GMO INTERNET

インターネット VPN
VyOS 接続設定ガイド

ユーザーマニュアル 1.0

2025 年 1 月 1 日

はじめに

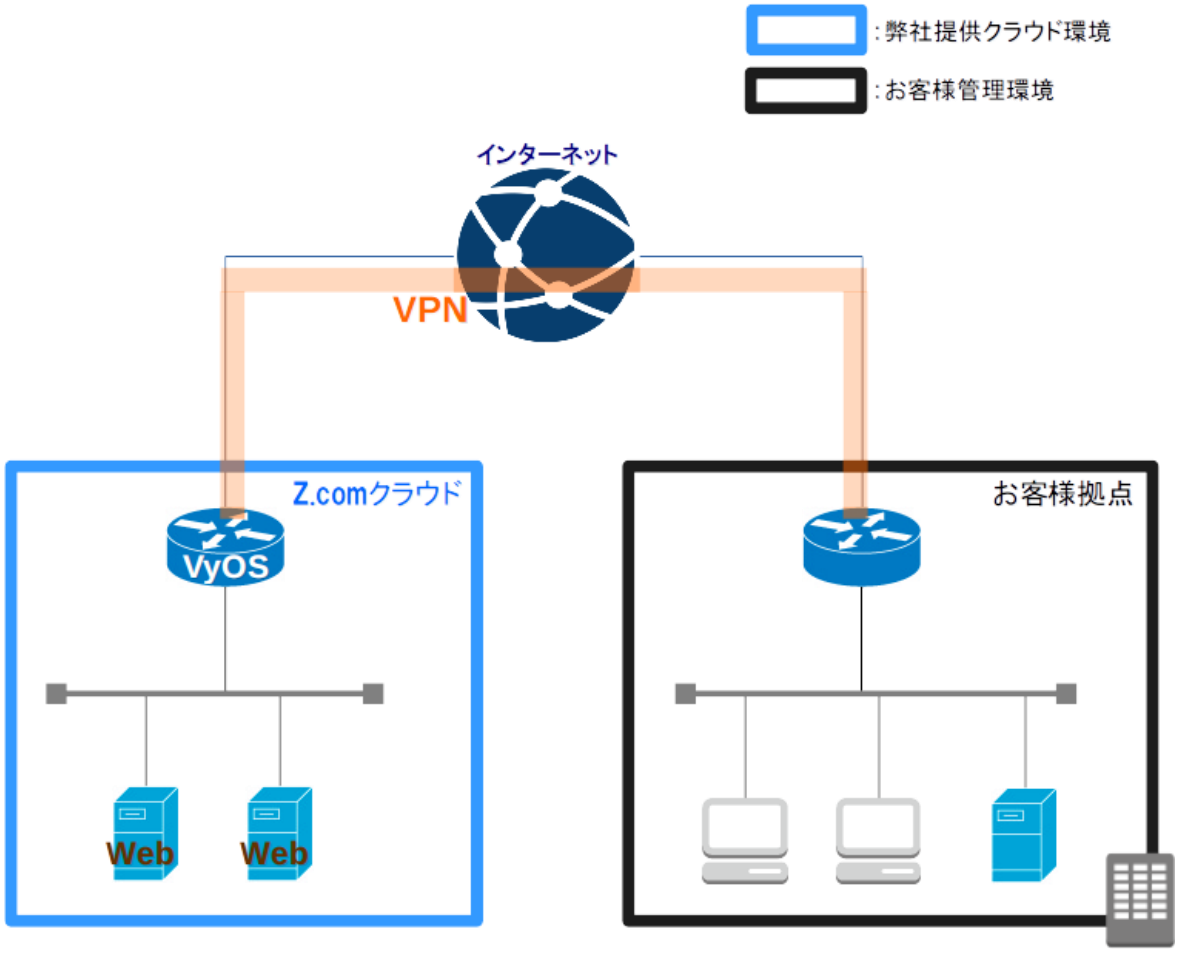
本書では当社の提供するクラウド環境で VyOS を利用して IPsec-VPN 接続を実現するための設定を記載します。本書を利用して拠点間での VPN 接続を行うことで、クラウド環境と安全なデータ通信が可能になります。

