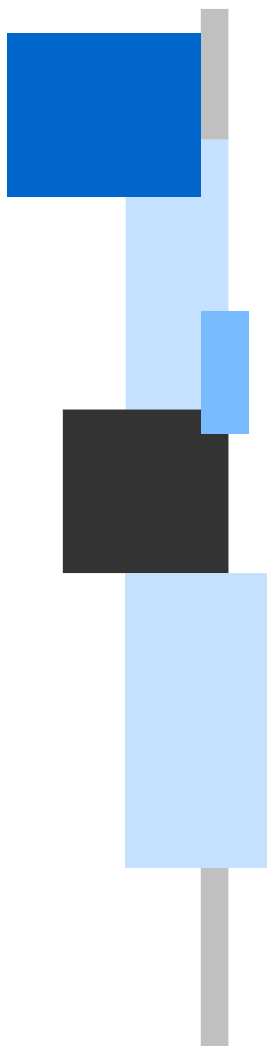




IDCF クラウド

WyOS での IPsec サイト間 VPN 接続ガイド

サービスマニュアル



Ver.1.12

2021 年 4 月 1 日

株式会社 IDC フロンティア

目次

1. はじめに	1
1.1. 想定接続例	1
1.2. IPsec 接続確認機器	2
1.3. 必要な情報 と 構成図 (例)	3
1.4. 通信不可の場合のご注意点	4
1.5. IDCf クラウドコンソールでの作業手順	5
1.5.1. VyOS マシンの作成	6
1.5.2. ネットワークの設定	8
1.6. スタティックルートの設定	10
1.7. VyOS の基本コマンド	11
2. SSG550M の 場合	12
2.1. クラウド側 VyOS の設定	12
2.2. SSG550M の設定	15
3. YAMAHA RTX1200 の 場合	17
3.1. クラウド側 VyOS の設定	17
3.2. YAMAHA RTX1200 の設定	21
4. Cisco7301 の 場合	22
4.1. クラウド側 VyOS の設定	22
4.2. Cisco7301 の設定	25
5. Cisco RVS4000 の 場合	26
5.1. クラウド側 VyOS の設定	26
5.2. Cisco RVS4000 の設定	29
6. VyOS Core 6.4 の 場合	31
6.1. クラウド側 VyOS の設定	31
6.2. ブランチ側 VyOS の設定	34
7. お問い合わせ	35

1. はじめに

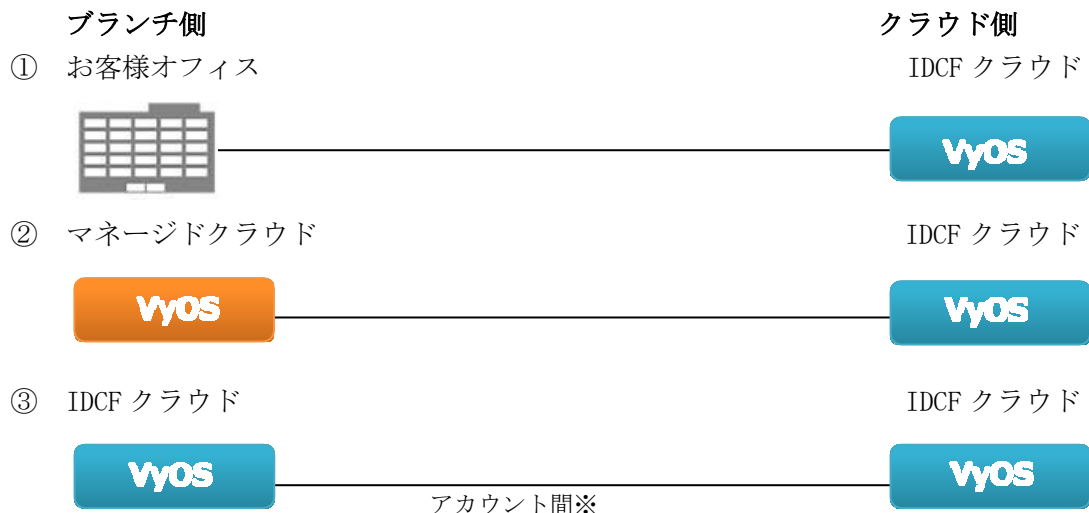
この文書では当社クラウド環境の VyOS での IPsec 接続の設定手順について記載します。
 なお、お客様環境により接続条件等は変わってくるため、接続できることを保証するものではありません。

VyOS は、外部のソフトウェアとなります為、当社サポート対象外となります。接続に関するご不明な点は、以下をご参照ください。

- VyOS マニュアルのダウンロード <http://wiki.vyos-users.jp/ユーザーガイド>
- 設定サポートをご希望の場合、弊社協力会社のご紹介が可能です。ご相談下さい。

また、当ガイドを見て、VyOS を利用したことにより、被った損害、及び損失について、いかなる理由に関わらず、当社は一切責任を負わないものとします。予めご了承ください。

1.1. 想定接続例



【注意】

IDCF クラウドのアカウント間を接続する場合、同一ゾーン同士の IPsec 接続はできません。別ゾーン間でのIPsec 接続は可能です。
同一ゾーン内でプライベート通信を行いたい場合にはプライベートコネクタのご利用をご検討下さい。

