ホワイトクラウド

ASPIRE

ホワイトクラウド ASPIRE

IPsec VPN 接続構成ガイド

RTX1210 を用いた接続構成例

ソフトバンク 株式会社

注意事項

本資料内の記載は、飽くまでも情報提供のみを目的としております。明示、黙示、または法令に基づく想定に関わらず、これらの情報についてソフトバンク株式会社はいかなる責任も負わないものとします。本資料内に記載された社名・製品名は、各社の商標、または登録商標です。

更新履歴

版	更新日	更新者	更新内容
初版	2016/11/8	ソフトバンク 株式会社	初版作成

SoftBank

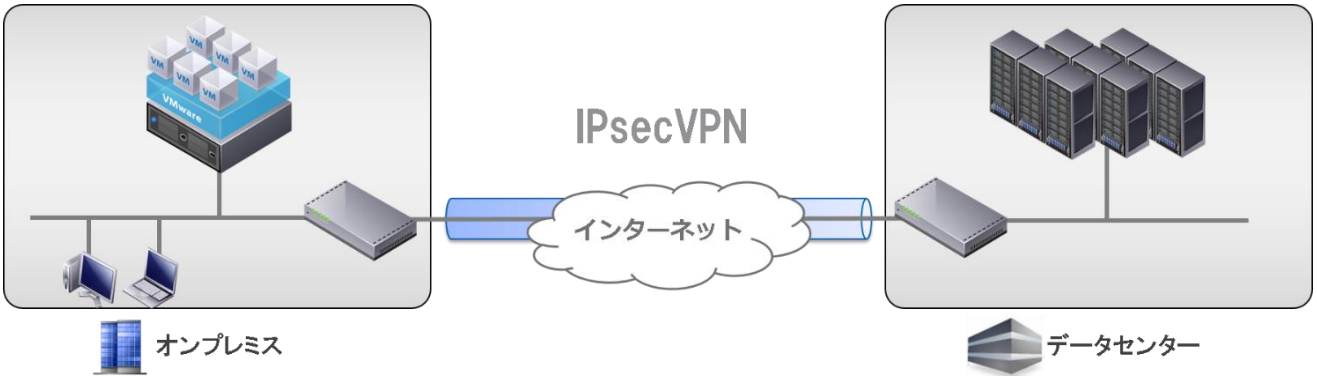
目次

1. ホワイトクラウド ASPIRE の IPsec VPN 機能概要 5
1.1. IPsec VPN について 5
1.2. ホワイトクラウド ASPIRE の IPsec VPN 機能 5
2. RTX1210 とホワイトクラウド ASPIRE の接続構成概要 6
2.1. 本資料でご紹介する RTX1210 を用いた構成 6
2.2. 論理構成 7
3. 構成手順 8
3.1. 設定前の状態について 8
3.1.1. オンプレミス側 RTX1210 の設定 8
3.1.2. ホワイトクラウド ASPIRE 側の設定 9
3.2. RTX1210 の VPN 設定 10
3.2.1. IPsecVPN 設定用コマンドを作成 11
3.2.1.1. トンネル用 IP フィルタの設定コマンド(任意) 11
3.2.1.2. IPsecVPN の設定コマンド 12
3.2.1.3. ルーティングの設定コマンド 13
3.2.1.4. WAN インターフェース用 IP フィルタの設定 14
3.2.1.5. NAT の設定 14
3.3. ホワイトクラウド ASPIRE の VPN 設定 17
3.3.1. VPN 設定 17
3.3.2. ファイアウォール設定 20
3.4. VPN 接続後の通信確認 24
3.4.1. ホワイトクラウド ASPIRE セルフサービスポータルから確認 24
3.4.2. YAMAHA RTX1210 から確認 25
3.4.3. 仮想マシンから確認 27
3.5. 参考資料 28
3.5.1. 参考:本設定での RTX1210Config設定(抜粋) 28
3.5.2. 参考:RTX1210 を用いて複数セグメント間で IPsec VPN を設定する場合 30
3.5.2.1. 複数セグメント間での IPsec VPN 設定 (RTX1210) 33
3.5.2.2. 複数セグメント間での IPsec VPN 設定 (ホワイトクラウド ASPIRE) 35
3.5.2.3. VPN 接続後の通信確認時の注意点 36

1. ホワイトクラウド ASPIRE の IPsec VPN 機能概要

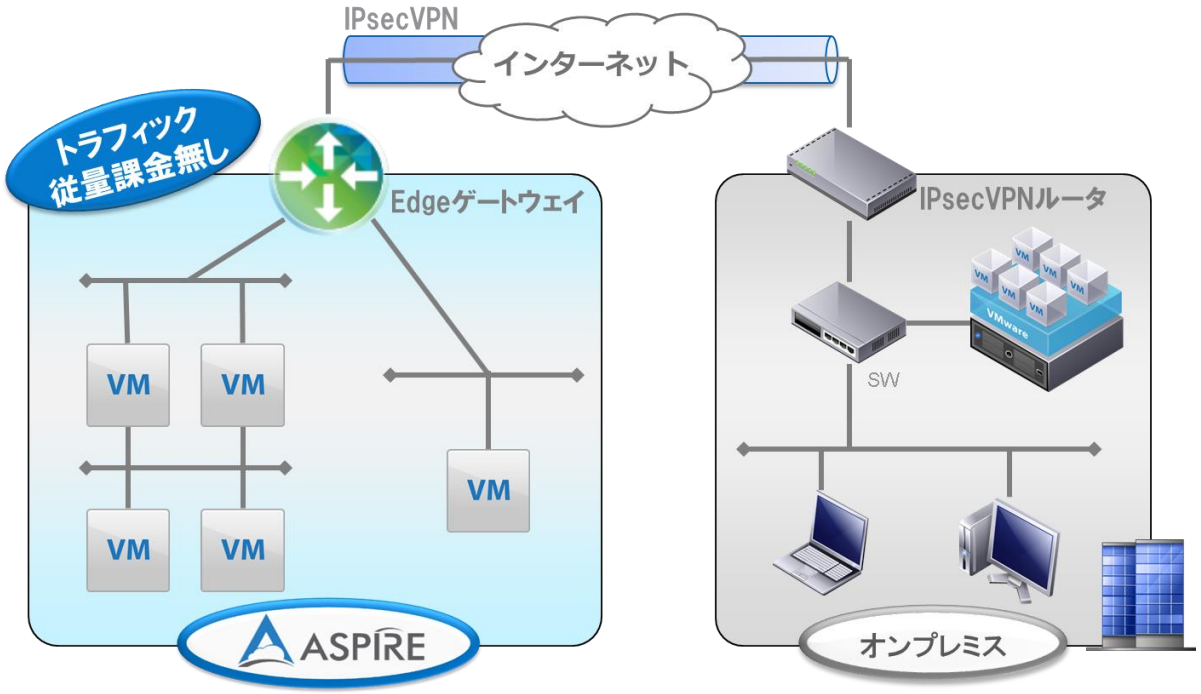
1.1. IPsec VPN について

IPsec (Security Architecture for Internet Protocol) は、IP 通信を暗号化することによって内容の秘匿と改ざん防止を実現するプロトコルです。この IPsec によって、異なる場所にあるネットワークやノードの間を、あたかも専用の回線を引いたかのように接続する技術が IPsec VPN です。この技術によって、重要性の高いデータ通信を安全に行うことができます。



1.2. ホワイトクラウド ASPIRE の IPsec VPN 機能

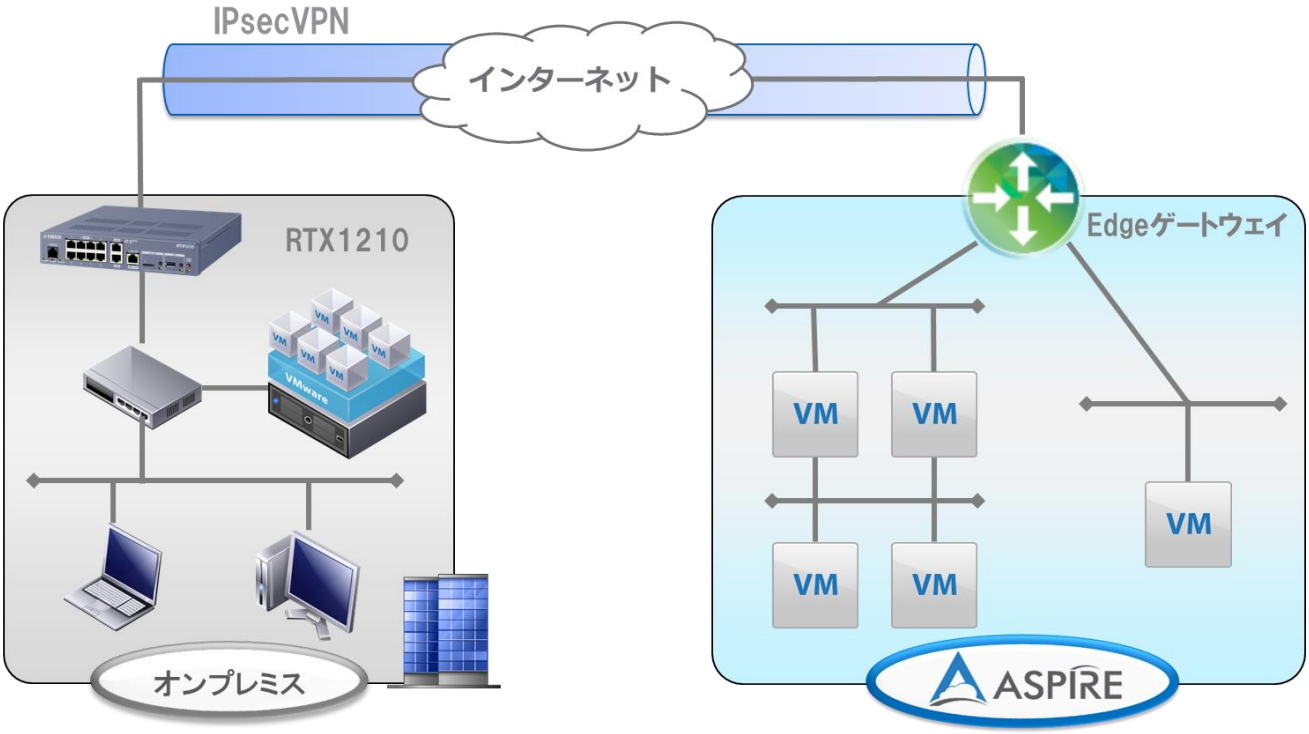
データセンタやオフィスなどの拠点との間で安全な通信を行うために、ホワイトクラウド ASPIRE は IPsec VPN 機能を標準搭載しています。ホワイトクラウド ASPIRE からインターネットへの接続に用いる Edge ゲートウェイが IPsec VPN 機能を提供します。IPsec VPN 接続機能を持つ拠点側の機器やソフトウェア等と Edge ゲートウェイの間で IPsec VPN による通信を行うことが可能です。