VyOS は、オープンソースのソフトウェアとなりますので、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 User Guide http://vyos.net/wiki/User_Guide
- 設定代行をご希望の場合、弊社パートナー企業のご紹介が可能です。お気軽にご相談下さい。

想定接続例

提供する VyOS で構築可能な VPN 接続例を以下に記載します。



接続動作確認済み機器

当社の提供する VyOS と IPsec-VPN 接続を確認した機器は以下の通りとなります。

表 1 動作確認済み機材一覧

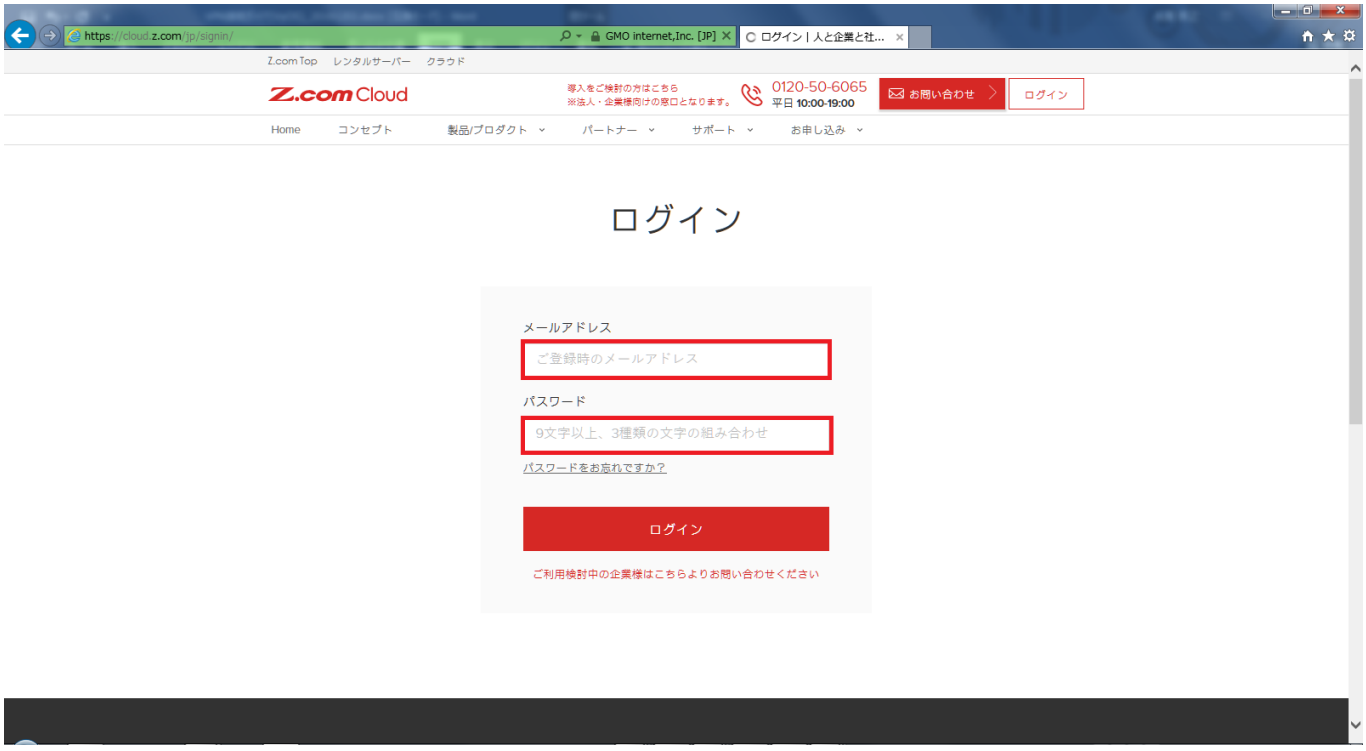
機器型番	OS バージョン
Juniper SSG140	ScreenOS 5.4.1
YAMAHA RTX1200	Rev.10.01.53
VyOS	VyOS 1.1.7