1.2. IPsec 接続確認機器

以下は、当社にて、Vyatta CoreOS と IPsec 接続確認を行った機器となります。

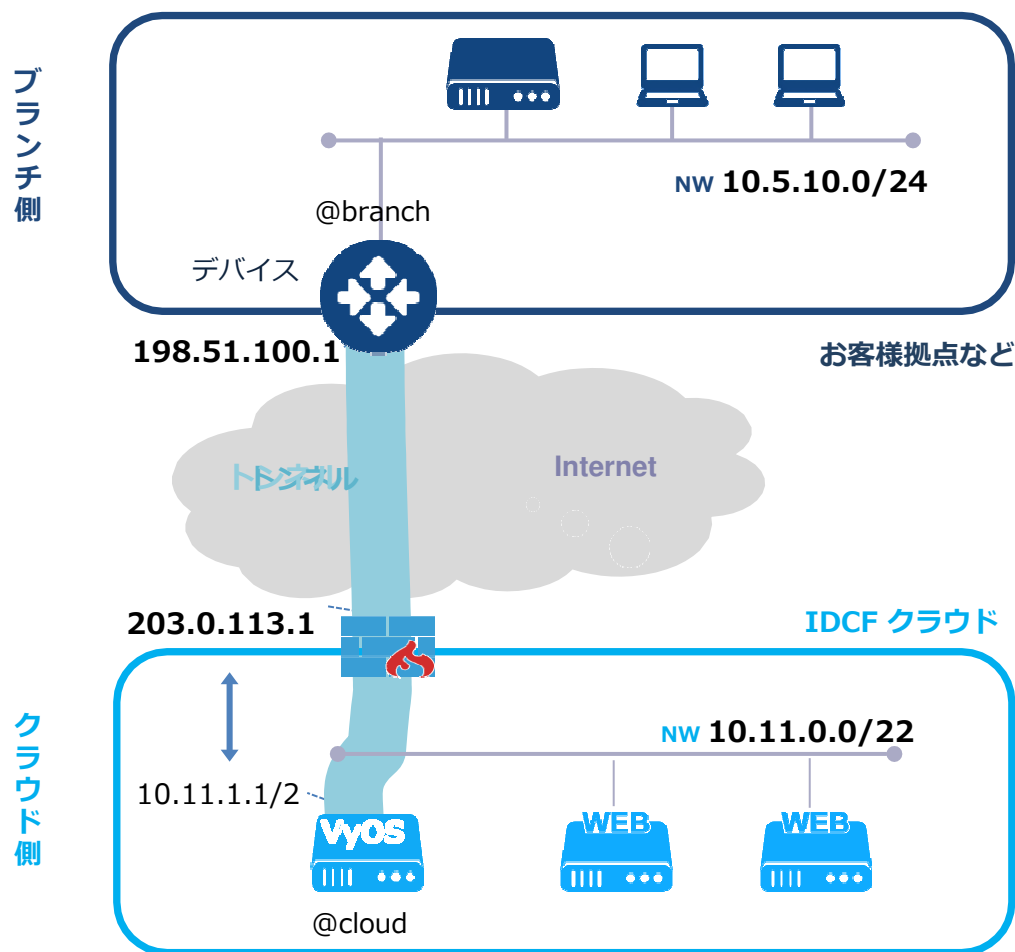
VyOS は Vyatta CoreOS から派生した OS となる為、基本的には同様の動作環境となると考えられます。（※接続を保証するものではありません）

[機器名]	[OS]
■ Juniper SSG550M	(ScreenOS 6.1)
■ YAMAHA RTX1200	(Firmware Version 10.01.38)
■ Cisco7301	(IOS 12.4(25f))
■ Cisco RVS4000	(Firmware Version 2.0.2.7)
■ VyattaOS Core	(VC6.4-2012.05.31)

1.3. 必要な情報と構成図(例)

この文書では、下記構成を例として説明します。値は実際の環境で置き換えて設定してください。この文書では、マネージドクラウド側に環境を「**クラウド側**」、それに対向する接続環境を「**ブランチ側**」と表現します。

ブランチ側	デバイスのグローバル IP アドレス	198.51.100.1	VyOS が IPsec で接続をする IP
	デバイスの ID	branch	<ul style="list-style-type: none"> 任意の文字列。 YAMAHA RTX1200 と Cisco7301 の場合は不要
	ネットワークアドレス	10.5.10.0/24	任意



クラウド側	VyOS に NAT されるパブリック IP アドレス	203.0.113.1	IDCF クラウドコンソールにて取得
	VyOS の eth0 の IP アドレス	10.11.1.1	左記は例。IDCF クラウドコンソールで確認
	VyOS の ID	cloud	<ul style="list-style-type: none"> 任意の文字列 YAMAHA RTX1200 の場合は不要
	ネットワークアドレス	10.11.0.0/22	固定 (サブネットは/22)

項目内容	本書での例	設定可能な選択肢
IPsec 事前共有鍵 (Pre-shared Secret)	my_shared_secret	任意の文字列
IKE で用いる暗号化アルゴリズム	3DES	3DES/AES128/AES256
IKE で用いる認証用ハッシュアルゴリズム	MD5	MD5/SHA1
ESP で用いる暗号化アルゴリズム	3DES	3DES/AES128/AES256
ESP で用いる認証用ハッシュアルゴリズム	MD5	MD5/SHA1

1.4. 通信不可の場合のご注意点

「IPsec セッションは張れており、ping などの小さいパケットは疎通可能であるのに、ファイルなどのパケットが通信できない」というような症状の場合は、以下の事象の可能性があるので、ご注意ください。

上記のような症状が発生する場合、ブランチ側ネットワークまでの途中経路の機器が Path-MTU discovery に対応していない可能性があります。



インターネットの途中経路の機器が ICMP Type=3 (Destination Unreachable) Code=4 (fragmentation needed and DF set) を返してこない場合に、Path-MTU discovery が行えず、MTU サイズを超えるパケットが破棄されてしまいます。

対処方法としては、MTU サイズを変えていただく、または、上記 ICMP メッセージが正しく届くように途中経路でのフィルタの見直し等をしていただく必要があります。



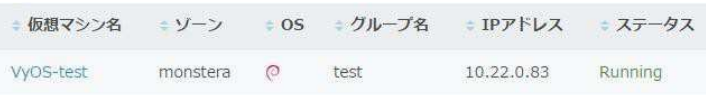
1.5. IDCF クラウドコンソールでの作業手順

IDCF クラウドコンソールで必要な作業について以下にご案内します。
IDCF クラウドコンソールにログインします。 <https://console.idcfcloud.com/>

1.5.1. VyOS マシンの作成

ご説明	操作方法
<p>① VyOS 用のマシンを作成します。</p> <p>コンピューティングから「仮想マシン作成」ボタンをクリックします。</p>	
<p>② ゾーンを選択後、</p> <ul style="list-style-type: none"> - マシンタイプを選択します。 <p>VyOS 用のマシンには S2 以上を推奨いたします。</p> <p>※作成後にスペックの変更が可能ですが、変更にはマシンの停止が伴う場合があります。</p> <p>- イメージ「その他」から、「VyOS...」を選択します。</p> <p>※バージョンは変わる可能性があります。</p>	

ご説明	操作方法															
<div>③ -ボリュームを設定します。</div> <div>必要の場合はCustom Disk で追加ディスクを作成します。(後から追加可能です)</div> <div>-SSH Keyを設定します。</div> <div>-仮想マシン台数を選択します。</div> <div>-ネットワークインターフェースで標準ネットワーク (10.X.0.0/22) を設定します。</div>	<div><div><div>ボリューム</div><div><table><thead><tr><th></th><th>サイズ</th><th>料金 (¥20/GB)</th></tr></thead><tbody><tr><td>ルートディスク ?</td><td>15 GB</td><td>¥300 30日計算</td></tr><tr><td>データディスク (High I/O) ?</td><td><input type="text"/> GB</td><td>¥0 30日計算</td></tr></tbody></table></div></div><div><div>SSH Key</div><div><div>SSH Key 選択作成アップロードなし</div><div>選択して下さい</div></div></div><div><div>基本的には以下のいずれかより選択となります。</div><div>[SSH Key選択] ・ 過去に作成した鍵と同じ鍵を利用する場合</div><div>[作成] ・ 新たに鍵を作成する場合</div><div>※画面に表示されるKey情報は必ずファイルに保存して下さい。</div><div>この画面でしか表示されません。</div><div>[アップロード] ・ 既存の鍵をアップロードする場合</div><div>※当社ではセキュリティ上、公開鍵認証を推奨しておりますが、公開鍵認証を使用しない場合は [なし] を選択してください。(その場合、デフォルトでは外部からの SSH 接続が許可されておりませんので、コンソールからのログインが必要となります。)</div></div><div><div><div>仮想マシン台数 ?</div><div><div>1</div><div>▼</div>台</div></div><div><div>ネットワークインターフェース ?</div><div><div>weber ゾーン</div><div><table><thead><tr><th>ネットワーク名</th><th>CIDR</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> weber-network1</td><td>10.31.0.0/22</td></tr><tr><td><input type="checkbox"/> weber</td><td>192.168.0.0/21</td></tr></tbody></table></div></div></div></div></div>		サイズ	料金 (¥20/GB)	ルートディスク ?	15 GB	¥300 30日計算	データディスク (High I/O) ?	<input type="text"/> GB	¥0 30日計算	ネットワーク名	CIDR	<input checked="" type="checkbox"/> weber-network1	10.31.0.0/22	<input type="checkbox"/> weber	192.168.0.0/21
	サイズ	料金 (¥20/GB)														
ルートディスク ?	15 GB	¥300 30日計算														
データディスク (High I/O) ?	<input type="text"/> GB	¥0 30日計算														
ネットワーク名	CIDR															
<input checked="" type="checkbox"/> weber-network1	10.31.0.0/22															
<input type="checkbox"/> weber	192.168.0.0/21															