2. RTX1210 とホワイトクラウド ASPIRE の接続構成概要

2.1. 本資料でご紹介する RTX1210 を用いた構成

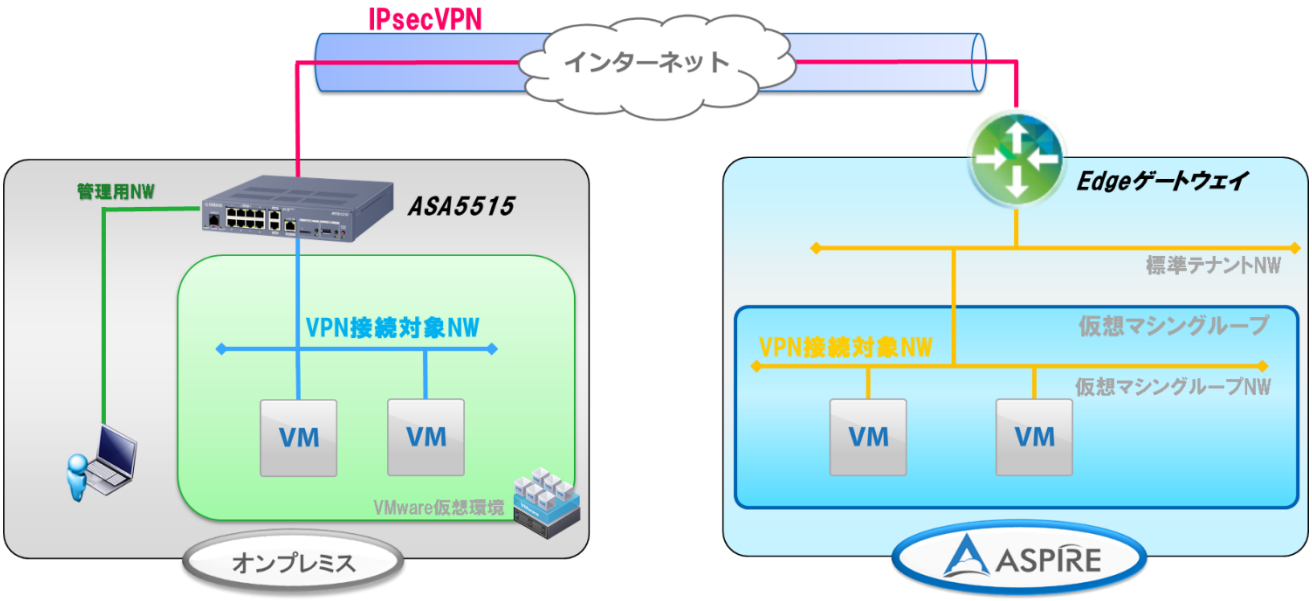
本資料では拠点側に RTX1210 を設置し、ホワイトクラウド ASPIRE の Edge ゲートウェイとの間を IPsec VPN で接続する設定例をご紹介します。



YAMAHA 製品の詳細に関しては、公式 Web サイトをご覧ください。
http://jp.yamaha.com/products/network/routers/

2.2. 論理構成

オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象ネットワーク間で通信できるように IPsec VPN を接続します。



次項より記載する構成手順は、上図のうち IPsec VPN 以外の部分が構成された状態を前提としております。本資料の作成にあたり使用した機器、OS バージョンは、下記となります。

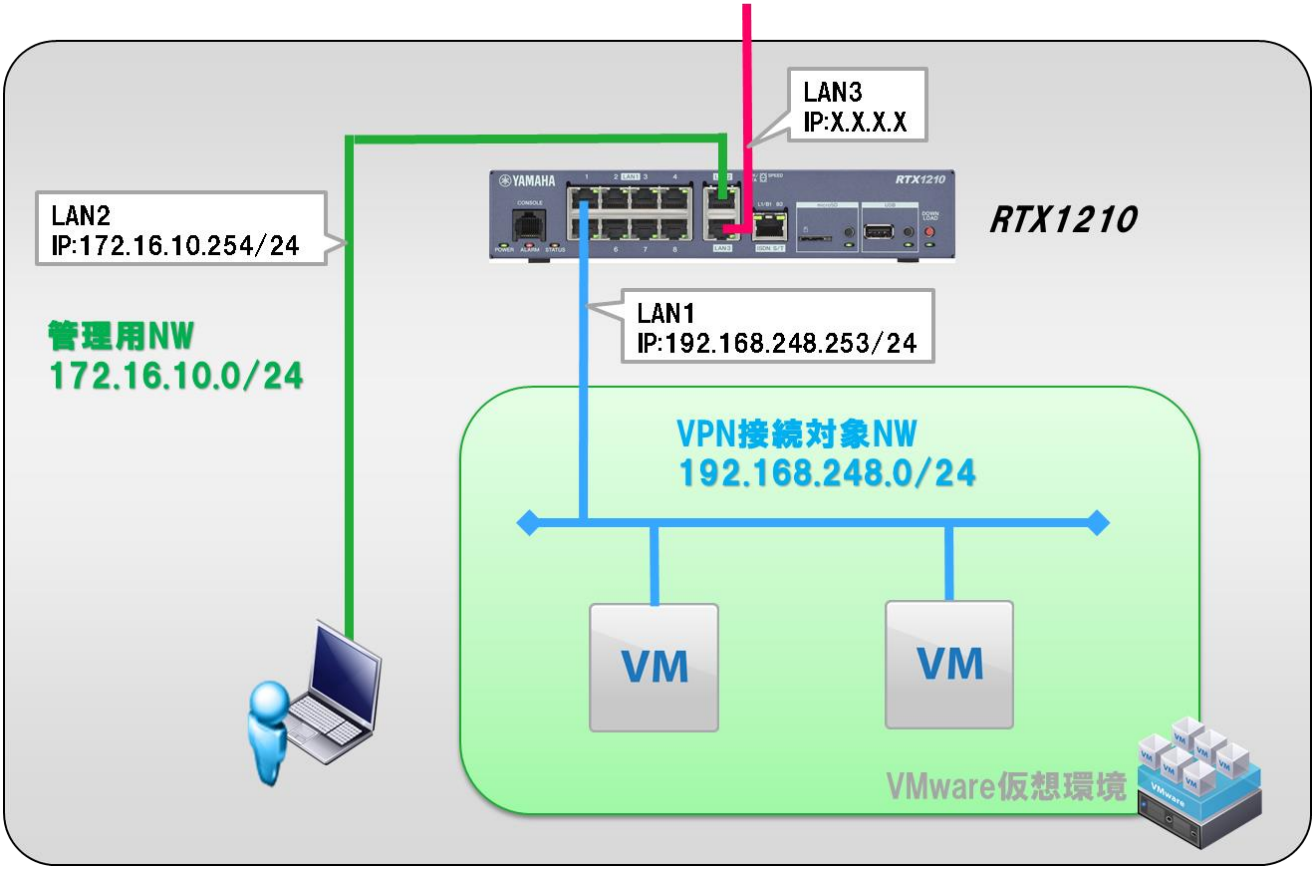
＜ RTX1210 ＞
機器:YAMAHA RTX1210
Firmware Version:Rev.14.01.14

3. 構成手順

3.1. 設定前の状態について

VPN 設定前のオンプレミスおよびホワイトクラウド ASPIRE それぞれの状態を示します。

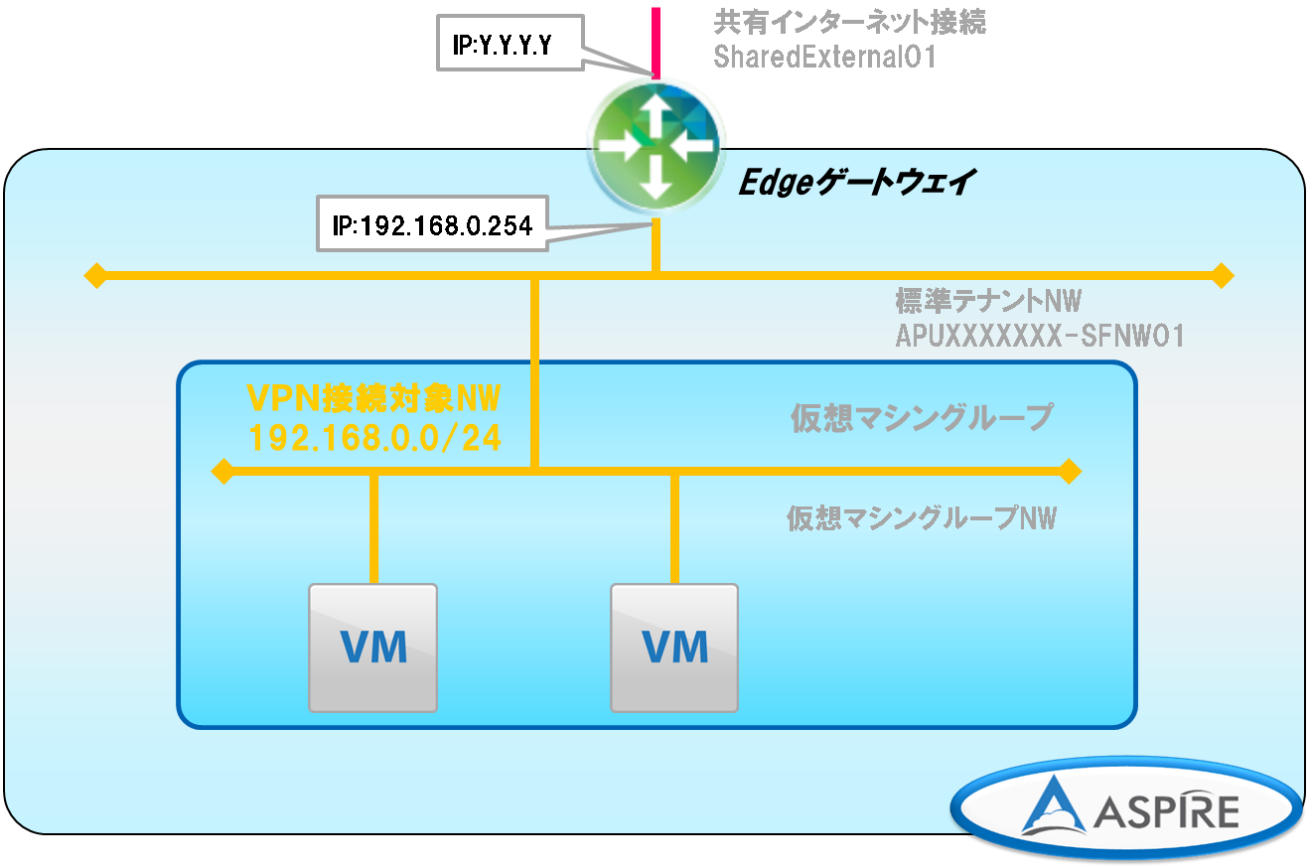
3.1.1. オンプレミス側 RTX1210 の設定



RTX1210

- ACL は WAN インターフェースへの設定のみ
- NAT は内→外のみ設定(NAPT)
- デフォルト GW は WAN 側に設定
- インターフェースは次の 3 つを使用
  - LAN3（WAN）IP アドレス ：X.X.X.X
  - LAN1（VPN 接続対象 NW）IP アドレス ： 192.168.248.253/24
  - LAN2（管理用 NW）

3.1.2. ホワイトクラウド ASPIRE 側の設定



Edge ゲートウェイ

- ファイアウォールではルールの設定が無い通信は全て拒否する
- NAT は内→外のみ（NAPT）
- VPN 接続対象 NW はデフォルトで存在する標準テナントNWを利用する
- インターフェースは次の2つを使用
  - Edge ゲートウェイ（WAN）IP アドレス：Y. Y. Y. Y
  - Edge ゲートウェイ（VPN 接続対象 NW）IP アドレス： 192.168.0.254/24

3.2. RTX1210 の VPN 設定

RTX1210 の VPN 設定手順を記します。大まかなステップは次のとおりです。

① IPsecVPN の設定用コマンドを作成
② WebGUI より①で作成したコマンドを実行

※前ページに記載された VPN 設定前の状態までの初期セットアップ手順は省略しております。
初期セットアップ手順はメーカー公開の各種ドキュメントをご参照ください。
RT シリーズのマニュアル配布
http://www.rtpro.yamaha.co.jp/RT/manual.html
Web GUI 操作マニュアル
http://www.rtpro.yamaha.co.jp/RT/manual/rtx1210/Webgui.pdf
※本資料では、WebGUI よりコマンドを実行し設定する方法を記載しております。
直接 CLI より設定される場合は、巻末に参考 Config を記載しておりますのでそちらをご確認ください。
本資料で IPsec VPN の設定に利用する VPN パラメータを下記に示します。

