1 を選択）
https://docs.fortinet.com/max-value-table

Q: FortiGate の他の設定方法を知りたい。

A: Fortinet の以下のサイトをご確認ください。
https://community.fortinet.com/
https://docs.fortinet.com/product/fortigate/

Q: smtp(25/tcp),pop3(110/tcp),imap(143/tcp),submission(587/tcp)がオープンしているように見えるのですが。

A: Anti Virus でメールを指定している場合、また WAF や Anti SAPM を使用している場合、FortiGate 側で応答を返します。

Q: msrpc(135/tcp)がオープンしているように見える。

A: Anti Virus で MAPI を指定している場合、また、Anti SAPM を使用している場合、FortiGate 側で応答を返します。

Q: ftp(21/tcp)がオープンしているように見える。

A: Anti Virus で FTP を指定している場合、FortiGate 側で応答を返します。

Q: http(80/tcp・8008/tcp)がオープンしているように見える。

A: Anti Virus で HTTP を指定している場合、また WAF を使用している場合、FortiGate 側で応答を返します。

Q: https(443/tcp)がオープンしているように見える。

A: WAF で SSL/SSH インスペクションを使用している場合、FortiGate 側で応答を返します。

Q: xmpp(8010/tcp)がオープンしているように見える。

A: WAF を使用している場合、FortiGate 側で応答を返します。

Q: auth（113/tcp）がクローズされているように見える。

A: 113/TCP に関しては、FortiGate により RST パケットを返します。
パケットドロップの場合、ident 認証（RFC1413）でタイムアウトするまでクエリの再送信が行われてしまうため、FortiGate 側でクローズしています。

Q: 仮想 UTM 下のサーバー間通信は UTM でフィルタされますか。
A: 同サブネット間通信は仮想 UTM を経由せず直接アクセスしますのでフィルタされません。

Q: 古い SSL バージョンの通信がブロックされます。
A: FortiOS7.0.4 から「SSL/SSH インスペクション」は tls-1.1 未満を block する仕様となりました。仮想 UTM イメージ バージョン 7.4.4 はその変更に準じた設定になっています。
古い SSL バージョンを許可する場合はプロファイルの該当プロトコルで「unsupported-ssl-version」を block から allow にするか、「min-allowed-ssl-version」を調整します。(default = TLS 1.1).

```
------------------------------------------------------------
config firewall ssl-ssh-profile
    edit <name>
        config SSL（※プロトコルが SSL の場合）
            set inspect-all deep-inspection
            set unsupported-ssl-version {allow | block}
            set min-allowed-ssl-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | tls-1.3}
        end
    next
end
------------------------------------------------------------
```

コメント欄に"Read-only～"とあるプロファイルは編集できません。新規作成で新たにプロファイルを作成するか、GUI で既存プロファイルをクローンしてから新しいプロファイルを編集し、ファイアウォールポリシーにセットしてください。
「firewall ssl-ssh-profile」 Fortinet: Home> FortiGate / FortiOS 7.4.4 >CLI Reference
https://docs.fortinet.com/document/fortigate/7.4.4/cli-reference/116695140/config-firewall-ssl-ssh-profile

Q: FortiOS をアップグレードした後、Web サイトがブロックされるようになりました。
「SSL/SSH インスペクション」の既存プロファイル設定において FortiGate がアクセス先サーバーに対して
証明書の審査を実施し、この審査でエラーが発生するとトラフィックをブロックする仕様が FortiOS7.0.0 から追加されました。
このブロックを回避するには対象プロファイルの「cert-probe-failure」 のアクションを「allow」に変更します。

```
------------------------------------------------------------
config firewall ssl-ssh-profile
    edit <certificate profile name>
        config <protocol name>
            set cert-probe-failure   {allow | block}
        end
    next
end
------------------------------------------------------------
```

初期状態で用意されているプロファイル「certificate-inspection」「custom-deep-inspection」「deep-inspection」の https プロトコルは block の設定になっています。

コメント欄に"Read-only～"とあるプロファイルは編集できません。新規作成で新たにプロファイルを作成するか、GUI で既存プロファイルをクローンしてから新しいプロファイルを編集し、ファイアウォールポリシーにセットしてください。
「firewall ssl-ssh-profile」 Fortinet: Home> FortiGate / FortiOS 7.0.0 >CLI Reference
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-allow-HTTPS-port-443-traffic-when/ta-p/200844

ファイアウォールアドレス

Q: ポリシー＆オブジェクト内のアドレスを削除できない。
A: そのアドレスをグループやポリシーで使用中の場合は削除できません。使用を解除してから削除してください。アドレスグループ、サービス、サービスグループについても同様です。