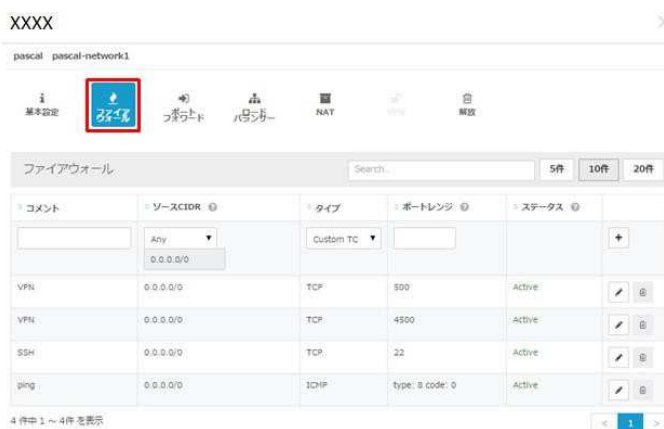
<p>詳細情報で仮想マシン名とグループ名（任意）を設定します。 ※作成後変更可能です</p> <p>確認画面へ進み、マシン情報をご確認の上、「作成」をクリックすると、マシン作成が開始します。</p>	
<p>④ マシン作成が開始されると、[仮想マシン]画面の一覧に表示されます。</p>	
<p>⑤ 仮想マシンの作成が完了すると、メールで初期パスワードが送信されますので、お客様にて保存してください。</p> <p><u>仮想マシンのログインIDは「vyos」となります。</u></p>	<ul style="list-style-type: none"> ・初期パスワードは、仮想マシンを作成したユーザーのメールアドレスにメールで送信されます。 ・パスワードを忘れた場合は、パスワードリセットで再設定が可能です。リセット時に仮想マシンの停止が必要です。 <p><u>セキュリティ上、初期パスワードは変更することを推奨します。</u></p>
<p>⑥ [仮想マシン] の画面で、作成した仮想マシンのステータスが「Running」になっていれば仮想マシン作成の完了です。</p>	

1.5.2. ネットワークの設定

ご説明	操作方法
<p>① [IPアドレス] を開きます。</p> <p>VPN接続に使用するパブリックIPアドレスを取得します。(有償)</p> <p>[IPアドレス取得] をクリック。</p>	<div data-bbox="860 383 1153 454" data-label="Image"> </div> <p>※ソースと書かれているIPアドレスはVyOS用には使用できません。VyOSではパブリックIPアドレスとプライベートIPアドレスが1対1に紐付けられている必要がありますが、ソースのIPアドレスは、仮想マシンと1対1に紐付け(スタティックNAT)が設定できない為です。</p>
<p>② 任意のIPアドレス名を入力し、VyOSを利用するゾーンとネットワークを選択します。</p> <p>「取得する」をクリックします。</p>	<div data-bbox="676 831 1334 1077" data-label="Image"> </div>
<p>③ 追加されたIPアドレスを選択します。</p> <p>画面右の設定ボタンをクリックします。</p> <p>[NAT] タブを選択し、スタティックNATを設定するVyOSの仮想マシンを選択し[有効化]をクリックします。</p>	<div data-bbox="684 1216 1374 1503" data-label="Image"> </div> <p>※[ポートフォワード]や[ロードバランサー]で設定しないでください。</p>

④ 追加したIPアドレスを選択した状態で、[ファイアウォール] タブを選択します。

※全てのプロトコル、ポートが
閉じられた状態から、設定した
部分のみが開放されます。



以下の設定を行います。

- ICMP ICMPタイプ: 8 ICMPコード: 0 [ping用]
- TCP ポート: 22番 [SSH用]
- UDP ポート: 4500番 [VPN用]
- UDP ポート: 500番 [VPN用]

※ソースCIDR :

許可する接続元CIDRを指定してください。

上記例では指定無し「0.0.0.0/0」としていますが、セキュリティ上、必要なソースを指定することを推奨します。
例えば、[VPN用]であれば、ブランチ側のパブリックIPアドレスを指定します。

- IPアドレス単位の場合は /32 で設定します。
- 複数 CIDR の場合は「カンマ」区切りで設定可能です。

※ポ一卜：

ファイアウォールで解放するポートの範囲を設定します。

上記例では [SSH 用] にて 22 番を指定していますが、セキュリティ上、お客様任意のポートにて指定することを推奨します。

1.6. スタティックルートの設定

クラウド側の各仮想マシン内にて、VyOS 向けのスタティックルートを設定する必要があります。

Linux 系 OS の場合

1. 下記のようにルーティングのファイルを作成する。

```
vi /etc /sysconfig/network-scripts/route-eth0
    ベアメタルサーバーの場合、/route-bond1
10.5.10.0/24 via 10.11.1.1(例)
[宛先ネットワーク] via [ゲートウェイ IP]
```

2. 反映の為、以下コマンドを実行

※SSH 接続や通信が切断されるのでコンソールから実施してください。

```
# ifdown eth0      ←eth0 を停止
# ifup eth0        ←eth0 を起動
```

3. 正しく設定されているか確認

```
# ip route show
```

Windows 系 OS の場合

1. コマンドプロンプトを起動

```
netstat -r 現在のルーティング状況を確認
```

2. 下記のようなコマンドを実行し、ルーティング設定（Administrator 権限で）

```
route -p add 10.5.10.0/24 mask 255.0.0.0 10.11.1.1 (例)
[宛先ネットワーク] [ネットマスク] [ゲートウェイ IP]
```