パラメータ	オンプレミス RTX1210	ホワイトクラウド　ASPIRE Edgeゲートウェイ
Local Network	192.168.248.0/24	192.168.0.0/24
Remote Network	192.168.0.0/24	192.168.248.0/24
Local ID	-	Y.Y.Y.Y
Remote ID	-	X.X.X.X
Remote IP	Y.Y.Y.Y	X.X.X.X
IKE version	V1	設定変更不可
認証方式	Pre-shared Key	設定変更不可
共有キー／Pre-shared Key	VpnaccessforASPIRE1vpnaccessforASPIRE1	VpnaccessforASPIRE1vpnaccessforASPIRE1
交換モード	Main mode	設定変更不可
暗号化・Hashアルゴリズム	AES256 / SHA-1	AES256 / SHA-1
Diffie-Hellman Group	group 2 (MODP1024 bits)	設定変更不可
PFS	On	設定変更不可
IKE SA Lifetime	28800 (no kbytes rekeying)	設定変更不可
IPsec SA Lifetime	3600 (no kbytes rekeying)	設定変更不可

※備考

・IKE フェーズ 1,2 では同じアルゴリズムを使用 （本資料では AES256 を利用※）
・オンプレミス側の NW 機器でホワイトクラウド　ASPIRE の IPsec VPN 仕様に沿ったパラメータを設定する
・ホワイトクラウド　ASPIRE 側は、ポリシーベース VPN のみ利用可能
※ご利用環境においてパケットロスが多発するようであれば AES128 での設定もご検討ください。

3.2.1. IPsecVPN 設定用コマンドを作成

以下の順番でコマンドを作成します。

1. トンネル用 IP フィルタの設定コマンド(任意)
2. IPsecVPN の設定コマンド
3. ルーティングの設定コマンド
4. WAN インターフェース用 IP フィルタの設定コマンド(※)
5. NAT の設定コナンド(※)

※必要に応じて作成

3.2.1.1. トンネル用 IP フィルタの設定コマンド(任意)

RTX1210 で IPsecVPN を経由する通信を制御したい場合は、トンネル用の IP フィルタ設定コマンドを作成します。

IP フィルタコマンド

ip filter	[filter_num]	[pass_reject]	[src_addr]	[dest_addr]	[protocol]	[src_port_list]	[dest_port_list]
固定値	重複しない 任意の値	pass/reject	送信元 アドレス	送信先 アドレス	任意 ※	任意 ※	任意 ※

※省略した場合は＊(ANY)となる

設定例 (本資料での VPN 対象 NW 通信のみを許可)

```
ip filter 101 pass 192.168.0.0/24 192.168.248.0/24 * * *
ip filter 102 pass 192.168.248.0/24 192.168.0.0/24 * * *
```

コマンドの詳細は下記をご確認ください。

9.1.8 IP パケットのフィルタの設定

http://www.rtpro.yamaha.co.jp/RT/manual/rt-common/ip/ip_filter.html

3.2.1.2. IPsecVPN の設定コマンド

ホワイトクラウド ASPIRE への IPsecVPN 設定コマンドを作成します。

IPsecVPN 設定に必要なコマンド

コマンド	概要	設定するパラメータ
tunnel select	トンネルインタフェース番号を選択	任意
description tunnel	トンネルインターフェースにメモを設定	任意
ipsec tunnel	使用する SA のポリシーの設定	使用する SA のポリシーの設定
ipsec sa policy	SA のポリシーの定義	暗号化方式、ローカルID(オンプレミス VPN対象NW)、リモートID(ホワイトクラウドASPIRE VPN対象NW)
ipsec ike always-on	常時接続モードの設定	on
ipsec ike duration ipsec-sa	IPsec SAの寿命の設定	3600
ipsec ike duration ike-sa	ISAKMP SAの寿命の設定	28800
ipsec ike encryption	IKE が用いる暗号アルゴリズムの設定	aes256-cbc
ipsec ike group	IKE が用いるグループの設定	modp1024
ipsec ike hash	IKE が用いるハッシュアルゴリズムの設定	sha
ipsec ike local address	RTX1210のWAN側IPアドレスの設定	X.X.X.X
ipsec ike pfs	PFS を用いるか否かの設定	on
ipsec ike pre-shared-key	Pre-shared Keyの設定	VpnaccessforASPIRE1vpnaccessforASPIRE1
ipsec ike remote address	VPN対向先のグローバルアドレスを設定	Y.Y.Y.Y
ipsec auto refresh	IKE の鍵交換を始動するか否かの設定	on
ip tunnel secure filter in	フィルタリングによるセキュリティの設定	任意
ip tunnel secure filter out	フィルタリングによるセキュリティの設定	任意
ip tunnel tcp mss limit	TCP セッションの MSS 制限の設定	auto
tunnel	有効／無効の設定	enable

設定例(暗号化アルゴリズム aes256 を利用)

```
tunnel select 1
 description tunnel Tunnel1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.0.0/24
  ipsec ike always-on 1 on
  ipsec ike duration ipsec-sa 1 3600
  ipsec ike duration ike-sa 1 28800
  ipsec ike encryption 1 aes256-cbc
  ipsec ike group 1 modp1024
  ipsec ike hash 1 sha
  ipsec ike local address 1 X.X.X.X
  ipsec ike local id 1 192.168.248.0/24
```

```
 ipsec ike pfs 1 on
 ipsec ike pre-shared-key 1 text VpnaccessforASPIRE1vpnaccessforASPIRE1
 ipsec ike remote address 1 Y.Y.Y.Y
 ipsec ike remote id 1 192.168.0.0/24
 ipsec auto refresh 1 on
ip tunnel secure filter in 101
ip tunnel secure filter out 102
ip tunnel tcp mss limit auto
tunnel enable 1
```

※ipsec ike negotiate-strictly コマンドについて

本資料では ipsec ike negotiate-strictly コマンドをデフォルトのまま設定しています。
デフォルトの設定では ipsec ike negotiate-strictly コマンドは off になっています。
必要に応じて設定を変更してください。
ipsec ike negotiate-strictly コマンドの詳細については下記 URL よりコマンドリファレンスをご確認ください。

18.10 設定が異なる場合に鍵交換を拒否するか否かの設定
http://www.rtpro.yamaha.co.jp/RT/manual/rt-common/ipsec/ipsec_ike_negotiate-strictly.html

他の IPsecVPN コマンドの詳細は下記をご確認ください。
Yamaha ルーターシリーズ コマンドリファレンス
http://www.rtpro.yamaha.co.jp/RT/manual/rt-common/

3.2.1.3. ルーティングの設定コマンド

ホワイトクラウド ASPIRE の VPN 対象 NW へのルーティング設定コマンドを作成します。

ルーティング設定コマンド（トンネルインターフェース）

ip route	[network]	gateway	tunnel	[tunnel_num]
固定値	宛先ネットワーク	固定値	固定値	トンネルインターフェース番号

設定例

```
ip route 192.168.0.0/24 gateway tunnel 1
```

コマンドの詳細は下記をご確認ください。
9.1.7 IP の静的経路情報の設定
http://www.rtpro.yamaha.co.jp/RT/manual/rt-common/ip/ip_route.html

3.2.1.4. WAN インターフェース用 IP フィルタの設定

WAN インターフェースに IPsecVPN の通信を許可する IP フィルタを設定します。

必要となるフィルタ

IKE（UDP：ポート 500 番）、esp パケットを許可

※すでに同様の設定がされている場合、本設定は不要です。

設定例

```
ip filter 1 pass * 192.168.248.253 udp * 500
ip filter 3 pass * * esp * *
ip lan3 secure filter in 1 2 3 2000
```

3.2.1.5. NAT の設定

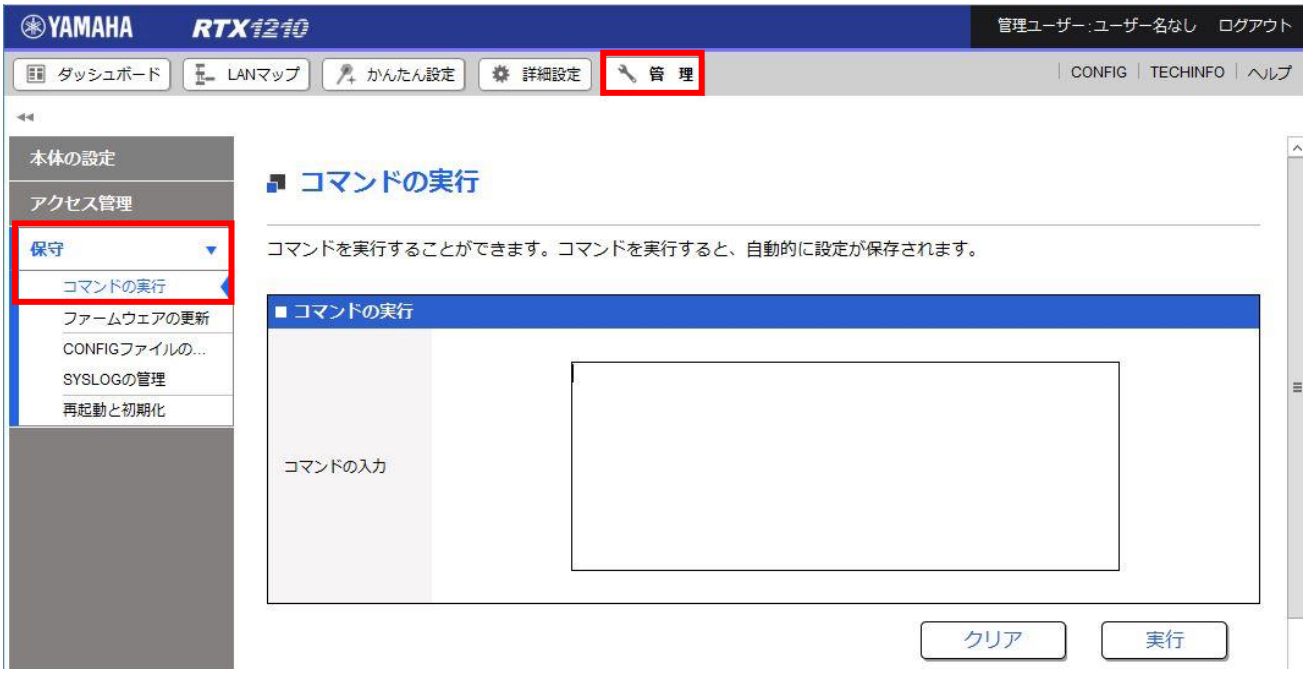
WAN インターフェースに IPsecVPN の通信を可能にする NAT を設定します。
この設定によりルータが IKE のパケット、ESP のパケットを送受信できるようになります。
※すでに同様の設定がされている場合、本設定は不要です。