ファイアウォールポリシー

Q: ポリシーの編集で、サービスを「HTTP」から「HTTPS」に変更したが、編集後に確認すると、「HTTP」と「HTTPS」の両方が指定されている。
A: ポリシーの編集から、サービスを変更した場合、「変更」ではなく「追加」となるため、名前の右側にある「×」をクリックしてエントリから除外してください。ポリシーのほかの項目、またアドレスグループ、サービスグループも同様です。

Q: ポリシーが勝手に動いた。
A: ポリシーは、ドラッグ＆ドロップで順番を変更することができます。その順番によって優先順位が変更されるため、優先順位を変更するとき以外はポリシーを動かさないように注意してください。

Q: ポリシーで通信を拒否したはずなのに、拒否されない。
A: ポリシーは上から順番に評価されます。設定した拒否ポリシーの上側に許可ポリシーがある場合、その許可ポリシーが優先されます。優先順位をご確認ください。

Q: マニュアルのように、ポリシーに Internet→SuitePRO_NW の表示がない。
A: ポリシー上部の右側に、「インタフェースペア表示」、「シーケンス順」のボタンがあります。「インタフェースペア表示」をクリックすると、マニュアルと同じ見え方になります。

Q: マニュアルよりも、ポリシーの項目が少ない。
A: ポリシー上部にある「ID」「名前」の行で右クリックをすると、カラムを選択できます。表示させたいカラムを選択し、下から二番目の「適用」をクリックさせるとポリシーの表示項目が増えます。

Q: セキュリティ検査を行ったが、HTTPS 通信で IPS や WAF で検知が検知されない。
A: HTTPS などの暗号化通信を監視するには Web サイトで使用しているキーペアをポリシーに設定する必要があります。
「証明書のインポート」を実施した後「セキュリティ SSL/SSH インスペクション」を実施してポリシーに設定を行ってください。

DoS ポリシー

Q: 着信インターフェースとは
A: ポリシーを適用するインターフェースになります。着信インターフェースによって対象の通信が異なります。
「Internet」・・・インターネットからの通信（Inbound）
「SuitePRO_NW」の場合・・・・仮想専用サーバーからの通信（Outbound）

Q:「しきい値」をどう決めたらよいのか

A: ある程度のおおまかな値を目安として設定し、一定期間モニターされることで検知状況の把握ができますので参考にされてください。ロギングを ON にした状態でアクションに「モニタ」を適用します。検知された結果はアノマリログで確認できます。

証明書エラー

Q: UTM 管理サイトへアクセスしたときに証明書のエラーが表示される。

A: お客さまにて UTM 管理サイト用のドメインと、そのドメインの証明書を取得してください。
また、ドメインの A レコードは「UTM 管理サイト」のドメインと同じ IP アドレスを指定します。

① ドメイン取得（FortiGate で使用するため、サーバーとは別に準備する）
② DNS 登録
A レコードで FG 管理サイトの IP アドレスを指定（例：fvd1111.fg.arena.ne.jp）
③ 取得したドメインの証明書購入
④ FortiGate：証明書インポート ※手順「証明書のインポート」参照
⑤ FortiGate：証明書設定
「システム」>「設定」メニュー
「管理者設定」>「HTTPS サーバー証明書」にて対象の証明書を選択し、適用

WAF（Web Application firewall）

Q: ファイアウォール設定画面上に WAF（Web アプリケーションファイアウォール）が表示されない

A:ポリシーのインスペクションモードを「プロキシベース」に変更すると表示されます。

Q: 設定画面上に WAF が表示されない（初期 OS6.0.3 をご利用のお客様）

A: FortiOS6.2 以降の環境では WAF の設定を GUI 上で表示させるために設定が必要となります。

(1)インスペクションモードの表示（FortiOS 7.2 以上のみ）
画面右上に並んでいるアイコンの左端の「CLI コンソール」をクリックしコンソールを開きます。

以下のコマンドを実行して閉じます。

```
-------------------------------------------------------------
  config system settings
       set gui-proxy-inspection enable
  end
-------------------------------------------------------------
```

(2)Web アプリケーションファイアウォールの有効化
システム>表示機能設定>Web アプリケーションファイアウォール
→有効であること。無効の場合は有効にして OK をクリックする

(3)インスペクションモードの変更
ポリシー＆オブジェクト＞ファイアウォールポリシー
WAF を設定したいポリシーを選択して、編集をクリック
インスペクションモードを「プロキシモード」に設定する。
→Web アプリケーションファイアウォールが表示されますので、
ここで対象のプロファイルを選択してください。

SSLVPN

Q: SSLVPN の設定メニューが表示されない

A: FortiOS7.4.1 から SSL VPN は GUI で非表示になりました。GUI 上に表示させるためには CLI コンソールから以下の設定を行って下さい。

```
-------------------------------------------------------------
  config system settings
        set gui-sslvpn enable
  end
-------------------------------------------------------------
```

Update SSL VPN default behavior and visibility in the GUI

https://docs.fortinet.com/document/fortigate/7.4.0/new-features/233856/update-ssl-vpn-default-behavior-and-visibility-in-the-gui-7-4-1