※オプションの-p を入れることで OS 再起動後も設定が残ります。

3. 正しく反映されているか確認

```
netstat -r 「固定ルート」の欄に正しく追加されていることを確認
```

1.7. VyOS の基本コマンド

VyOS の基本コマンドは以下となります。

■ モードの移行

VyOS には 2 種類のモードがあり、モードを移行して編集を行います。

- 一般モード：vyos@vyos:~\$ （設定状態や動作状態の参照モード）
- 設定モード：vyos@vyos# （設定ファイルの編集を行うモード）

```
$ configure    一般モード から 設定モードへ移行
# exit        設定モードから 一般モードへ戻る
```

■ 設定の保存方法

```
# commit    設定の反映
# save       設定の保存。commit で反映させた後に使用
```

※commit だけでは、マシン再起動後に設定が消えてしまいます。

■ 設定内容の確認方法

接続が出来ない時などは、これらのコマンドにて設定内容を確認してください。

```
?                ヘルプ。コマンド一覧（両モードで実行できます）
$ show ?        show の後に指定できるコマンド一覧（一般モード）
$ show c?       show c の後に続けて指定できるコマンド一覧
$ show c? を二回  show c の後に続けて指定できるコマンドの説明

$ show configuration    設定内容の参照（一般モードで実行する場合）
# run show configuration 設定内容の参照（設定モードで実行する場合）
$ show ip route         ルーティングの確認
$ show vpn ike sa       IKE SA の確認
$ show vpn ipsec sa     ESP SA の確認
$ show log vpn ipsec    IPsec 関連のログ確認
```

■ 設定方法

設定手順（検証例）は、次項よりご案内します。

機器毎に章が分かれており、はじめにクラウド側 VyOS の設定手順を説明し、その後それぞれの対向となるデバイスの設定手順を説明します。

2. SSG550M の場合

以下に設定手順をご案内します。設定内容は例となります。適宜変更して設定してください。

2.1. クラウド側 VyOS の設定

1. IPsec の通信に用いるインターフェースの設定

```
set vpn ipsec ipsec-interfaces interface eth0
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

2. IKE グループの設定

```
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des
set vpn ipsec ike-group IKE-G proposal 1 hash md5
set vpn ipsec ike-group IKE-G lifetime 3600
```

設定例では、以下の内容を定義しています。

- ike-group (IKE グループ名) : IKE-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (IKE の有効期限) : 3600 秒 (1 時間) ※IKE の鍵交換間隔

* encryption と hash は複数種類登録が可能です。「proposal 1」とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

3. ESP グループの設定

```
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des
set vpn ipsec esp-group ESP-G proposal 1 hash md5
set vpn ipsec esp-group ESP-G lifetime 1800
```

設定例では、以下の内容を定義しています。

- esp-group (ESP グループ名) : ESP-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (ESP の有効期限) : 1800 秒 (30 分) ※ESP の交渉間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

4. NAT トラバーサルの設定の有効化

```
set vpn ipsec nat-traversal enable
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

5. ブランチ側デバイスとの通信で用いる IKE グループと ESP グループを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 ike-group IKE-G  
set vpn ipsec site-to-site peer 198.51.100.1 default-esp-group ESP-G
```

*IP アドレスは実際の設定に置き換えてください。

- 198.51.100.1 は、ブランチ側デバイスのパブリック IP アドレスに置き換え。

(これ以降も同様に置き換えてください)

6. 接続で用いる認証方式を事前共有鍵方式に設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication mode pre-shared-secret  
  
set vpn ipsec site-to-site peer 198.51.100.1 authentication pre-shared-secret  
my_shared_secret (*1行で入力してください)
```

*「my_shared_secret」の部分は、実際の IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列) で置き換えてください。

7. 自分自身 (クラウド側 VyOS) の ID と対向デバイス (ブランチ側デバイス) の ID を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication id @cloud  
set vpn ipsec site-to-site peer 198.51.100.1 authentication remote-id @branch
```

クラウド側 VyOS とブランチ側デバイスの ID を付加します。

*ID の頭に@ (半角) を入力します。

*cloud と branch の部分は実際の値に置き換えてください。

8. 自分自身（クラウド側 VyOS）の eth0 の IP アドレスを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 local-address 10.11.1.1
```

*IP アドレスは実際の設定に置き換えてください。

- 198.51.100.1 は、ブランチ側デバイスのパブリック IP アドレスに置き換え
- 10.11.1.1 は、クラウド側 VyOS の eth0 の IP アドレスに置き換え
(これ以降も同様に置き換えてください)

9. IPsec トンネルを通す宛先ネットワークと送信元ネットワークの対を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 local prefix 10.11.0.0/22
```

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 remote prefix 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

- 10.11.0.0/22 は、クラウド側のネットワークに置き換え
- 10.5.10.0/24 は、ブランチ側のネットワークに置き換え

10. ファイアウォールのルール設定

```
set firewall name FW_RULE rule 100 action accept
set firewall name FW_RULE rule 100 source address 10.11.0.0/22
set firewall name FW_RULE rule 110 action accept
set firewall name FW_RULE rule 110 source address 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

*rule 番号（上記 100 と 110）は任意で設定します。

上記例では、「FW_RULE」という名前（任意）のルールにて、クラウド側のネットワークアドレスとブランチ側のネットワークアドレスからのパケットを許可する設定を追加しています。VyOS では、Firewall のルールで許可されていないパケットは拒否されます。

*もし eth0 に対して送受信時のフィルタを定義している場合（set interfaces ethernet eth0 firewall in の設定がされている場合）は、クラウド側のネットワークとブランチ側のネットワークの双方で通信ができるためのルールが設定されている必要があります。

*また、VyOS 自身に対してフィルタを定義している場合（set interfaces ethernet eth0 firewall local の設定がされている場合）は peer 同士の IP アドレスを許可する設定が必要となります。

11. 設定の反映

```
sudo /etc/init.d/ipsec restart
```


2.2. SSG550M の設定

ここでは以下の構成を例に説明します。設定内容は例となります。適宜変更して設定してください。

トンネルインターフェース	tunnel.1
WAN 側の Ethernet インターフェース	ethernet0/2
VPN 設定 ID	0x1
IKE 設定名	ike_cloud
VPN 設定名	vpn_cloud

すでに複数の IPsec サイト間接続 VPN の設定がされている場合は、すでにトンネルインターフェース tunnel.1 と VPN 設定 ID 0x1 が使用されている可能性があります。そのときは tunnel.2、 tunnel.3、や 0x2、 0x3 で適宜置き換えてください。

1. トンネルインターフェースのゾーンを “Untrust” に設定

```
set interface "tunnel.1" zone "Untrust"
```

2. トンネルインターフェースと WAN 側インターフェースの対応付け

```
set interface tunnel.1 ip unnumbered interface ethernet0/2
```

3. IKE の設定

```
set ike gateway "ike_cloud" address 203.0.113.1 id "cloud" Main local-id "branch"
outgoing-interface "ethernet0/2" preshare "my_shared_secret" proposal "pre-g2-3des-md5" (* 1 行で入力してください)
```