設定例

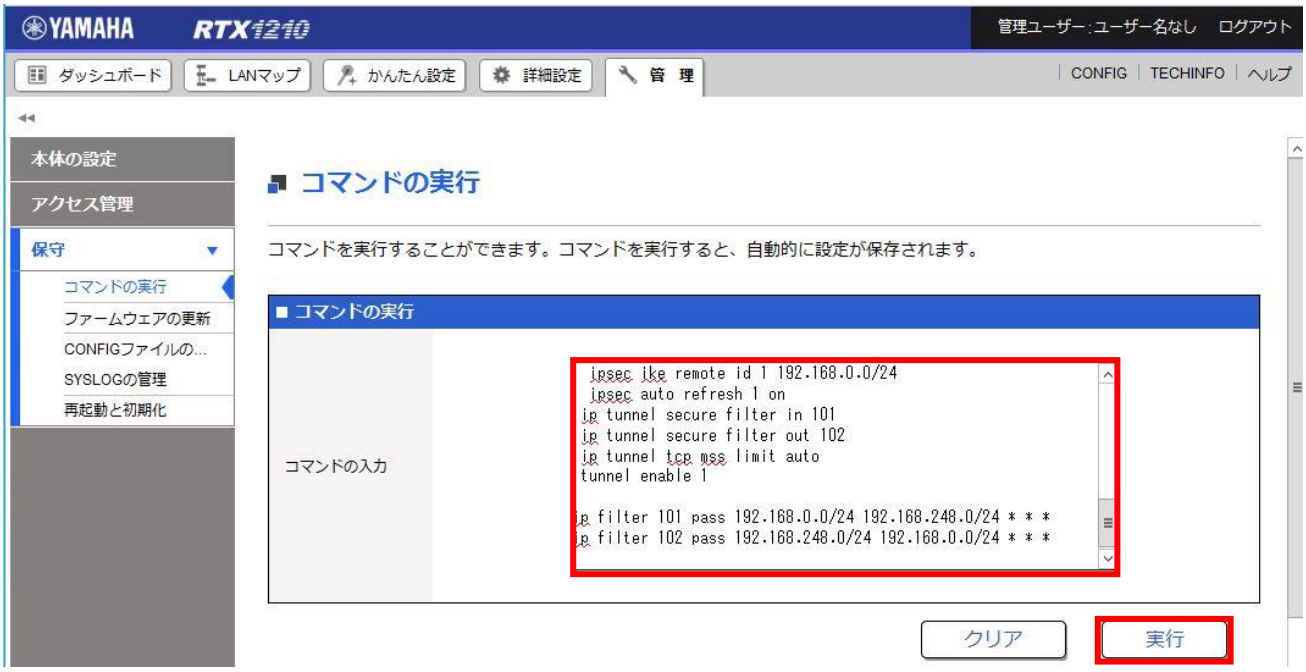
```
nat descriptor type 1 masquerade
nat descriptor address outer 1 X.X.X.X
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 X.X.X.X udp 500
nat descriptor masquerade static 1 3 X.X.X.X esp
```

3.2.2. WebGUI より作成した設定コマンドを実行

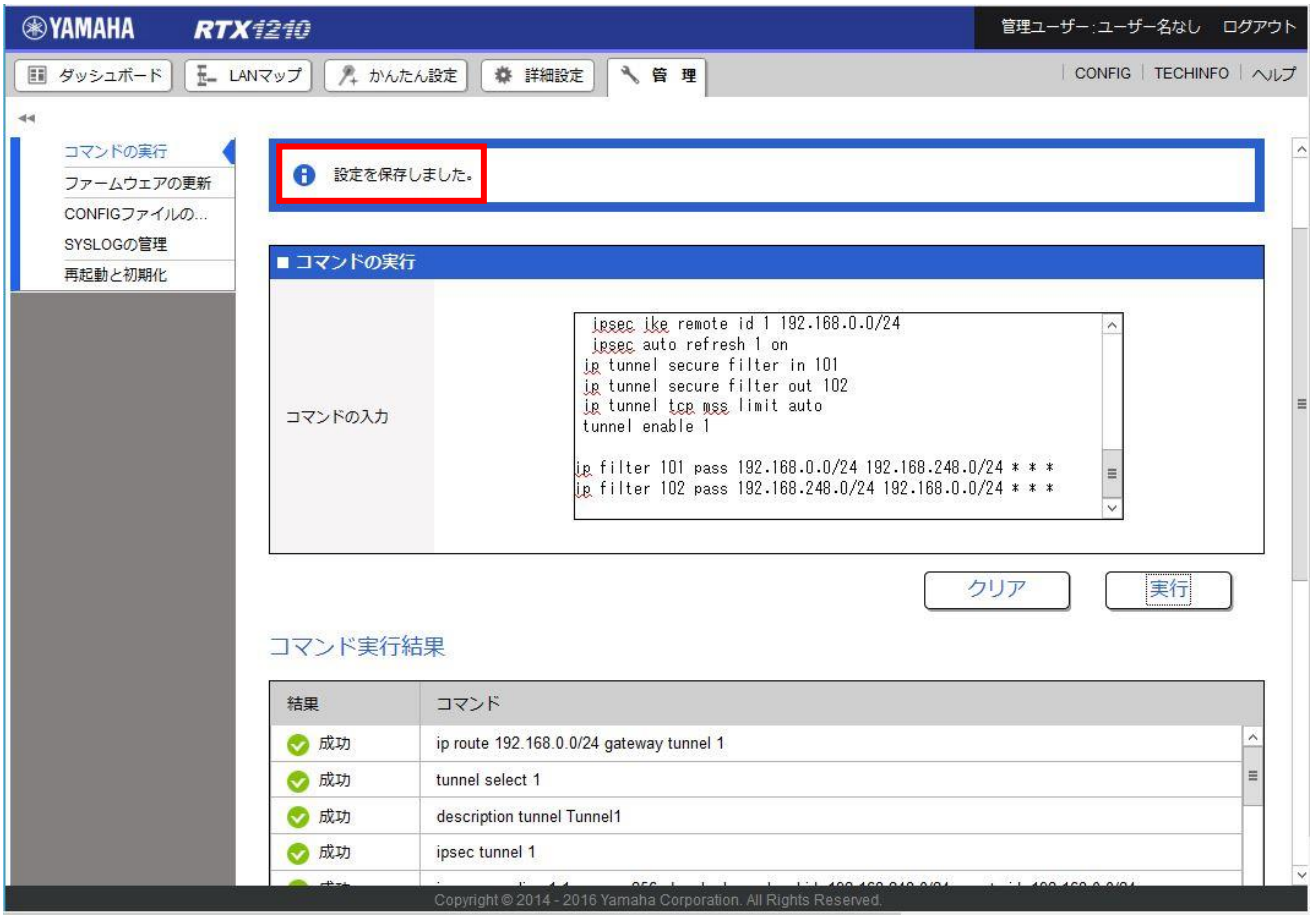
（1）. WebGUI にアクセスします。「管理」 より 「保守」 、 「コマンドの実行」をクリックします。



（2）. 作成したコマンドをコピーし、「コマンドの入力」に貼り付け、「実行」をクリックします。



(3). コマンドが実行されると自動で保存されます。



3.3. ホワイトクラウド ASPIRE の VPN 設定

ホワイトクラウド ASPIRE とオンプレミスの RTX1210 を IPsec VPN で接続する設定を行います。

3.3.1. VPN 設定

(1). Web ブラウザからホワイトクラウド ASPIRE のセルフサービスポータルへアクセスし、ユーザ名とパスワードを入力してログインします。

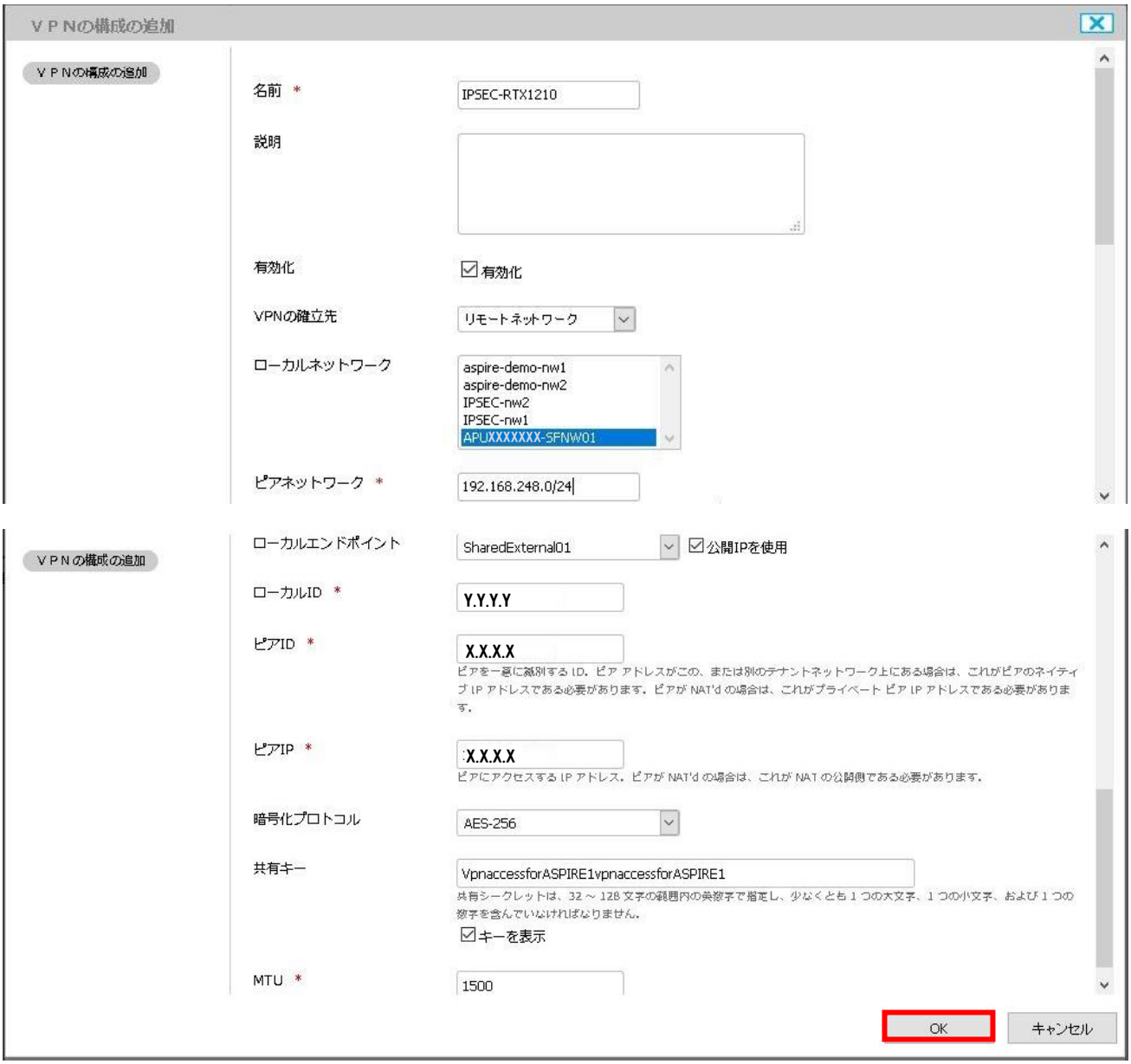
(2). 2 段階認証に設定したパターンの場所の数字を入力し、ログインをクリックします。

(3). テナント設定をクリックします。

(4). 左側のメニューより「Edge ゲートウェイ」 をクリックします。表示された Edge ゲートウェイ名（本資料では APUXXXXXXX-EdgeGW01）を右クリックし、「サービス設定」 をクリックします。

(5). 左側のメニューより「VPN」 をクリックします。「VPN を有効化」 のチェックボックスを有効化し、「追加」をクリックします。

(6). VPN パラメータを入力し、「OK」 をクリックします。



名前 ： 任意 （本設定では IPSEC-RTX1210）

説明 ： 任意

有効化 ： チェックボックス をオン

VPN の確立先 ： リモート ネットワーク を選択

ローカルネットワーク ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を選択
（本設定では APUXXXXXXX-SFNW01）

ピアネットワーク ： オンプレミスの VPN 接続対象 NW を指定（本設定では 192.168.248.0/24）

ローカルエンドポイント ：Edge ゲートウェイが接続している共有インターネット接続ネットワーク名を選択
（本設定では SharedExternal01）

ローカル ID： ホワイトクラウド ASPIRE のグローバル IP アドレス

ピア ID：オンプレミスの RTX1210 のグローバル IP アドレス（本設定では X.X.X.X）
ピア IP：オンプレミスの RTX1210 のグローバル IP アドレス（本設定では X.X.X.X）
暗号化プロトコル ：AES-256
共有キー ：RTX1210 のコマンド作成時に作成した事前共有キーを指定
（本設定では vpnaccessforASPIRE1vpnaccessforASPIRE1）
キーの表示 ： 無効を推奨（共有キーの内容確認のため一時的に ON にする場合以外は OFF を推奨）
MTU：1500

(7). VPN 設定が完了しました。しかし、この時点ではまだ VPN 設定は Edge ゲートウェイに反映されていません。引き続きファイアウォールを設定します。

3.3.2. ファイアウォール設定

(1). オンプレミスとホワイトクラウド ASPIRE の VPN 対象 NW 間の通信を許可するファイアウォール設定を追加します。「ファイアウォール」 より 「追加」 をクリックします。