オートメーション

Q: 「Email Notification」内にある「FortiCare の E メールに送信」に記載のアドレスはどこのものですか。

A: 製品登録に使用しているメールアドレスになります。こちらの設定は OFF にしてご利用ください。

24. 提供 仕様

24-1.仮想 UTM OS イメージの違い

初期 OS	FortiOS 6.0.3 2017/04 以降インストール	FortiOS 7.4.4 2024/11/08 以降インストール
お客さまアカウントのプロファイル	prof_admin ポリシーなどの設定変更が可能	super_admin すべての権限を持ちます ※プロファイルが変化したことにより「admin」アカウントも表示されるようになります。このアカウントは弊社管理のサポート用になります。削除や変更はお控えいただくようお願い致します。削除・変更されますと、お問い合わせの際にお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。
お客様アカウントの形式	アカウント名@UTM 名	アカウント名-UTM 名

- そのほかの FortiGate の設定や仕様に関しては FortiOS の仕様に準じます
- 弊社変更内容については「24-2 イメージ初期設定」をご参照ください。
- 「FortiOS 6.0.3」のお客さまアカウントのプロファイルを「prof_admin」から「super_admin」に変更することも可能です。
  ※ご希望の場合は、仮想 UTM のホスト名情報を添えてテクニカルサポートまでお問い合わせください。OS インストール時に作成したアカウントが変更対象となります。

24-2 イメージ初期設定

イメージ バージョン 7.4.4 の初期設定です。他の設定は ForiOS7.4.4 の初期設定に準じます。
これらの初期設定は CLI コンソールなどで変更可能です。

Home >FortiGate / FortiOS 7.4.4 >CLI Reference
https://docs.fortinet.com/document/fortigate/7.4.4/cli-reference/84566/fortios-cli-reference

config system global	
management-port-use-admin-sport	disable
proxy-auth-timeout	5
refresh	5
sys-perf-log-interval	0
timezone	Asia/Tokyo

config system settings	
default-voip-alg-mode	kernel-helper-based
gui-load-balance	enable
gui-spamfilter	enable
gui-wireless-controller	disable
gui-wan-load-balancing	disable
gui-waf-profile enable	enable
gui-allow-unnamed-policy	enable
gui-multiple-interface-policy	enable

config system ntp	
syncinterval	10

config system automation-action **edit "Email Notification"**	
forticare-email	disable

config report layout	
schedule-type	demand

config vpn ssl settings	
port	4443

config system admin	
admin	※弊社管理のサポート用アカウントになります。削除や管理者権限を変更はお控えいただくようお願い致します。削除されますとお問い合わせの際にお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。

config system session-ttl

```
 set default 600
     config port
          edit 1
               set protocol 17
               set timeout 10
               set start-port 53
               set end-port 53
          next
     end
end
```

以下オブジェクトとして追加しています。

FW ポリシー　オブジェクト

アドレス	
OfficeA	203.0.113.0（掲示用アドレス）
OfficeB	198.51.100.5（掲示用アドレス）
Japan_Segment	日本アドレス（タイプ geography）
SuitePRO_NW	仮想 UTM ネットワーク/29
NTTPC_Port_Monitoring	203.138.84.18
アドレスグループ	
Office	OfficeA,OfficeB
サービスグループ	
MAIL	POP3/IMAP/SMTP/Submission

セキュリティプロファイル

IPS プロファイル	
	IPS_Mail
	IPS_DNS
	IPS_HTTP
	IPS_HTTPS
アンチウイルスプロファイル	
	AV_MAIL
	AV_FTP
アンチスパムプロファイル	
	ANTISPAM
Web Application firewall プロファイル	
	default
セキュリティプロファイル	
	custom-default

FW ポリシー（1 以外すべて無効化）

ID	名前	接続元	宛先	サービス	アクション	IPS	SSL インスペクション	プロキシ
1	preset1	SuitePRO_NW	All	All	許可	なし	no-inspection	フロー
2	preset1	NTTPC_Port_Monitoring	SuitePRO_NW	All	許可	なし	no-inspection	フロー
3	preset2	Office_Group	SuitePRO_NW	SSH	許可	なし	no-inspection	フロー
4	preset3	Office_Group	SuitePRO_NW	RDP	許可	なし	no-inspection	フロー
5	preset4	All	SuitePRO_NW	DNS	許可	なし	no-inspection	フロー
6	preset5	All	SuitePRO_NW	HTTP	許可	なし	no-inspection	フロー
7	preset6	All	SuitePRO_NW	HTTPS	許可	なし	no-inspection	プロキシ
8	preset7	All	SuitePRO_NW	MAIL	許可	なし	no-inspection	プロキシ

DoS ポリシー（すべて有効化）

ID	名前	接続元	宛先	サービス
1	preset1	port1	All	All
2	preset2	port2	All	All