設定例では、以下の内容を定義しています。

- ike_cloud →IKE 設定名
- 203.0.113.1 →クラウド側 VyOS に NAT されるパブリック IP アドレスに置き換え
- branch →ブランチ側デバイスの ID に置き換え
- cloud →クラウド側 VyOS の ID に置き換え
- ethernet0/2 →WAN 側の Ethernet インターフェース
- my shared secret →IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列)
- pre-g2-3des-md5 →IKE で用いる暗号化アルゴリズムとハッシュアルゴリズムに対応する値

4. NAT トラバーサルの設定

```
set ike gateway "ike_cloud" nat-traversal
set ike gateway "ike_cloud" nat-traversal udp-checksum
set ike gateway "ike_cloud" nat-traversal keepalive-frequency 5
```

NAT のステータスを保持するためキープアライブの設定も行います。
上記の例では 5 秒間隔で実施します。

5. VPN の設定

```
set vpn "vpn_cloud" gateway "ike_cloud" no-replay tunnel idletime 0 proposal "g2-esp-3des-md5" (*1 行で入力してください)
```

- 「vpn_cloud」は VPN 設定名に置き換え。
- 「g2-esp-3des-md5」は ESP で用いる暗号化アルゴリズムとハッシュアルゴリズムに対応する値に、それぞれ置き換えてください。

6. VPN の設定をトンネルインターフェースとバインド

```
set vpn "vpn_cloud" id 0x1 bind interface tunnel.1

set vpn "vpn_cloud" proxy-id local-ip 10.5.10.0/24 remote-ip 10.11.0.0/22 "ANY"
```

- 「0x1」は実際の VPN 設定 ID に置き換え。
- 「10.5.10.0/24」はブランチ側のネットワークアドレスに置き換え。
- 「172.16.1.0/24」はクラウド側のネットワークアドレスに置き換え。

7. ルーティングの設定

```
set route 10.11.0.0/22 interface tunnel.1
```

宛先ネットワーク

*ネットワークアドレスは実際の設定に置き換えてください。
クラウド側ネットワーク宛のパケットが、トンネルを通るようにするルーティング設定

3. YAMAHA RTX1200 の場合

以下に設定手順をご案内します。設定内容は例となります。適宜変更して設定して下さい。

YAMAHA RTX1200 では、NAT-Traversal 機能を利用し、ID と IP アドレスが一致しない構成で IPsec を利用したい場合、IKE phase 1 で Aggressive mode しかサポートしていません。一方 VyOS は Main mode しかサポートしていません。

そのため IPIP トンネルを設定し、その上で IPsec トンネルを設定する必要があります。

IPsec の前にトンネリングが行われるような構成の場合には、そのトンネリングに使われる通信をファイアウォールを許可する必要があります。

(※なお、IDCF クラウドコンソールの [ファイアウォール] では、IPIP 通信のフィルタ解除のルール設定が出来ません。しかし、VyOS から対向機器に対しVPN 通信を行ったタイミングで、動的に当社ファイアウォールでの IPIP 通信のフィルタが解除される為、対向側からのVPN 通信も到達可能となりますので、問題ありません。)

IPIP トンネルをつなぐ為の対向する IP アドレスを、以下を例として設定ご案内します。

- 192.168.123.1/24 (クラウド側 VyOS)
- 192.168.123.2/24 (ブランチ側 YAMAHA RTX1200)

※この 2 つの IP アドレスは、同じセグメントの任意のプライベート IP アドレスを設定します。接続するVPN 環境内で、他で使われていないネットワークアドレスを設定してください。

3.1. クラウド側 VyOS の設定

1. IPIP トンネルの設定を行います。

```
set interfaces tunnel tun0 address 192.168.123.1/24
set interfaces tunnel tun0 encapsulation ipip
set interfaces tunnel tun0 local-ip 10.11.1.1
set interfaces tunnel tun0 mtu 1422
set interfaces tunnel tun0 remote-ip 198.51.100.1
```

*IP アドレスは実際の設定に置き換えてください。

- 10.11.1.1 は、クラウド側 VyOS の eth0 の IP アドレスに置き換え。
- 198.51.100.1 は、ブランチ側デバイスのパブリック IP アドレスに置き換え。

2. IPsec の通信に用いるインターフェースの設定

```
set vpn ipsec ipsec-interfaces interface eth0
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

3. IKE グループの設定

```
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des  
set vpn ipsec ike-group IKE-G proposal 1 hash md5  
set vpn ipsec ike-group IKE-G lifetime 3600
```

設定例では、以下の内容を定義しています。

- ike-group (IKE グループ名) : IKE-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (IKE の有効期限) : 3600 秒 (1 時間) ※IKE の鍵交換間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

4. ESP グループの設定

```
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des  
set vpn ipsec esp-group ESP-G proposal 1 hash md5  
set vpn ipsec esp-group ESP-G lifetime 1800
```

設定例では、以下の内容を定義しています。

- esp-group (ESP グループ名) : ESP-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (ESP の有効期限) : 1800 秒 (30 分) ※ESP の交渉間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

5. ブランチ側デバイスとの通信で用いる IKE グループと ESP グループを設定

```
set vpn ipsec site-to-site peer 192.168.123.2 ike-group IKE-G
set vpn ipsec site-to-site peer 192.168.123.2 default-esp-group ESP-G
```

6. 接続で用いる認証方式を事前共有鍵方式に設定

```
set vpn ipsec site-to-site peer 192.168.123.2 authentication mode pre-shared-secret

set vpn ipsec site-to-site peer 192.168.123.2 authentication pre-shared-secret
my_shared_secret (*1 行で入力してください)
```

*「my_shared_secret」の部分は実際の IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列) で置き換えてください。

7. 自分自身 (クラウド側 VyOS) の tun0 の IP アドレスを設定

```
set vpn ipsec site-to-site peer 192.168.123.2 local-address 192.168.123.1
```

*192.168.123.1 の部分は実際のクラウド側 VyOS の tun0 の IP アドレスの値に置き換えてください。

8. IPsec トンネルを通す宛先ネットワークと送信元ネットワークの対を設定

```
set vpn ipsec site-to-site peer 192.168.123.2 tunnel 1 local prefix 10.11.0.0/22

set vpn ipsec site-to-site peer 192.168.123.2 tunnel 1 remote prefix 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