(2).ポップアップしたウィザード内へオンプレミスからホワイトクラウド ASPIRE への通信（Inbound）を許可するパラメータを入力し、「OK」ボタンをクリックします。

有効 ： チェックボックスをオン
名前 ： 任意（本設定では IPSEC-IN）
順番 ： 任意（重複しない番号を割り当て）
ソース ： オンプレミスの VPN 接続対象 NW を指定（本設定では、192.168.248.0/24）
ソースポート ： 任意（本設定では、ANY）
ターゲット ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定（本設定では、192.168.0.0/24）
ターゲットポート ： 任意（本設定では、ANY）
プロトコル ： 任意
アクション ： 許可

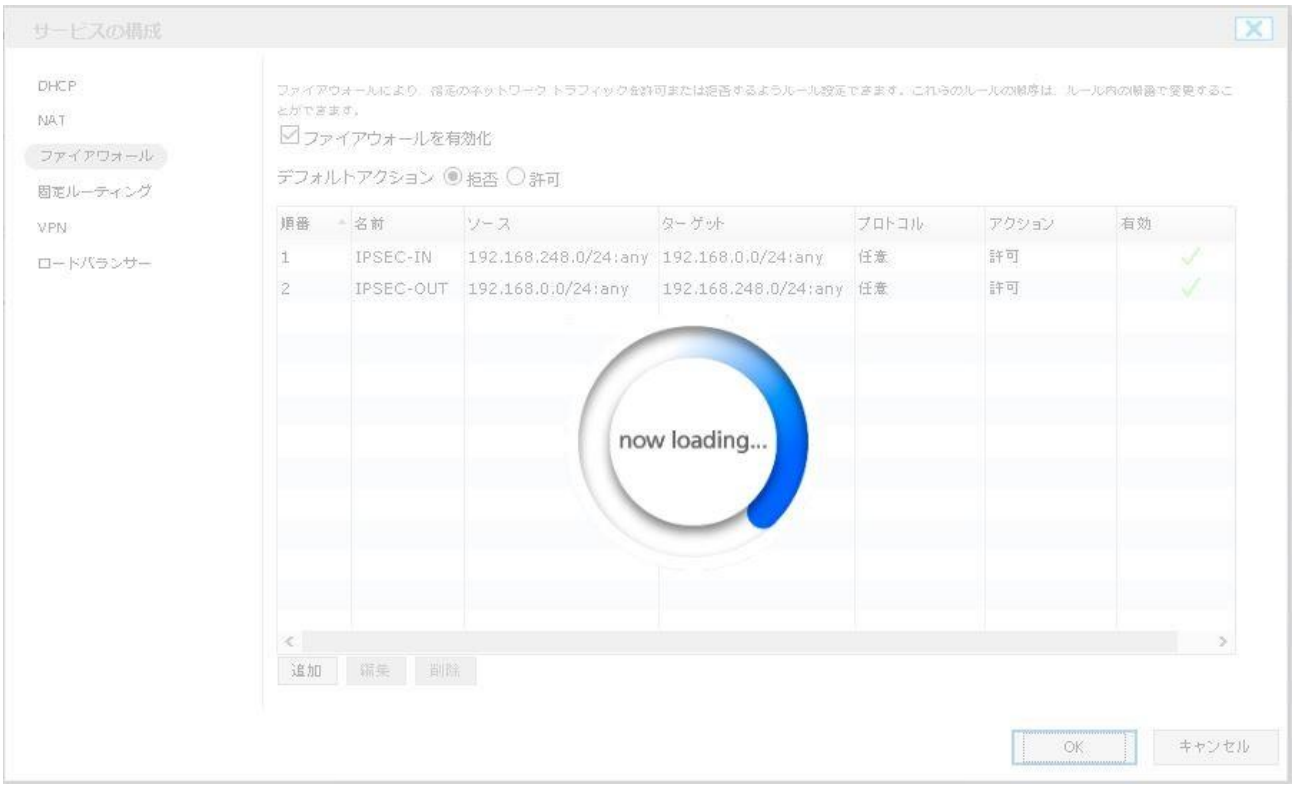
（3）. 続いて、反対方向の通信のファイアウォール設定を追加します。「追加」 をクリックします。

（4）. ポップアップしたウィザード内にホワイトクラウド ASPIRE からオンプレミスへの通信（Outbound）を許可するパラメータを入力し、「OK」ボタンをクリックします。

有効 ： チェックボックスをオン
名前 ： 任意（本設定では IPSEC-OUT）
順番 ： 任意（重複しない番号を割り当て）
ソース ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定（本設定では、192.168.0.0/24）
ソースポート ： 任意（本設定では、ANY）
ターゲット ： オンプレミス側 VPN 接続対象 NW を指定（本設定では、192.168.248.0/24）
ターゲットポート ： 任意（本設定では、ANY）
プロトコル ： 任意
アクション ： 許可

（5）. VPN 設定とファイアウォール設定をホワイトクラウド ASPIRE へ反映させる為、「OK」をクリックします。

（6）.完了するまで待機します。変更は数秒で完了します。



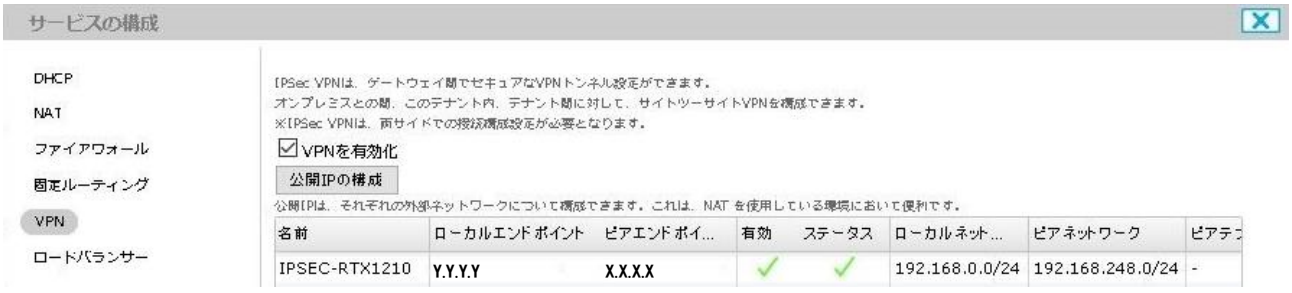
（7）.設定が完了しました。

3.4. VPN 接続後の通信確認

オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象 NW の間で通信が行えることを確認します。

3.4.1. ホワイトクラウド ASPIRE セルフサービスポータルから確認

ホワイトクラウド ASPIRE のセルフサービスポータルより「Edge ゲートウェイ」へアクセスします。「サービス設定」より「VPN」を表示し、以下のように「ステータス」に緑色のチェックが表示されていれば、VPN 接続は正常に確立されています。



以下のように、「ステータス」表示に異常を示す赤色のマークが表示されている場合は、RTX1210、もしくはホワイトクラウド ASPIRE の VPN 設定に誤りがないかを確認して下さい。（※1）
VPN 確立先のアドレスや VPN 接続対象 NW、暗号化設定（事前共有キーやアルゴリズムの選択）に誤りがある場合、VPN 接続が正常に確立できません。

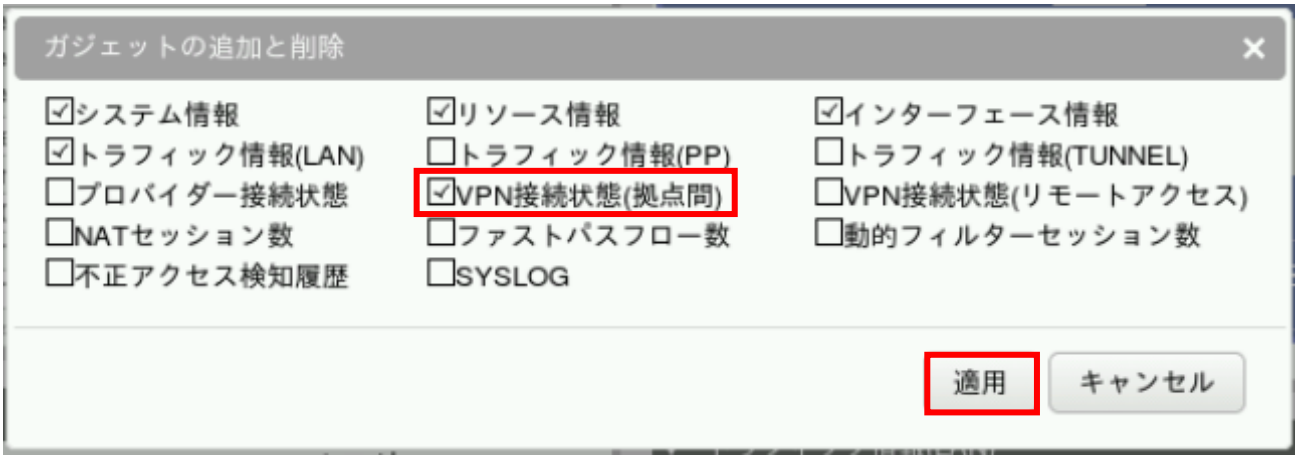
※1 ： VPN 接続が正常に確立されるまで多少時間が必要な場合があります。

3.4.2. YAMAHA RTX1210 から確認

ガジェットの機能を有効化するとダッシュボードよりVPN接続状態の確認ができます。

（1）． ダッシュボードよりガジェットをクリックします。

（2）． VPN接続状態（拠点間）を有効化し適用をクリックします。



（3）． VPN接続状態（拠点間）のガジェットが表示されました。

VPN 接続（拠点間）の一覧とそれぞれの接続状態が表示されます。状態に描かれているアイコンで接続の状態を確認できます。

(4)． マウスのカーソルを状態に描かれているアイコン上に合わせると詳細情報が表示されます。

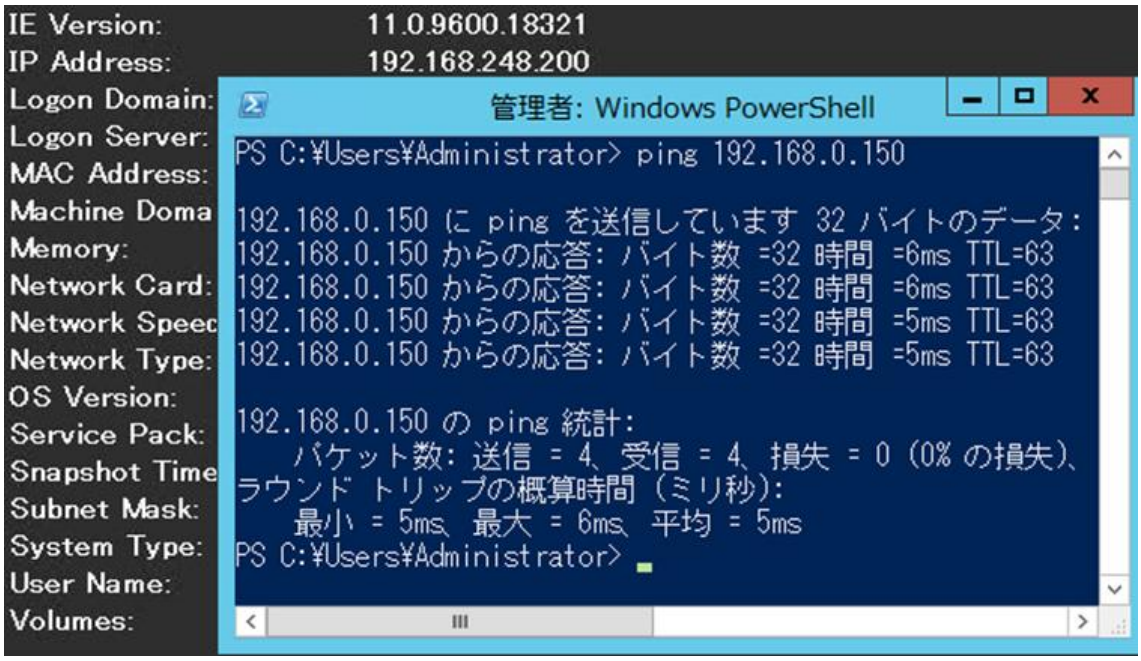
Web コンソールの詳細については、下記よりご確認ください。
ヤマハルーター Web GUI 操作マニュアル
http://www.rtpro.yamaha.co.jp/RT/manual/rtx1210/Webgui.pdf