仮想サーバー追加方法

当社の提供する Z.comCloud 環境で VyOS を作成する手順を記載します。

- コントロールパネルへのログイン

以下のアドレスをブラウザへ入力し、アカウント情報を入力して「ログイン」をクリックします。
URL: https://cloud.z.com/jp/signin/

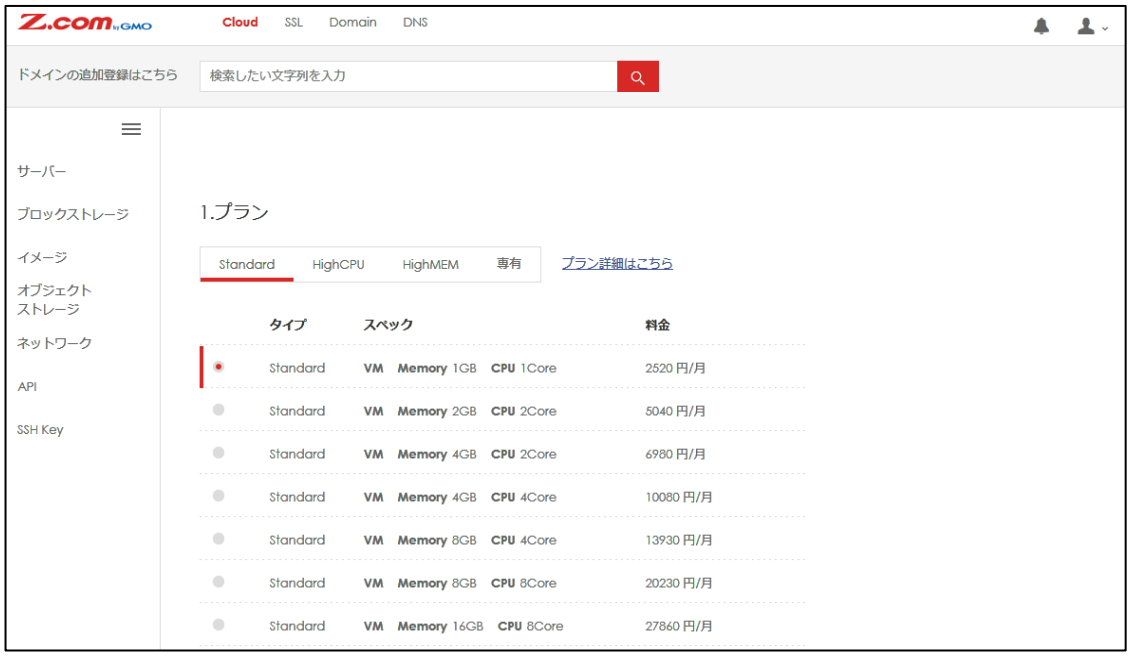


- 仮想サーバーの追加

仮想サーバーリストが表示されましたら、「+サーバー」をクリックします。

- プランの選択

利用したいサーバーのスペックを選択します。



- ブロックストレージの選択

利用したいストレージ容量を選択し、OS から「VyOS」を選択します。
VyOS 選択方法：OS -> その他 -> VyOS

- ネットワークの選択

利用したいネットワークを選択します。
※本書では VyOS にグローバル IP アドレスとプライベート IP アドレスを割り当てる操作を行います。

➢ 標準グローバルネットワークではセグメント選択で「新規 IP アドレス追加」を選択

➢ プライベートネットワーク設定では「ネットワーク」で割り当てたいネットワークを選択し、「IP アドレス」で割り当てたい IP アドレスをプルダウンから選択してください。