- 10.11.0.0/22 は実際のクラウド側ネットワークアドレスに置き換え
- 10.5.10.0/24 は実際のブランチ側のネットワークに置き換え

9. ファイアウォールのルール設定

```
set firewall name FW_RULE rule 100 action accept
set firewall name FW_RULE rule 100 source address 10.11.0.0/22

set firewall name FW_RULE rule 110 action accept
set firewall name FW_RULE rule 110 source address 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

*rule 番号（上記 100 と 110）は任意で設定します。

上記例では、「FW_RULE」という名前（任意）のルールにて、クラウド側のネットワークアドレスとブランチ側のネットワークアドレスからのパケットを許可する設定を追加しています。

VyOS では、Firewall のルールで許可されていないパケットは拒否されます。

*もし eth0 に対して送受信時のフィルタを定義している場合（set interfaces ethernet eth0 firewall in の設定がされている場合）は、クラウド側のネットワークとブランチ側のネットワークの双方で通信ができるためのルールが設定されている必要があります。

*また、VyOS 自身に対してフィルタを定義している場合（set interfaces ethernet eth0 firewall local の設定がされている場合）は peer 同士の IP アドレスを許可する設定が必要となります。

10. 設定の反映

```
sudo /etc/init.d/ipsec restart
```

3.2. YAMAHA RTX1200 の設定

1. IPIP トンネルの設定を行います。

```
tunnel select 1
tunnel encapsulation ipip
tunnel endpoint address 192.51.100.1 203.0.113.1
ip tunnel address 192.168.123.2/24
tunnel enable 1
```

*203.0.113.1 はクラウド側 VyOS のパブリック IP アドレスに置き換えてください。

2. IPsec の設定

```
tunnel select 2
ipsec tunnel 2
ipsec sa policy 2 2 esp 3des-cbc md5-hmac
ipsec ike duration ipsec-sa 2 1800
ipsec ike encryption 2 3des-cbc
ipsec ike group 2 modp1024
ipsec ike hash 2 md5
ipsec ike keepalive use 2 on icmp-echo 10.11.1.1
ipsec ike local address 2 192.168.123.2
ipsec ike pre-shared-key 2 text my_shared_secret
ipsec ike remote address 2 192.168.123.1
tunnel enable 2
ipsec auto refresh on
```

*10.11.1.1 はクラウド側 VyOS の eth0 の IP アドレスに置き換えて下さい。

IPIP トンネル上で NAT-Traversal を利用しない IPsec トンネルを設定する場合、IPIP トンネルのセッションがタイムアウトすることで通信ができなくなる可能性があります。そのため ipsec ike keepalive コマンドでキープアライブの設定を行います。

3. ルーティングの設定

```
ip route 10.11.0.0/22 gateway tunnel 2
宛先ネットワーク
```

*ネットワークアドレスは実際の設定に置き換えてください。

クラウド側ネットワーク宛のパケットが、トンネルを通るようにするルーティング設定

4. Cisco7301 の場合

以下に設定手順をご案内します。設定内容は例となります。適宜変更して設定してください。

4.1. クラウド側 VyOS の設定

1. IPsec の通信に用いるインターフェースの設定

```
set vpn ipsec ipsec-interfaces interface eth0
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

2. IKE グループの設定

```
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des  
set vpn ipsec ike-group IKE-G proposal 1 hash md5  
set vpn ipsec ike-group IKE-G lifetime 3600
```

設定例では、以下の内容を定義しています。

- ike-group (IKE グループ名) : IKE-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (IKE の有効期限) : 3600 秒 (1 時間) ※IKE の鍵交換間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

3. ESP グループの設定

```
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des  
set vpn ipsec esp-group ESP-G proposal 1 hash md5  
set vpn ipsec esp-group ESP-G lifetime 1800
```

設定例では、以下の内容を定義しています

- esp-group (ESP グループ名) : ESP-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (ESP の有効期限) : 1800 秒 (30 分) ※ESP の交渉間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

4. NAT トラバーサルを設定を有効化

```
set vpn ipsec nat-traversal enable
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

5. ブランチ側デバイスとの通信で用いる IKE グループと ESP グループを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 ike-group IKE-G  
set vpn ipsec site-to-site peer 198.51.100.1 default-esp-group ESP-G
```

198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスで置き換えてください。(これ以降も同様に置き換えてください。)

6. 接続で用いる認証方式を事前共有鍵方式に設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication mode pre-shared-secret  
  
set vpn ipsec site-to-site peer 198.51.100.1 authentication pre-shared-secret  
my_shared_secret (*1 行で入力してください)
```

* 「my_shared_secret」の部分は実際の IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列) で置き換えてください。

7. クラウド側 VyOS の ID を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication id @cloud
```

ID の設定には ID の頭に “@ (アットマーク)” を付加します。cloud の部分は実際の値に置き換えてください。

8. クラウド側 VyOS の eth0 の IP アドレスを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 local-address 10.11.1.1
```

*10.11.1.1 の部分は実際のクラウド側 VyOS の eth0 の IP アドレスの値に置き換えてください。

9. IPsec トンネルを通す宛先ネットワークと送信元ネットワークの対を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 local prefix 10.11.0.0/22  
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 remote prefix 10.5.10.0/24
```

- 198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスに置き換え
- 10.11.0.0/22 は実際のクラウド側のネットワークアドレスに置き換え
- 10.5.10.0/24 は実際のブランチ側のネットワークに置き換え

10. ファイアウォールのルール設定

```
set firewall name FW_RULE rule 100 action accept  
set firewall name FW_RULE rule 100 source address 10.11.0.0/22  
set firewall name FW_RULE rule 110 action accept  
set firewall name FW_RULE rule 110 source address 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

*rule 番号（上記 100 と 110）は任意で設定します。

上記例では、『FW_RULE』という名前（任意）のルールにて、クラウド側のネットワークアドレスとブランチ側のネットワークアドレスからのパケットを許可する設定を追加しています。

VyOS では、Firewall のルールで許可されていないパケットは拒否されます。

*もし eth0 に対して送受信時のフィルタを定義している場合（set interfaces ethernet eth0 firewall in の設定がされている場合）は、クラウド側のネットワークとブランチ側のネットワークの双方で通信ができるためのルールが設定されている必要があります。

*また、VyOS 自身に対してフィルタを定義している場合（set interfaces ethernet eth0 firewall local の設定がされている場合）は peer 同士の IP アドレスを許可する設定が必要となります。

11. 設定の反映

```
sudo /etc/init.d/ipsec restart
```

4.2. Cisco7301 の設定

1. IKE の設定

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key my_shared_secret address 203.0.113.1
crypto isakmp nat keepalive 20
```

*203.0.113.1 はクラウド側 VyOS のパブリック IP に置き換えてください。

2. IPsec のポリシーを設定

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

*上記例では、myset という名前（任意）でポリシーを定義しています。

3. 対向の ID を定義

```
crypto identity cloudid
  fqdn cloud
```

*上記例では、cloudid という名前（任意）で cloud という ID を設定しています。

4. IPsec ピアの設定

```
crypto map myvpn 10 ipsec-isakmp
  set peer 203.0.113.1
  set transform-set myset
  set identity cloudid
  match address 101
```

*上記例では、myvpn という名前（任意）で設定しています。

5. IPsec トンネルを通す IP パケットの定義

```
access-list 101 permit ip 10.5.10.0 0.0.0.255 10.11.0.0 0.0.3.255
```

5. Cisco RVS4000 の場合

以下に設定手順をご案内します。設定内容は例となります。適宜変更して設定してください。

5.1. クラウド側 VyOS の設定

1. IPsec の通信に用いるインターフェースの設定

```
set vpn ipsec ipsec-interfaces interface eth0
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

2. IKE グループの設定

