

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。





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



目次

1. ホワイト	・クラウド ASPIRE の IPsec VPN 機能概要	5
1 1 IPsec V	VPN について	5
1.2. ホワイ	トクラウド ASPIRE の IPsec VPN 機能	5
2. RTX12	10 とホワイトクラウド ASPIRE の接続構成概要	6
91 木容紫	マご 22 介する RTV 1 2 10 を田いた構成	6
2.1. 本員作	「ここれ」」。 「「ここ」」。 「ここ」」、 「ここ、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ 「ここ」、 「ここ」、 「ここ」、 「ここ」、 「ここ 「ここ」、 「ここ 「ここ」、 「ここ」、 「ここ 「ここ」、 「ここ 「ここ」、 「ここ 「ここ」、 「ここ 「ここ」、 「ここ 「ここ」、 「ここ」、 「ここ、 「ここ」、 「 「」、 「 「」、 「 「」、 「 「 「」、 「 「」、 「 「 「 「 「 「 「 「 「 「 「 「 「	
3. 構成手	順	8
3.1. 設定前	うの状態について	8
3.1.1. オン	[,] プレミス側 RTX1210 の設定	
3.1.2. ホワ	ワイトクラウド ASPIRE 側の設定	9
3.2. RTX12	10の VPN 設定	10
3.2.1. IPse	cVPN 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	
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	
3.4. VPN 接	続後の通信確認	24
3.4.1. ホワ	ワイトクラウド ASPIRE セルフサービスポータルから確認	
3.4.2. YAN	IAHA RTX1210 から確認	25
3.4.3. 仮丸	見マシンから確認	
3.5. 参考資	『料	28
3.5.1. 参考	š:本設定での RTX1210Config設定(抜粋)	
3.5.2. 参考	ぎ:RTX1210 を用いて複数セグメント間で IPsec VPN を設定する場合	
3.5.2.1.	複数セグメント間での IPsec VPN 設定 (RTX1210)	
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)	
3.5.2.3.	VPN 接続後の通信確認時の注意点	

4 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.

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。



5 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.

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



<u>RTX1210</u>

- ・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



<u>Edge ゲートウェイ</u>

- ・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]
固定值	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

Copyright 2016 SoftBank Corp. All Rights Reserved.



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。

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/

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

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)

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

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。

®YAMAHA RTX	/1210	管理ユーザー:ユーザー名なし ログアウト
🏼 ダッシュボード 🔚 LA	Nマップ 🎢 かんたん設定 🏾 🌞 詳細設定 🌂 🏾 管 理	CONFIG TECHINFO ヘルプ
44		
本体の設定		^
アクセス管理	■ コマンドの実行	
保守 🔻	コマンドを実行することができます。コマンドを実行すると、自動的に設定が保存されます。	2
コマンドの実行		
ファームウェアの更新	■ コマンドの実行	
CONFIGファイルの		
SYSLOGの管理		=
冉起動と初期化		
	コマンドの入力	
		8
		フリア 実行

(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。



SoftBank

(3). コマンドが実行されると自動で保存されます。

⊛YAMAHA <i>Rtx121</i>	0	管理工	-ザー:ユーザ	「一名なし	ログアウト
ダッシュボード 王 LANマップ	າ 🍂 ກໍ່ມີເປັນ	定 🗱 詳細設定 🥄 管 理	CONFIG	TECHINFO	トーヘレプ
▲4 コマンドの実行 ファームウェアの更新 CONFIGファイルの 2010.000 第1時	₿ 設定を保存しま	ute.			
再起動と初期化	コマンドの実行				
	コマンドの入力	ipsec ike remote id 1 192.168.0.0/24 ipsec auto refresh 1 on ig tunnel secure filter in 101 ig tunnel secure filter out 102 ig tunnel tog mss limit auto tunnel enable 1 ig filter 101 pass 192.168.0.0/24 192.168.248.0/24 * * ig filter 102 pass 192.168.248.0/24 192.168.0.0/24 * *	* = >		
	マンド実行結果	クリア		実行)
*	結果	ארצר			
	📀 成功	p route 192.168.0.0/24 gateway tunnel 1			^
· · · · · · · · · · · · · · · · · · ·	📀 成功	unnel select 1			=
	Ӯ 成功	description tunnel Tunnel1			
	Ӯ 成功	psec tunnel 1			
	*-+	Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.	0.460.0.0/04		