3.4.3. 仮想マシンから確認

オンプレミス、ホワイトクラウド ASPIRE 双方の VPN 接続対象 NW 上の仮想マシンから ping やリモートアクセスなどを実行し、双方間での疎通確認を行います。

（オンプレミス側からの確認例）

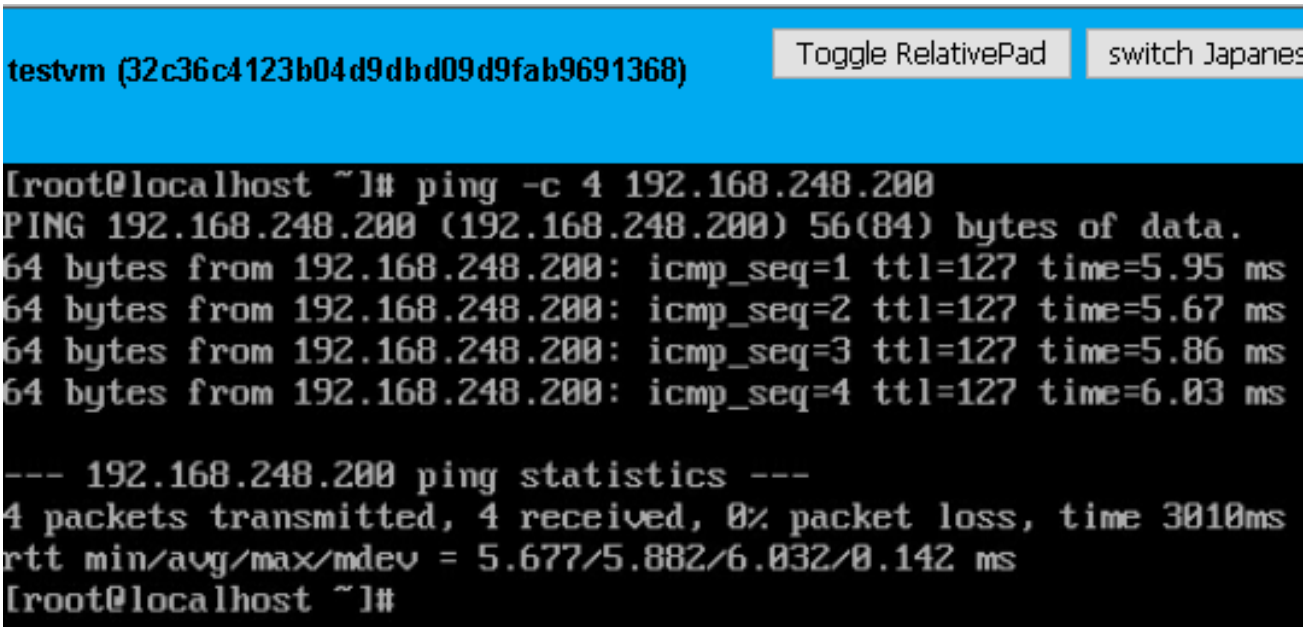
下記はオンプレミスの VPN 接続対象 NW 上の仮想マシン(Windows)から ping を実行した確認例です。



（ホワイトクラウド ASPIRE 側からの確認例）

ホワイトクラウド ASPIRE のセルフポータルサイトから「仮想マシン」をタブをクリックし、対象の仮想マシンを右クリックして「コンソールを開く」をクリックします。

ポップアウトしたコンソール内をクリックし、必要に応じてログイン操作等を行います。コンソールよりオンプレミスの仮想マシンへ通信ができることを確認します。
下記は Linux から ping を実行した確認例です。



ホワイトクラウド ASPIRE への IPsec VPN 接続手順は以上です。

3.5. 参考資料

3.5.1. 参考:本設定での RTX1210Config設定(抜粋)

```
ip route default gateway X.X.X.1
ip route 192.168.0.0/24 gateway tunnel 1
ip filter source-route on
ip filter directed-broadcast on
ip lan1 address 192.168.248.253/24
ip lan2 address 172.16.10.254/24
ip lan3 address X.X.X.X/29
ip lan3 secure filter in 1 2 3 2000
ip lan3 secure filter out 1010 1011 1012 1013 1014 1015 3000 dynamic 100 101 102 103 104 105 106 107
ip lan3 nat descriptor 1
tunnel select 1
 description tunnel Tunnel1
 ipsec tunnel 1
```

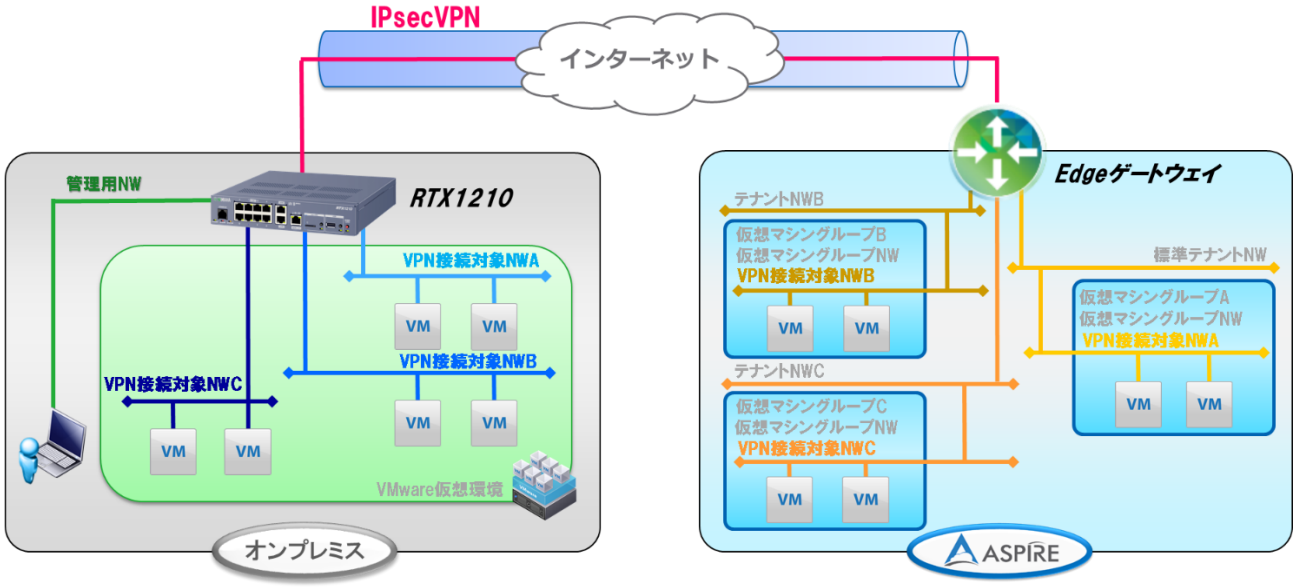
```
  ipsec sa policy 1 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.0.0/24
  ipsec ike always-on 1 on
  ipsec ike duration ipsec-sa 1 3600
  ipsec ike duration ike-sa 1 28800
  ipsec ike encryption 1 aes256-cbc
  ipsec ike group 1 modp1024
  ipsec ike hash 1 sha
  ipsec ike local address 1 X.X.X.X
  ipsec ike local id 1 192.168.248.0/24
  ipsec ike pfs 1 on
  ipsec ike pre-shared-key 1 text VpnaccessforASPIRE1vpnaccessforASPIRE1
  ipsec ike remote address 1 Y.Y.Y.Y
  ipsec ike remote id 1 192.168.0.0/24
  ipsec auto refresh 1 on
 ip tunnel secure filter in 101
 ip tunnel secure filter out 102
 ip tunnel tcp mss limit auto
 tunnel enable 1
ip filter 1 pass * 192.168.248.253 udp * 500
ip filter 2 pass * 192.168.248.253 udp * 4500
ip filter 3 pass * * esp * *
ip filter 101 pass 192.168.0.0/24 192.168.248.0/24 * * *
ip filter 102 pass 192.168.248.0/24 192.168.0.0/24 * * *
ip filter 1010 reject * * udp,tcp 135 *
ip filter 1011 reject * * udp,tcp * 135
ip filter 1012 reject * * udp,tcp netbios_ns-netbios_ssn *
ip filter 1013 reject * * udp,tcp * netbios_ns-netbios_ssn
ip filter 1014 reject * * udp,tcp 445 *
ip filter 1015 reject * * udp,tcp * 445
ip filter 2000 reject * *
ip filter 3000 pass * *
ip filter dynamic 100 * * ftp
ip filter dynamic 101 * * www
ip filter dynamic 102 * * domain
ip filter dynamic 103 * * smtp
ip filter dynamic 104 * * pop3
ip filter dynamic 105 * * tcp
ip filter dynamic 106 * * udp
```

```
ip filter dynamic 107 * * ping
nat descriptor type 1 masquerade
nat descriptor address outer 1 X.X.X.X
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 X.X.X.X udp 500
nat descriptor masquerade static 1 2 X.X.X.X udp 4500
nat descriptor masquerade static 1 3 X.X.X.X esp
ipsec use on
ipsec auto refresh on
#
```

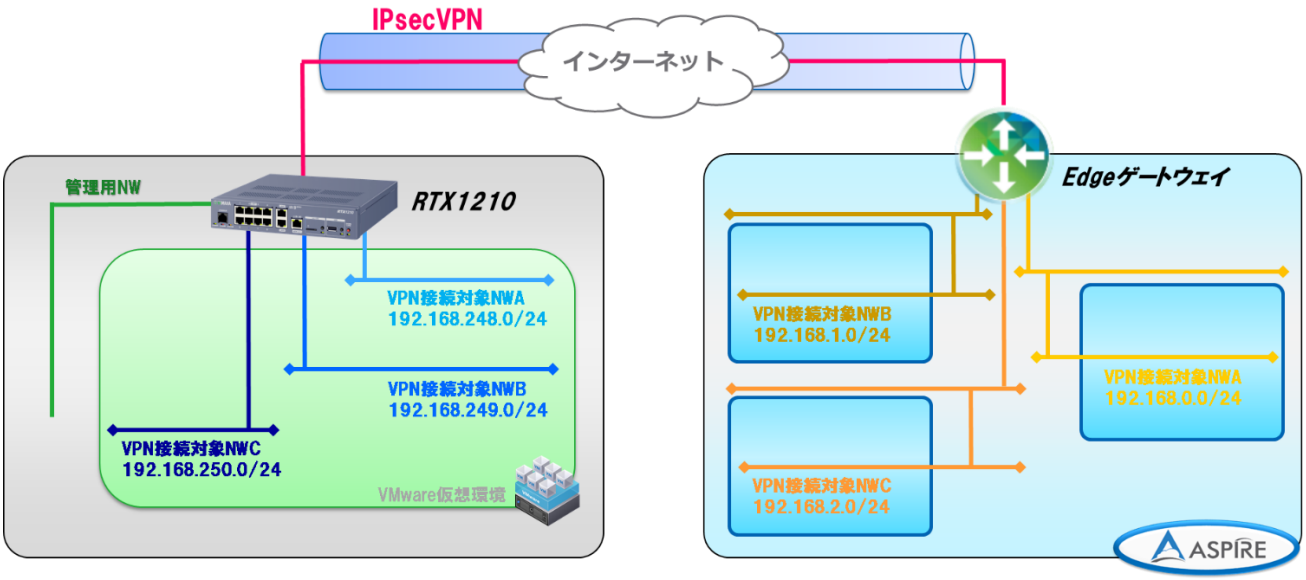
3.5.2. 参考:RTX1210 を用いて複数セグメント間で IPsec VPN を設定する場合