```
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des
set vpn ipsec ike-group IKE-G proposal 1 hash md5
set vpn ipsec ike-group IKE-G lifetime 3600
```

設定例では、以下の内容を定義しています。

- ike-group (IKE グループ名) : IKE-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (IKE の有効期限) : 3600 秒 (1 時間) ※IKE の鍵交換間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

3. ESP グループの設定

```
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des
set vpn ipsec esp-group ESP-G proposal 1 hash md5
set vpn ipsec esp-group ESP-G lifetime 1800
```

設定例では、以下の内容を定義しています。

- esp-group (ESP グループ名) : ESP-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (ESP の有効期限) : 1800 秒 (30 分) ※ESP の交渉間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

4. NAT トラバーサルの設定の有効化

```
set vpn ipsec nat-traversal enable
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

5. ブランチ側デバイスとの通信で用いる IKE グループと ESP グループを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 ike-group IKE-G  
set vpn ipsec site-to-site peer 198.51.100.1 default-esp-group ESP-G
```

* 198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスで置き換えてください。(これ以降も同様に置き換えてください。)

6. 接続で用いる認証方式を事前共有鍵方式に設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication mode pre-shared-secret  
  
set vpn ipsec site-to-site peer 198.51.100.1 authentication pre-shared-secret  
my_shared_secret (*1 行で入力してください)
```

* 「my_shared_secret」の部分は実際の IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列) で置き換えてください。

7. ID 設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication id @cloud  
set vpn ipsec site-to-site peer 198.51.100.1 authentication remote-id @branch
```

クラウド側 VyOS とブランチ側デバイスの ID を設定します。

*ID の頭に@ (半角) を付加します。

*cloud と branch の部分は実際の値に置き換えてください。

8. 自分自身（クラウド側 VyOS）の eth0 の IP アドレスを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 local-address 10.11.1.1
```

上記の実行例のうち 10.11.1.1 の部分は実際のクラウド側 VyOS の eth0 の IP アドレスの値に置き換えてください。

9. IPsec トンネルを通す宛先ネットワークと送信元ネットワークの対を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 local prefix 10.11.0.0/22
```

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 remote prefix 10.5.10.0/24
```

- 198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスに置き換え
- 10.11.0.0/22 は実際のクラウド側のネットワークアドレスに置き換え
- 10.5.10.0/24 は実際のブランチ側のネットワークに置き換え

10. ファイアウォールのルール設定

```
set firewall name FW_RULE rule 100 action accept
set firewall name FW_RULE rule 100 source address 10.11.0.0/22
set firewall name FW_RULE rule 110 action accept
set firewall name FW_RULE rule 110 source address 10.5.10.0/24
```

*ネットワークアドレスは実際の設定に置き換えてください。

*rule 番号（上記 100 と 110）は任意で設定します。

上記例では、「FW_RULE」という名前（任意）のルールにて、クラウド側のネットワークアドレスとブランチ側のネットワークアドレスからのパケットを許可する設定を追加しています。

VyOS では、Firewall のルールで許可されていないパケットは拒否されます。

*もし eth0 に対して送受信時のフィルタを定義している場合（set interfaces ethernet eth0 firewall in の設定がされている場合）は、クラウド側のネットワークとブランチ側のネットワークの双方で通信ができるためのルールが設定されている必要があります。

*また、VyOS 自身に対してフィルタを定義している場合（set interfaces ethernet eth0 firewall local の設定がされている場合）は peer 同士の IP アドレスを許可する設定が必要となります。

11. 設定の反映

```
sudo /etc/init.d/ipsec restart
```

5.2. Cisco RVS4000 の設定



1. ローカルセキュリティゲートウェイのタイプを“IP とドメイン名 (FQDN)による認証” に設定します。
2. ドメイン名にブランチ側デバイスの ID (この例では“branch”) を設定します。
3. ローカルセキュリティのグループを“サブネット” に設定し、IP アドレスとサブネットマスクにブランチ側のネットワーク情報を入力します。



1. リモートセキュリティゲートウェイのタイプを“IP とドメイン名 (FQDN)による認証” に設定します。
2. ドメイン名にクラウド側 VyOS の ID (この例では“cloud”) を設定します。
3. IP アドレスにクラウド側 VyOS のパブリック IP アドレスを入力します。
4. リモートセキュリティグループのタイプを“サブネット” にし、クラウド側ネットワークの情報を入力します。



1. キー入力モードを“事前共有キー付きIKE”にし、暗号化、認証、グループをそれぞれ設定します。
2. 事前共有キーにクラウド側 VyOS で設定した事前共有キーを入力します。

6. VyOS Core 6.4 の場合

クラウド側 VyOS とブランチ側VyOS（お客様用意／IDCF クラウド／マネージド）を接続する場合は、以下の手順となります。設定内容は例となります。適宜変更して設定して下さい。

【注意】 IDCF クラウドのアカウント間を接続する場合、同一ゾーン同士の IPsec 接続はできません。別ゾーン間での IPsec 接続は可能です。同一ゾーン内でプライベート通信を行いたい場合にはプライベートコネクトのご利用をご検討下さい。

6.1. クラウド側 VyOS の設定

1. IPsec の通信に用いるインターフェースの設定

```
set vpn ipsec ipsec-interfaces interface eth0
```

（これは当社初期設定で投入されていますので設定の必要はありません。）

2. IKE グループの設定

```
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des
set vpn ipsec ike-group IKE-G proposal 1 hash md5
set vpn ipsec ike-group IKE-G lifetime 3600
```

設定例では、以下の内容を定義しています。

- ike-group (IKE グループ名) : IKE-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (IKE の有効期限) : 3600 秒 (1 時間) ※IKE の鍵交換間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

3. ESP グループの設定

```
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des
set vpn ipsec esp-group ESP-G proposal 1 hash md5
set vpn ipsec esp-group ESP-G lifetime 1800
```

設定例では、以下の内容を定義しています。

- esp-group (ESP グループ名) : ESP-G 任意の名前を設定
- encryption (暗号化アルゴリズム) : 3DES
- hash (認証用ハッシュアルゴリズム) : MD5
- lifetime (ESP の有効期限) : 1800 秒 (30 分) ※ESP の交渉間隔

* encryption と hash は複数種類登録が可能です。proposal 1 とは異なる encryption と hash を、「proposal 2」、「proposal 3」として、同じグループ名で設定します。

4. NAT トラバーサルの設定の有効化

```
set vpn ipsec nat-traversal enable
```

(これは当社初期設定で投入されていますので設定の必要はありません。)