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。

ASPIRE セルフポータルサイト	
ユーザ名:	
ロヴイン	
SoftBank	

(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。

	ASPIRE セルフポータルサイト												
		ಕೂನ:	2段階語 ス目に表	認証に診 見示され	定され ている	たパタ・ 数字をフ	ーンに消 しカして	iった場 「ログ	所と順 イン」し	番で、 Jてくた	ざさい。		
	5	0	8	6	1	5	5	2	0	3	7	2	
	1	3	3	7	0	4	8	3	8	9	1	0	
	9	2	3	9	6	6	4	7	7	5	6	6	
	2	5	4	1	9	1	2	7	8	0	4	4	
パスワード:													
SoftBank													



(3). テナント設定をクリックします。

SoftBank		A	ASPIRE	セルフポータ	ルサイト	test-admin1(ユーザ管理) ・イト 〇 環境設定 サ				
ダッシュポード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	00	2-¥	テナント設定	1		
■ダッシュボ 最新の情報	(一ド 服に更新	ダッシュボード 	s	4011608104			`штр 7 к. 7 *	Renation of C		
		ענטי <u>ר</u> ט עטיבקע נפע 1%	。 使用量 。 0 GHz/10(-APU1608194 3Hz						

(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 APUXXXXXX-EdgeGW01)を右クリックし、「サービス設定」をクリックします。

Soft	Bank	A	ASPIRE	test-ac	test-admin1(ユーザ管理者(契約番 〇 環境設定 サポート				
ダッシュボード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	D19	7-4	テナント設定		
▼ 契約リソー リソース 最新の値	ス (使用量の表示 詳報に更新 - ウェイ	Edgeガートウ C III (マ	IT All Fields	Search					
最新の情	報に更新	名前		ステータス	使用済みNIC数	外部ネットワーク	ク数 テナントネ	ットワーク数	Edgeゲートウェイサ
▶設定		APU XXXXXXX - E	dgeGW01 サービス級 ネットワー サービス線 両デブロイ ブロパティ	7月 17日 - 小27頃形 186の阿利用		1	5		S

(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。

イアウォール ルーティング	LPSec VPNは、ク オンプレミスとの ※LPSec VPNは、 VPNを有効	ナートワエイ間でセキュアな\ D間、このテナント内、テナ: 両サイドでの接続構成設定! 別化	/PNトンネル設定ができま ント間に対して、サイト) が必要となります。	ます. ソーサイト)	VPNを構成で	きます.		
D	公開IPの構成 公開IPは、それる 名前	成 デれの外部ネットワークについ ローカルエンド…	いて痛成できます。これ ピアエンドポイント	は、NATを 有効	使用している ステ	5環境において便利です。 ローカルネットワ…	ピアネットワーク	ピアテナント
	追加編	集 削除		4				

18 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.

SoftBank

(6). VPN パラメータを入力し、「OK」をクリックします。

V P Nの構成の追加			×
	名前 *	IPSEC-RTX1210	^
	説明		
	有効化	☑ 有効化	
	VPNの <u>確立</u> 先	リモートネットワーク	
	ローカルネットワーク	aspire-demo-nw1 aspire-demo-nw2 IPSEC-nw2 IPSEC-nw1 APUXXXXXXSFNW01	
	ピアネットワーク *	192.168.248.0/24	~
VPNの構成の追加	ローカルエンドポイント	SharedExternal01 公開IPを使用	^
	ローカルID *	Y.Y.Y.Y	
	ピアID *	XXXXX ビアを一意に減別する ID・ビア アドレスがこの、または別のテナントネットワーク上にある場合は、これがビアのネイティ ブ IP アドレスである必要があります。ビアが NAT'd の場合は、これがプライベート ビア IP アドレスである必要がありま す。	
	ピアIP *	XXXXX ビアにアクセスする IP アドレス・ビアが NAT'd の場合は、これが NAT の公開側である必要があります。	L
	暗号化プロトコル	AES-256	
	共有キー	VpnaccessforASPIRE1vpnaccessforASPIRE1 共有シークレットは、32~128文字の範囲内の英数字で指定し、少なくとも1つの大文字、1つの小文字、および1つの 数字を含んでいなければなりません。 □ キーを表示	
	MTU *	1500 OK キャンセル	~ V

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 APUXXXXXX-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

19 / 40

Copyright 2016 SoftBank Corp. All Rights Reserved.