下記のように複数のネットワーク間で IPsec VPN を設定することもできます。
参考としてホワイトクラウド ASPIRE 側の3つのネットワークとオンプレミス側の3つのネットワーク間で IPsec VPN を構築する例を記載します。

・論理構成図



・ネットワーク図

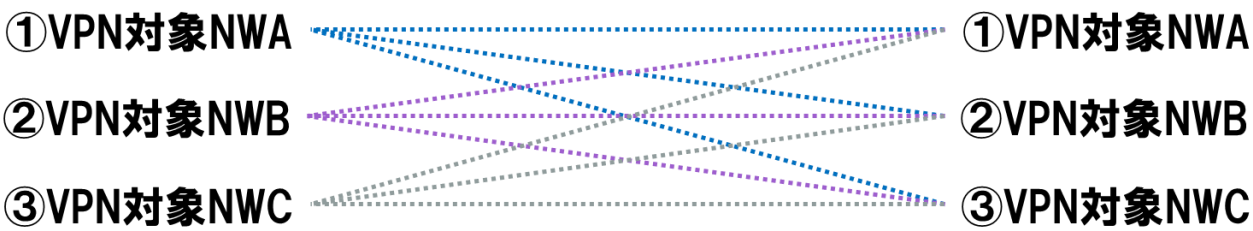


・設定概念図

ホワイトクラウドASPIREのEdgeゲートウェイのIPsecVPN方式は、ポリシーベースVPNです。
IPsecVPN通信を構成したいトラフィックのルールを全て設定します。

構成例

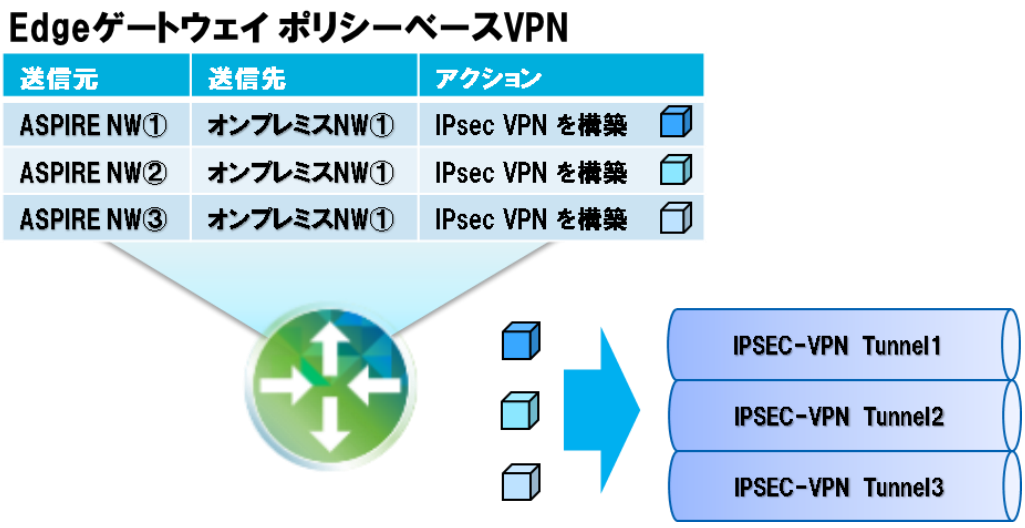
双方の3セグメントを全てIPsecVPN経由で
通信させる場合、すべてのルールを記載します。



・VPN 設定上の注意点

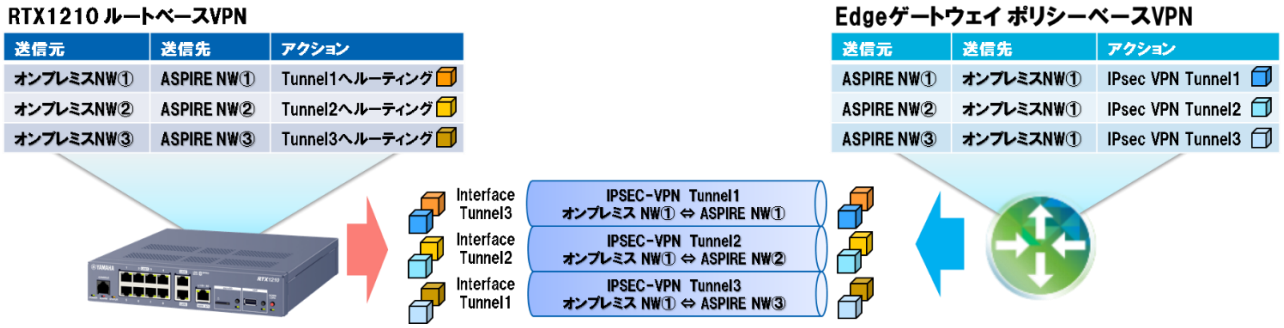
・VPN 接続対象 NW ごとに SA ポリシーの定義が必要

ホワイトクラウド ASPIRE はポリシーベース VPN の為、VPN 対象通信のトラフィックごとに VPN が構築されます。RTX 製品では VPN 対象ネットワーク毎に ipsec sa policy コマンドを利用し、ローカル ID、リモート ID（Proxy-ID）を設定します。

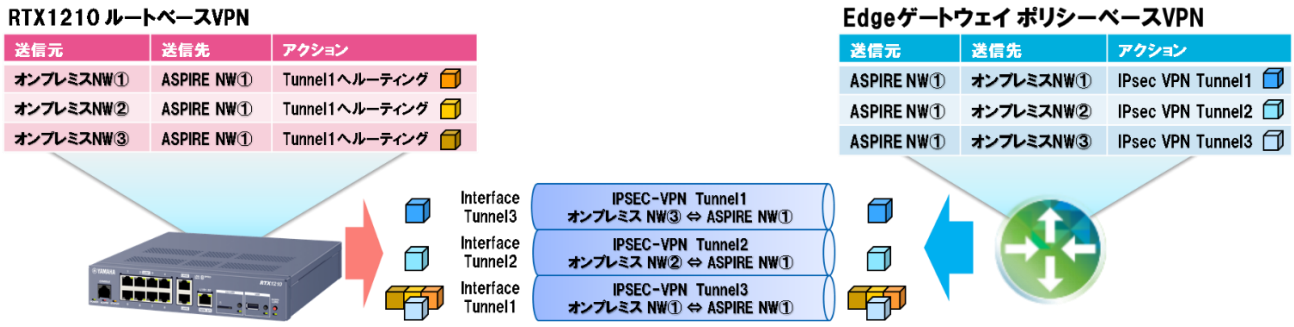


・RTX 側に複数ネットワーク存在する場合はフィルタ型ルーティングが必要

オンプレミスとホワイトクラウド ASPIRE の複数の VPN 接続対象 NW と VPN で接続する場合は、RTX 製品でルーティング上の問題は発生しません。



オンプレミスの複数の VPN 接続対象 NW とホワイトクラウド ASPIRE を VPN で接続する場合は、往復の通信で通る経路を一致させる為にフィルタ型ルーティングの設定が必要です。



3.5.2.1. 複数セグメント間での IPsec VPN 設定（RTX1210）

複数の VPN 対象 NW との VPN 設定における差分を記載します。

1. トンネル用 IP フィルタの設定（任意）
2. IPsecVPN の設定
3. **トンネルインターフェースに ipsec sa policy を設定し有効化**
4. **フィルタ型ルーティングを設定**
5. WAN インターフェース用 IP フィルタの設定
6. NAT の設定

※参考 Config は巻末に記載しております。

①トンネルインターフェースを有効化

下記コマンドでトンネルインターフェースを有効化します。

コマンド	概要	設定するパラメータ
tunnel select	トンネルインタフェース番号を選択	任意
description tunnel	トンネルインターフェースにメモを設定	任意
ipsec tunnel	使用する SA のポリシーの設定	使用する SA のポリシーの設定
ipsec sa policy	SA のポリシーの定義	暗号化方式、ローカルID（オンプレミス VPN対象NW）、リモートID（ホワイトクラウドASPIRE VPN対象NW）
ip tunnel secure filter in	フィルタリングによるセキュリティの設定	任意
ip tunnel secure filter out	フィルタリングによるセキュリティの設定	任意
ip tunnel tcp mss limit	TCP セッションの MSS 制限の設定	auto
tunnel	有効／無効の設定	enable

ipsec sa policy 設定コマンド詳細

ipsec sa policy	[Policy_id]	[Gateway_id]	Esp	[認証アルゴリズム]	Sha-hmac	[Local-id]	[Remote-id]	anti-replay-check=off
固定値	ipsec tunnel コマンドで設定した値	1で固定 ※	固定値	下記から選択 3des-cbc aes-cbc aes256-cbc	固定値	オンプレミス VPN対象NW	ホワイトクラウド ASPIRE VPN対象NW	固定値

※ISAKMP SAを1本のみ設定する場合

設定例（本資料での設定の一部を抜粋して記載）

```
tunnel select 2
 description tunnel WhiteCloud-ASPIRE-A-Onp-B
ipsec tunnel 2
 ipsec sa policy 2 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.0.0/24 anti-replay-check=off
 ip tunnel secure filter in 1201
 ip tunnel secure filter out 1202
 ip tunnel tcp mss limit auto
tunnel enable 2
```

設定コマンドの詳細は下記をご確認ください。
Yamaha ルーターシリーズ コマンドリファレンス
http://www.rtpro.yamaha.co.jp/RT/manual/rt-common

②フィルタ型ルーティングを設定

前工程にて作成した ipsec sa policy に合致する IP フィルタを作成し、フィルタ型ルーティングを設定します。記述されている順にフィルタが適用され、合致したゲートウェイが選択されます。

設定例（本資料での設定の一部を抜粋して記載）

```
ip filter 100 pass 192.168.248.0/24 192.168.0.0/24 * * *
ip filter 200 pass 192.168.249.0/24 192.168.0.0/24 * * *
ip filter 300 pass 192.168.250.0/24 192.168.0.0/24 * * *
ip route 192.168.0.0/24 gateway tunnel 1 filter 100 gateway tunnel 2 filter 200 gateway tunnel 3 filter 300
```

設定コマンドの詳細は下記をご確認ください。
Yamaha ルーターシリーズ コマンドリファレンス 9.1.7 IP の静的経路情報の設定
http://www.rtpro.yamaha.co.jp/RT/manual/rt-common/ip/ip_route.html

Yamaha ルーターシリーズ フィルタ型ルーティング
http://www.rtpro.yamaha.co.jp/RT/docs/filter-routing/filter-routing.html#command

3.5.2.2. 複数セグメント間での IPsec VPN 設定 （ホワイトクラウド ASPIRE）

ホワイトクラウド ASPIRE のセルフポータルサイトより複数セグメント間での IPsec VPN を設定する場合の異なる設定箇所を記載します。

・VPN 設定

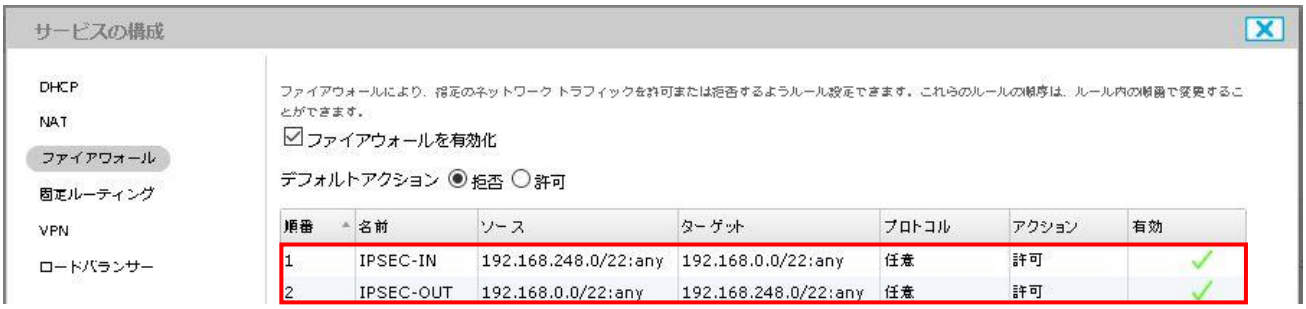
(1). VPN の構成の追加時に設定する VPN を全て選択します。

ローカルネットワーク ： Ctrl キーを押しながら、設定したいテナントネットワーク名を選択
ピアネットワーク ： 設定するネットワークを “ , ”（カンマ）で区切ります。