5. ブランチ側デバイスとの通信で用いる IKE グループと ESP グループを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 ike-group IKE-G  
set vpn ipsec site-to-site peer 198.51.100.1 default-esp-group ESP-G
```

*198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスで置き換えてください。(これ以降も同様に置き換えてください。)

6. 接続で用いる認証方式を事前共有鍵方式に設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication mode pre-shared-secret  
  
set vpn ipsec site-to-site peer 198.51.100.1 authentication pre-shared-secret  
my_shared_secret (*1 行で入力してください)
```

*「my_shared_secret」の部分は実際の IPsec 事前共有鍵 [Pre-shared Secret] (任意の文字列) で置き換えてください。

7. ID 設定

```
set vpn ipsec site-to-site peer 198.51.100.1 authentication id @cloud  
set vpn ipsec site-to-site peer 198.51.100.1 authentication remote-id @branch
```

クラウド側 VyOS とブランチ側デバイスの ID を設定します。

*ID の頭に@ (半角) を付加します。

* cloud と branch の部分は実際の値に置き換えてください。

8. 自分自身 (クラウド側 VyOS) の eth0 の IP アドレスを設定

```
set vpn ipsec site-to-site peer 198.51.100.1 local-address 10.11.1.1
```

* 10.11.1.1 の部分は実際のクラウド側 VyOS の eth0 の IP アドレスの値に置き換えてください。

9. IPsec トンネルを通す宛先ネットワークと送信元ネットワークの対を設定

```
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 local prefix 10.11.0.0/22  
set vpn ipsec site-to-site peer 198.51.100.1 tunnel 1 remote prefix 10.5.10.0/24
```

*IP アドレスは実際の設定に置き換えてください。

- 198.51.100.1 は実際のブランチ側デバイスのパブリック IP アドレスに置き換え
- 10.11.0.0/22 は実際のクラウド側のネットワークアドレスに置き換え
- 10.5.10.0/24 は実際のブランチ側のネットワークに置き換え

10. ファイアウォールのルール設定

```
set firewall name FW_RULE rule 100 action accept  
set firewall name FW_RULE rule 100 source address 10.11.0.0/22  
  
set firewall name FW_RULE rule 110 action accept  
set firewall name FW_RULE rule 110 source address 10.5.10.0/24
```

*ネットワークアドレスは実際の設定に置き換えてください。

*rule 番号（上記 100 と 110）は任意で設定します。

上記例では、「FW_RULE」という名前（任意）のルールにて、クラウド側のネットワークアドレスとブランチ側のネットワークアドレスからのパケットを許可する設定を追加しています。

VyOS では、Firewall のルールで許可されていないパケットは拒否されます。

*もし eth0 に対して送受信時のフィルタを定義している場合（set interfaces ethernet eth0 firewall in の設定がされている場合）は、クラウド側のネットワークとブランチ側のネットワークの双方で通信ができるためのルールが設定されている必要があります。

*また、VyOS 自身に対してフィルタを定義している場合（set interfaces ethernet eth0 firewall local の設定がされている場合）は peer 同士の IP アドレスを許可する設定が必要となります。

11. 設定の反映

```
sudo /etc/init.d/ipsec restart
```

6.2. ブランチ側 VyOS の設定

以下に設定手順をご案内します。設定内容は例となります。適宜変更して設定してください。

WAN 側の Ethernet インターフェース	eth0
--------------------------	------

1. 基本的にはクラウド側 VyOS と同じ設定を行います。

(アドレスやネットワーク、ID などの情報が入れ替わるだけです。)

```
set vpn ipsec esp-group ESP-G lifetime 1800
set vpn ipsec esp-group ESP-G proposal 1 encryption 3des
set vpn ipsec esp-group ESP-G proposal 1 hash md5
set vpn ipsec ike-group IKE-G lifetime 3600
set vpn ipsec ike-group IKE-G proposal 1 encryption 3des
set vpn ipsec ike-group IKE-G proposal 1 hash md5
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal enable
set vpn ipsec site-to-site peer 203.0.113.1 authentication id @branch

set vpn ipsec site-to-site peer 203.0.113.1 authentication mode pre-shared-secret

set vpn ipsec site-to-site peer 203.0.113.1 authentication pre-shared-secret
my_shared_secret (*1 行で入力してください)

set vpn ipsec site-to-site peer 203.0.113.1 authentication remote-id @cloud
set vpn ipsec site-to-site peer 203.0.113.1 default-esp-group ESP-G
set vpn ipsec site-to-site peer 203.0.113.1 ike-group IKE-G
set vpn ipsec site-to-site peer 203.0.113.1 local-address 10.11.1.1

set vpn ipsec site-to-site peer 203.0.113.1 tunnel 1 local prefix 10.5.10.0/24

set vpn ipsec site-to-site peer 203.0.113.1 tunnel 1 remote prefix 10.11.0.0/22
```

ただし、WAN 側で NAT を使用している場合は注意点があります。

VyOS では IPsec を通すか通さないかの判断をする前の段階で、NAT のルールが適用されてしまうため、NAT ルールから、以下を除外する必要があります。

■ 「宛先アドレスがクラウド側のネットワークアドレス」を除外

```
set nat source rule 1 destination address 10.11.0.0/22
```

仮に rule 1 として Source NAT が設定されている場合、上記のコマンドで「宛先アドレスがクラウド側のネットワークアドレス」の packets を NAT ルールから除外することができます。

7. お問い合わせ

サービスに関するお問い合わせは、IDCF クラウドコンソール内のお問い合わせチケットシステムを利用したオンラインサポートをご利用ください。また、プレミアムサポート（有償オプション）をお申し込みいただければ、お電話でのお問い合わせも可能となります。

※ただし、VyOS の接続設定は、当社サポート範囲外となっておりますので、あらかじめご了承ください。 設定サポートをご希望の場合、当社協力会社のご紹介が可能です。ご相談ください。

対応内容		標準サポート		プレミアムサポート（有償）	
		受付時間	対応時間	受付時間	対応時間
サービス 問い合わせ	電話	—	—	平日9:00～17:00	平日9:00～17:00
	メール			—	—
	オンライン サポート	24時間365日	平日9:00～17:00	24時間365日	24時間365日
障害連絡 受付	電話	—	—	平日9:00～17:00	平日9:00～17:00
	メール	—	—	—	—
	オンライン サポート	24時間365日	24時間365日	24時間365日	24時間365日

※プレミアムサポートは電話サポートが可能となるサービスです。

改版履歴

改訂日	改訂章	改訂内容
2017 年 3 月 8 日	全章	新規作成
2019 年 3 月 12 日	P15	「3. IKE の設定」のコマンドを一部修正
2020 年 1 月 20 日	奥付	会社所在地を更新
2021 年 4 月 1 日	全章	レイアウト改訂
	P35	お問い合わせ窓口情報の修正

IDCF クラウド

VyOS での IPsec サイト間 VPN 接続ガイド

サービスマニュアル

Ver.1.12

発行日：2021 年 4 月 1 日

株式会社 IDC フロンティア

<https://www.idcf.jp/>

CS-PUB-M0143-ET