SoftBank

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。

サービスの構成											
DHCP NAT ファイアワォール 固定ルーティング	IPSec VPNは、ゲートウ・ オンプレミスとの制、この ※IPSec VPNは、両サイ ✓ VPNを有効化 公開IPの構成 公開IPの構成	ェイ聞でゼキュアなVPA カテナント内、テナント ドでの授続環感設定が必 ポネットワークについて	トンネル設定ができま 間に対して、サイトツ・ 寝となります。 病感できます。これは、	す。 - サイトVPNを NAT を使用し	- 横成できま。 している環境	す。					
VPN	名前	ローカルエンド	ピアエンドポイ	有効	ステ	ローカルネット	ビアネットワーク	ピアテナン			
ロードバランサー	IPSEC-RTX1210	Y.Y.Y.Y	X.X.X.X	1	0	192.168.0.0/24	192.168.248.0/24	20			

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。

順番 ▲ 名前 ソース ターゲット プロトコル	アクション	有効
<u>追加</u> 編集 削除		

(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。

SoftBank

ファイアウォールルールの	自加		X
77-7758-14-14-258分日	有効	☑有効化	^
	名前 *	IPSEC-IN	
	.順番 *	1 1~999の間で入力お問いいたします。	
	ソース *	192.168.248.0/24 有効な優は、IP アドレス、CIDR、IP 範囲、「any」、「internal」 および featernal」 です。	
	ソースポート	任意 v any	
	ターゲット *	192.168.0.0/24 有効な液は、IP アドレス、CIDR、IP 範囲、「any」、「internal」 および「external」です。	
	ターグットポート	任意 V any	~
	プロトコル *	任意	
	アクション	●許可 ○拒否	*
		OK ‡ *	ンセル

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。

イアロォール	<i>とができま</i> 2ア	す。 イアウォールを有	动化				
ルーティング	デフォル	トアクション ④	● 拒否 ○ 許可	5. H.L	701 31	700-00	- <u></u>
トバランサー	加雷 1	- 名和 IPSEC-IN	192.168.248.0/24:any	9-09F 192.168.0.0/24:any	ノロトコル 任意	ドワション	

21 / **40** Copyright 2016 SoftBank Corp. All Rights Reserved.



(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。

ファイアウォールルール	の追加		X
ファイアウォールールの追加	有効	☑ 有効化	^
	名前 *	IPSEC-OUT	
	顺番 *	2 1~999の間で入力お預いいたします。	
	ソース *	192.168.0.0/24 参加た時日 12 ズムノス CIDD (12新聞) Lany() Unternal) および feetornal) つす。	
	ソースポート	任意 💟 any	
	ターグット *	192.168.248.0/24 得効な預は、IPアドレス、CIDR、IP範囲、「any」、「internal」および「external」です。	- 1
	ターグットポート	任意 💟 any	~
	วื่อหว่าม *	任意	- 1
	アクション	●許可 ○拒否	~
		ОК	キャンセル

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。

⊾r .T アイアワォール Fルーティング	ファイア とができ ☑ ファ デフォ.	ゥォールにより、福祉 ます。 マイアウォールを和 ルトアクション(Eのネットワーク トラフィックをお 有効化 ① 拒否 ○許可	可または泡否するようルール改足	できます。 これら(カルールの順序は、ルー	-ル内の順爵で変更するこ
N	順番	* 名前	ソース	ターゲット	プロトコル	アクション	有効
ードバランサー	1	IPSEC-IN	192.168.248.0/24:any	192.168.0.0/24:any	任意	許可	1
	2	IPSEC-OUT	192.168.0.0/24:any	192.168.248.0/24:any	任意	許可	1
	۲						>
	追加	編集 削別	余				

(6).完了するまで待機します。変更は数秒で完了します。

HCP はT ファイアワォール ITEルーティング	ファイヌ とが下き ☑ ファ デフォ)	ウォールにより、ほだ ます。 > イアウォールを有 ルトアクション(のネットワーク トラフィックを約 19効化 9 拒否 〇 許可	可または絶否するようルール改正	で変ます。これら	かルールの網際は、ルー	-ル内の樹島で変更するこ
PN	順番	* 名前	ソース	ターゲット	プロトコル	アクション	有効
コードパランサー	1	IPSEC-IN	192.168.248.0/24:any	192.168.0.0/24:any	任意	計可	
	2	IPSEC-OUT	192,168.0.0/24:any	192.168.248.0/24:any	任意	許可	
			Q				
	<.						>
	這方口						