(2). 設定した対象 NW を下記のように確認できます。

・ファイアウォール設定

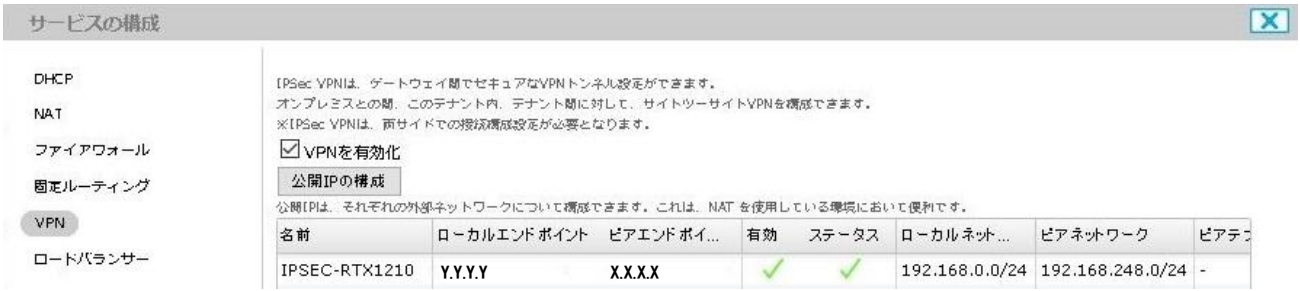
（1）. 通信させたいすべてのトラフィックルールをファイアウォールに設定します。



本資料の構成ですべてのトラフィックルールを VPN 対象 NW 毎に設定すると、
最低でも ３ × ３ × ２（In/Out） = 18 本のルール設定が必要です。
ネットワークをサマライズすることで設定本数を減らすことができます。

3.5.2.3.VPN 接続後の通信確認時の注意点

稀に ASPIRE 上のステータスが有効となっていても双方での IPsec VPN のネゴシエーションの一部が失敗し、その一部のルールの通信が不可となるケースがあります。
その場合は、オンプレミスのネットワーク機器で IPsec VPN の SA を削除してください。



RTX1210 の場合は下記コマンドを実行することで SA を削除できます。

ipsec sa delete all

参考：本設定での RTX1210Config設定（抜粋）

```
## RTX1210 グローバルアドレス X.X.X.X
## ホワイトクラウド ASPIRE グローバルアドレス Y.Y.Y.Y
## 192.168.0.0/24 向けの設定のトンネル番号1、2、3
## 192.168.1.0/24 向けの設定のトンネル番号11、12、13
## 192.168.2.0/24 向けの設定のトンネル番号21、22、23
##
ip route default gateway X.X.X.1
ip route 192.168.249.0/24 gateway 192.168.248.96
ip route 192.168.250.0/24 gateway 192.168.248.96
```

```
ip route 192.168.0.0/24 gateway tunnel 1 filter 100 gateway tunnel 2 filter 200 gateway tunnel 3 filter 300
ip route 192.168.1.0/24 gateway tunnel 11 filter 400 gateway tunnel 12 filter 500 gateway tunnel 13 filter 600
ip route 192.168.2.0/24 gateway tunnel 21 filter 700 gateway tunnel 22 filter 800 gateway tunnel 23 filter 900
ip lan1 address 192.168.248.253/24
ip lan2 address 172.16.10.254/24
ip lan3 address X.X.X.X/29
ip lan3 secure filter in 1 2 3 2000
ip lan3 secure filter out 1010 1011 1012 1013 1014 1015 3000 dynamic 100 101 102 103 104 105 106 107
ip lan3 nat descriptor 1
tunnel select 1
 description tunnel ASPIRE-A-Onp-A
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.0.0/24 anti-replay-check=off
  ipsec ike always-on 1 on
  ipsec ike duration ipsec-sa 1 3600
  ipsec ike duration ike-sa 1 28800
  ipsec ike encryption 1 aes256-cbc
  ipsec ike group 1 modp1024
  ipsec ike hash 1 sha
  ipsec ike local address 1 X.X.X.X
  ipsec ike pfs 1 on
  ipsec ike pre-shared-key 1 text VpnaccessforASPIRE1vpnaccessforASPIRE1
  ipsec ike remote address 1 Y.Y.Y.Y
  ipsec auto refresh 1 on
 ip tunnel secure filter in 1101
 ip tunnel secure filter out 1102
 ip tunnel tcp mss limit auto
 tunnel enable 1
tunnel select 2
 description tunnel WhiteCloud-ASPIRE-A-Onp-B
 ipsec tunnel 2
  ipsec sa policy 2 1 esp aes256-cbc sha-hmac local-id=192.168.249.0/24 remote-id=192.168.0.0/24 anti-replay-check=off
 ip tunnel secure filter in 1201
 ip tunnel secure filter out 1202
 ip tunnel tcp mss limit auto
 tunnel enable 2
tunnel select 3
 description tunnel WhiteCloud-ASPIRE-A-Onp-C
```

```
 ipsec tunnel 3
  ipsec sa policy 3 1 esp aes256-cbc sha-hmac local-id=192.168.250.0/24 remote-id=192.168.0.0/24 anti-replay-check=off
 ip tunnel secure filter in 1301
 ip tunnel secure filter out 1302
 ip tunnel tcp mss limit auto
 tunnel enable 3
tunnel select 11
 description tunnel WhiteCloud-ASPIRE-B-Onp-A
 ipsec tunnel 11
  ipsec sa policy 11 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.1.0/24 anti-replay-check=off
 ip tunnel secure filter in 1401
 ip tunnel secure filter out 1402
 ip tunnel tcp mss limit auto
 tunnel enable 11
tunnel select 12
 description tunnel WhiteCloud-ASPIRE-B-Onp-B
 ipsec tunnel 12
  ipsec sa policy 12 1 esp aes256-cbc sha-hmac local-id=192.168.249.0/24 remote-id=192.168.1.0/24 anti-replay-check=off
 ip tunnel secure filter in 1501
 ip tunnel secure filter out 1502
 ip tunnel tcp mss limit auto
 tunnel enable 12
tunnel select 13
 description tunnel WhiteCloud-ASPIRE-B-Onp-C
 ipsec tunnel 13
  ipsec sa policy 13 1 esp aes256-cbc sha-hmac local-id=192.168.250.0/24 remote-id=192.168.1.0/24 anti-replay-check=off
 ip tunnel secure filter in 1601
 ip tunnel secure filter out 1602
 ip tunnel tcp mss limit auto
 tunnel enable 13
tunnel select 21
 description tunnel WhiteCloud-ASPIRE-C-Onp-A
 ipsec tunnel 21
  ipsec sa policy 21 1 esp aes256-cbc sha-hmac local-id=192.168.248.0/24 remote-id=192.168.2.0/24 anti-replay-check=off
 ip tunnel secure filter in 1701
 ip tunnel secure filter out 1702
 ip tunnel tcp mss limit auto
 tunnel enable 21
```

```
tunnel select 22
 description tunnel WhiteCloud-ASPIRE-C-Onp-B
 ipsec tunnel 22
  ipsec sa policy 22 1 esp aes256-cbc sha-hmac local-id=192.168.249.0/24 remote-id=192.168.2.0/24 anti-replay-check=off
 ip tunnel secure filter in 1801
 ip tunnel secure filter out 1802
 ip tunnel tcp mss limit auto
 tunnel enable 22
tunnel select 23
 description tunnel WhiteCloud-ASPIRE-C-Onp-C
 ipsec tunnel 23
  ipsec sa policy 23 1 esp aes256-cbc sha-hmac local-id=192.168.250.0/24 remote-id=192.168.2.0/24 anti-replay-check=off
 ip tunnel secure filter in 1901
 ip tunnel secure filter out 1902
 ip tunnel tcp mss limit auto
 tunnel enable 23
ip filter 1 pass * 192.168.248.253 udp * 500
ip filter 2 pass * 192.168.248.253 udp * 4500
ip filter 3 pass * * esp * *
ip filter 100 pass 192.168.248.0/24 192.168.0.0/24 * * *
ip filter 200 pass 192.168.249.0/24 192.168.0.0/24 * * *
ip filter 300 pass 192.168.250.0/24 192.168.0.0/24 * * *
ip filter 400 pass 192.168.248.0/24 192.168.1.0/24 * * *
ip filter 500 pass 192.168.249.0/24 192.168.1.0/24 * * *
ip filter 600 pass 192.168.250.0/24 192.168.1.0/24 * * *
ip filter 700 pass 192.168.248.0/24 192.168.2.0/24 * * *
ip filter 800 pass 192.168.249.0/24 192.168.2.0/24 * * *
ip filter 900 pass 192.168.250.0/24 192.168.2.0/24 * * *
ip filter 1010 reject * * udp,tcp 135 *
ip filter 1011 reject * * udp,tcp * 135
ip filter 1012 reject * * udp,tcp netbios_ns-netbios_ssn *
ip filter 1013 reject * * udp,tcp * netbios_ns-netbios_ssn
ip filter 1014 reject * * udp,tcp 445 *
ip filter 1015 reject * * udp,tcp * 445
ip filter 1101 pass 192.168.0.0/24 192.168.248.0/24 * * *
ip filter 1102 pass 192.168.248.0/24 192.168.0.0/24 * * *
ip filter 1201 pass 192.168.0.0/24 192.168.249.0/24 * * *
ip filter 1202 pass 192.168.249.0/24 192.168.0.0/24 * * *
```

```
ip filter 1301 pass 192.168.0.0/24 192.168.250.0/24 * * *
ip filter 1302 pass 192.168.250.0/24 192.168.0.0/24 * * *
ip filter 1401 pass 192.168.1.0/24 192.168.248.0/24 * * *
ip filter 1402 pass 192.168.248.0/24 192.168.1.0/24 * * *
ip filter 1501 pass 192.168.1.0/24 192.168.249.0/24 * * *
ip filter 1502 pass 192.168.249.0/24 192.168.1.0/24 * * *
ip filter 1601 pass 192.168.1.0/24 192.168.250.0/24 * * *
ip filter 1602 pass 192.168.250.0/24 192.168.1.0/24 * * *
ip filter 1701 pass 192.168.2.0/24 192.168.248.0/24 * * *
ip filter 1702 pass 192.168.248.0/24 192.168.2.0/24 * * *
ip filter 1801 pass 192.168.2.0/24 192.168.249.0/24 * * *
ip filter 1802 pass 192.168.249.0/24 192.168.2.0/24 * * *
ip filter 1901 pass 192.168.2.0/24 192.168.250.0/24 * * *
ip filter 1902 pass 192.168.250.0/24 192.168.2.0/24 * * *
ip filter 2000 reject * *
ip filter 3000 pass * *
ip filter dynamic 100 * * ftp
ip filter dynamic 101 * * www
ip filter dynamic 102 * * domain
ip filter dynamic 103 * * smtp
ip filter dynamic 104 * * pop3
ip filter dynamic 105 * * tcp
ip filter dynamic 106 * * udp
ip filter dynamic 107 * * ping
nat descriptor type 1 masquerade
nat descriptor address outer 1 X.X.X.X
nat descriptor masquerade static 1 1 X.X.X.X udp 500
nat descriptor masquerade static 1 2 X.X.X.X udp 4500
nat descriptor masquerade static 1 3 X.X.X.X esp
ipsec use on
ipsec auto refresh on
syslog notice on
```

以上