(7).設定が完了しました。

Soft	Bank	ASPIRE セルフボータルサイト				★ASPIRE セルフボータルサイト test-admin1(ユーザ管理者(契約) では、 ないので、 ないので、 ないので、 たいので、 たいので、 ないので、 た						
ダッシュポード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	00	ユーザ	テナント設定					
■ 契約リソー: リソース 最新の情	ス 使用量の表示 報に更新	Edgeゲートウ	II									
▼Edgeゲート 最新の情	>ウエイ 補に更新	C III へ 名前	All Fields	Search マステータス	使用済みNIC製	女 外部ネット 5	フーク数 テナント	ネットワーク数 Ec	lgeゲートウェイサイズ			
▶設定		APUXXXXXXXX-E	dgeGW01	<i>✓</i>	6	1	5	S				

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」 ヘアクセスします。 「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。

サービスの構成								L
DHCP	(PSec VPNは、ゲートウ	ェイ間でセキュアなVPNトン。	ネル設定ができます。					
NAT	オンプレミスとの間、この ※IPSec VPNは、両サイ	カテナント内、テナント間にす ドでの接続構成設定が必要と1	対して、サイトツーサィ なります。	(FVPN 숲성	「成できます。			
ファイアワォール	☑ VPNを有効化							
固定ルーティング	公開IPの構成							
NIDU	公開[Pla. それぞれの外約	#キットワークについて構成1	できます。これは、NAT	「を使用し	ている環境におい	いて便利です。		
VEN	名前	ローカルエンドポイント	ピアエンドボイ	有効	ステータス	ローカルネット	ピアネットワーク	ピアテン
ロードバランサー	IPSEC-RTX1210	Y.Y.Y.Y	X.X.X.X	1	1	192.168.0.0/24	192.168.248.0/24	-

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。

ク ピアテナン	ピアネットワーク	ローカルネットワ	ステ	有効	ビアエンドポイ	ローカルエンド	名前	VPIN
18.0/24 -	192.168.248.0/24	192.168.2.0/24	0	1	X.X.X.X	Y.Y.Y.Y	IPSEC-RTX1210	ロードバランサー
4	192.168.2	192.168.2.0/24	0	×.	X.X.X.X	Y.Y.Y.Y	IPSEC-RTX1210	

※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。

® YAMAHA	RTX1210	管理ユーザー:ユーザー名なし ログアウト
匪 ダッシュホード	王_ UNマップ 九 かんたん設定 尊 詳細設定 弐 管 理	CONFIG TECHINFO へレプ

(2). VPN接続状態(拠点間)を有効化し適用をクリックします。

ガジェットの追加と削除		×
 	 ✓リソース情報 □トラフィック情報(PP) ✓VPN接続状態(拠点問) □ファストパスフロー数 □SYSLOG 	 ✓インターフェース情報 □トラフィック情報(TUNNEL) □VPN接続状態(リモートアクセス) □動的フィルターセッション数
		適用 キャンセル

(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。

(*) YAMAHA	RTX1210		管理	ユーザー:ユーザー名なし ログアウト
ダッシュボード	🔚 LANマップ 🧏 かんたん設定	🐥 詳細設定 🔪 管理		CONFIG TECHINFO ヘレプ
1995- SV				
▼ VPN接続状態(拠点	問)	▼ インターフェ	ース情報	<u>^</u>
Up 1 Do	wn 0 Error 0	All 1 🐨 YAMAHA	LAN1	LAN2 RTX1210
設定名 1 Tunnel1	接続種別 インターフェース IPsec接続 TUNNEL[01]	秋態 CONSOLE		L1 / B1 B2

25 / **40** Copyright 2016 SoftBank Corp. All Rights Reserved.



(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。

®YAMAHA RTX 1210		管理ユーザー:ユーザー名なし ログアウト
「	定 气 管 理	CONFIG TECHINFO ヘルプ
▼ VPN接続状態(拠点間)	▼ インターフェース情報	
Up 1 Down 0 Error 0	All 1 SYAMAHA LAN1	LAN2 RTX1210
設定名 接続種別 インターフェース * 1 Tunnel1 IPsec擴続 TUNNEL[01] ●●●	大服 CONSOLE 1 2 3	4 L1/B1B2
	接続状態: 接続中 接続開始時間: 2016/10/28 20:17:25	LAN3 ISDN S/T
	通信時間: 2分8秒 IPv4 受信パケット: 347 パケット(29581 オクテット)	microSD USB DOWN LOAD
▼ システム情報	IPv6 受信パケット:0パケット(0オクテット)	
ファームウェアRev. Rev.14.01.14 (Mon May 30 15:09:02 2016) シリアルNo. S4H042903	IPv6送信パケット:0パケット(0オクテット)	

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。

IE Version:	11.0.9600.18321	
IP Address:	192.168.248.200	
Logon Domain:	☑ 管理者: Windows PowerShell	x
Logon Server:	PS C: Vilcare Vidministrator, ping 192, 168, 0, 150	
MAC Address:	10 C. FOSEISFAGIIIIIIISCIACOI2 PINg 102.100.0.100	
Machine Doma	192.168.0.150 に ping を送信しています 32 バイトのデータ	: 🗖
Memory:	192.168.0.150 からの応答: バイト数 =32 時間 =6ms TTL=63	
Network Card:	192.168.0.150 からの応答: バイト数 =32 時間 =6ms TTL=63	
Network Speec	192.168.0.150 からの応答: バイト数 =32 時間 =5ms TTL=63	
Network Type:	192.168.0.150 からの応答: バイト数 =32 時間 =5ms TTL=63	
OS Version:		
Service Pack:	192.168.0.150の ping 統計:	
Snapshot Time	- ハケット数: 送信 = 4、安信 = 4、損失 = 0(0% の損失). ニウンド レリンゴの押算は問(ミリシ).	
Subnet Mask:	フラフト トリッフの職身时间(ミリ約)・ 	
System Type:	PS C:¥Users¥Administrator>	
User Name:		~
Volumes:	< III	>

(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。

	A	SPIRE	セルコ	フボー	タルサイト			test-adm	in1(ユーザ管 環境設定	理者 サボ
仮想マシン		ליםקל	ネット	ワーク	D7		ユーザ	テナント設定		
+										
仮想マシン										
с III (2: All Field	ls	Sea	arch						
ステータス	メディア	名前	CPU	хŧIJ	os		ネットワーク	IPアドレス	仮想マシングループ	7 🔺
のパワーオン	0	testvm	1vCPU	1GB	CentOS 4/5/6/7 (64-bit)	NIC#0 : APU	192.168.0.150	test-group1	
🙂 パワーオン	0	Win2012	コンワール	を聞く		Serv	NIC#0 : aspi	172.24.0.200	test01	
			パワーオン 05のシャッ	・トダウン						
			パワーオフ							

27 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.

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。

testym (32c36c4123b04d9dbd09d9fab9691368)	Toggle RelativePad	switch Japanes
[root@localhost ~]# ping -c 4 192.168 PING 192.168.248.200 (192.168.248.200 64 bytes from 192.168.248.200: icmp_s 64 bytes from 192.168.248.200: icmp_s 64 bytes from 192.168.248.200: icmp_s 64 bytes from 192.168.248.200: icmp_s	.248.200) 56(84) bytes eq=1 ttl=127 t; eq=2 ttl=127 t; eq=3 ttl=127 t; eq=4 ttl=127 t;	of data. ime=5.95 ms ime=5.67 ms ime=5.86 ms ime=6.03 ms
192.168.248.200 ping statistics 4 packets transmitted, 4 received, 0% rtt min/avg/max/mdev = 5.677/5.882/6.1 [root@localhost ~]#	 packet loss, 1 032/0.142 ms	time 3010ms

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

SoftBank



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: RTX 1210 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。





・ネットワーク図



·設定概念図





・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。

Edgeゲートウェイ ポリシーベースVPN



・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。

RTX1210ルー	ヽベースVPN			Edgeゲート	ウェイ ポリシー・	ベースVPN
送信元	送信先	アクション		送信元	送信先	アクション
オンプレミスNW①	ASPIRE NW(1)	Tunnel1ヘルーティング 🗐		ASPIRE NW ^①	オンプレミスNW①	IPsec VPN Tunnel1 🗐
オンプレミスNW②	ASPIRE NW2	Tunnel2ヘルーティング 🗍		ASPIRE NW2	オンプレミスNW①	IPsec VPN Tunnel2 🗇
オンプレミスNW③	ASPIRE NW3	Tunnel3ヘルーティング 🗐		ASPIRE NW3	オンプレミスNW①	IPsec VPN Tunnel3 🗇
			IPSEC-VPN Tunnel1 オンプレミス NW① ⇔ ASPIRE NW① rface IPSEC-VPN Tunnel2 オンプレミス NW① ⇔ ASPIRE NW2 rface IPSEC-VPN Tunnel3 オンプレミス NW① ⇔ ASPIRE NW3			

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。



32 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.

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	設定するバラメータ
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
固定值	ipsec tunnel コマンドで 設定した値	1で固定 ※	固定值	下記から選択 3des-cbc aes-cbc aes256-cbc	固定值	オンプレミス VPN対象NW	ホワイトクラウド ASPIRE VPN対象NW	固定值

※ISAKMP SAを1本のみ設定する場合

SoftBank

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。

V P Nの構成の追加			X
Y P N 动精成动脉的	名前 * 説明	IPSEC-RTX1210	^
	有効化		
	VPN <i>の</i> 確立先	リモートネットワーク	
	ローカルネットワーク	aspire-demo-nw1 A aspire-demo-nw2 IPSEC-nw2 IPSEC-nw1 APU -SENW01 V	
	ピアネットワーク *	192.168.248.0/24,192.168.:	~

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。

ナービスの構成		[
DHCP IAT ファイアワォール 固定ルーティング	[PSec VPNIま オンプレミスとc ※[PSec VPNIま ✓ VPNを有 : 公開[Pの構 公開[P1ま、それ ²	トウェイ関でゼキュアなVPNトンネル設定ができます。 1. このデナント内、デナント間に対して、サイトツーサイトVPNを構成できます。 1サイドの物気構成設定が必要となります。 と の外線チットワークについて構成できます。これは、NAT 全使用している環境において使利です。
/PN	名前	ビフ有気ス5ローカルネットワーク ビアネットワーク
ードバランサー	IPSEC-R	1 12 🗸 🚫 192.168.2.0/24,192.168.1.0/24,192.168.0 192.168.248.0/24,192.168.249.0/24,192.168
PNの構成の構築	名前 *	IPSEC-RTX1210
	名則 *	IPSEC-RTX1210
	有効化	
		ローカルネットワーク ピアネットワーク 192.168.1.0/24 192.168.2.0/24 192.168.2.0/24 192.168.250.0/24

35 / 40 Copyright 2016 SoftBank Corp. All Rights Reserved.



・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。

サービスの構成											
DHCP NAT ファイアウォール	ファイアウォールにより、 将足のキットワーク トラフィックを許可または拒否するようルール設定できます。これらのルールの順序は、 ルール内の順番で変更するこ とができます。 「 ファイアウォールを有効化 デフォルトアクション ● 拒否 〇 許可										
VPN	順番	* 名前	ソース	ターゲット	プロトコル	アクション	有効				
ロードバランサー	1	IPSEC-IN	192.168.248.0/22:any	192.168.0.0/22:any	任意	許可	1				
	2	IPSEC-OUT	192.168.0.0/22:any	192.168.248.0/22:any	任意	許可	1				

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 (ln/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。

サービスの構成											
DHCP	(PSec VPNIa, ゲートウ	エイ聞でゼキュアなVPNトン。	ネル設定ができます。								
NAT	オンプレミスとの間、このテナント内、テナント間に対して、サイトツーサイトVPNを構成できます。 ※IPSec VPNは、両サイドでの接続構成設定が必要となります。										
ファイアワォール	☑ VPNを有効化										
固定ルーティング	公開IPの構成										
NDN	公開[Pld」それぞれの外部ネットワークについて構成できます。これは、NAT を使用している環境において便利です。										
VEIN	名前	ローカルエンドポイント	ピアエンドボイ	有効	ステータス	ローカルネット	ピアネットワーク	ピアテン			
ロードバランサー	IPSEC-RTX1210	Y.Y.Y.Y	X.X.X.X	~	~	192.168.0.0/24	192.168.248.0/24	20			

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

Copyright 2016 SoftBank Corp. All Rights Reserved.



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

SoftBank 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

SoftBank 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
```