● サーバー情報設定

以下の情報を入力し、「追加」をクリックします。

➢ ホスト名：仮想サーバーへ割り当てるホスト名になります。

➢ ネームタグ：コントロールパネル上で表示する名前になります。

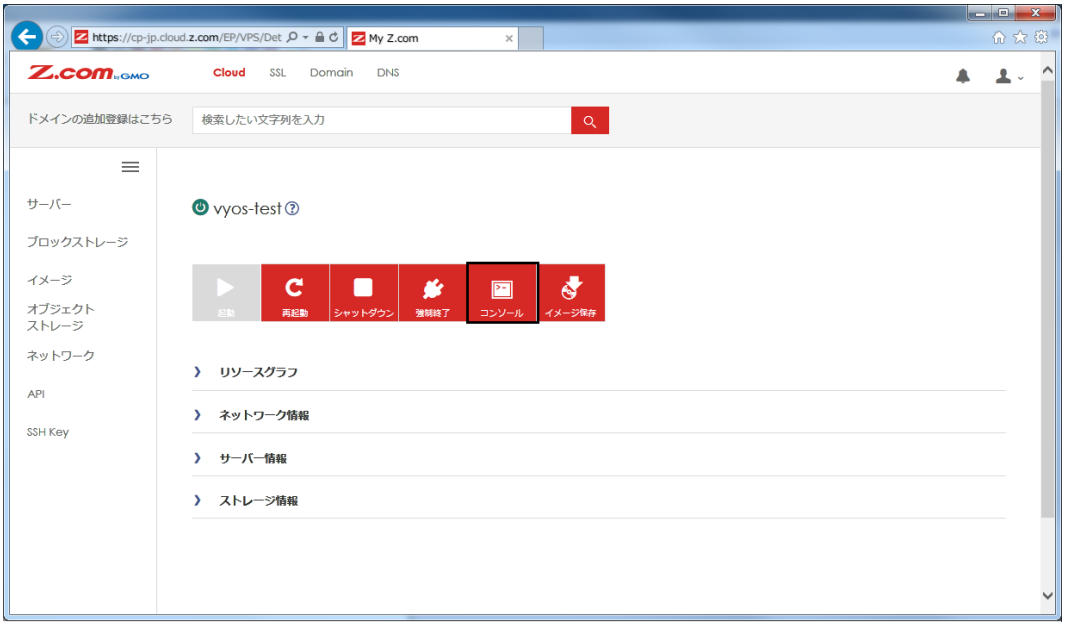
➢ root パスワード：仮想サーバーへログイン時に使用するパスワードになります。

- 作成した仮想サーバーの確認

追加した仮想サーバーが、仮想サーバーリストに表示されていることを確認してください。

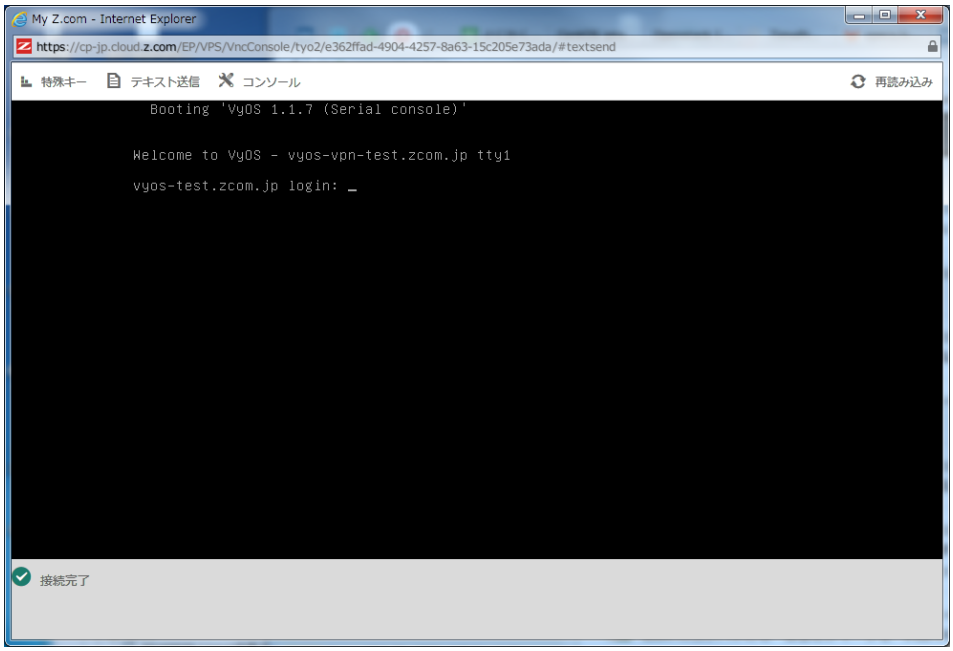
- 仮想サーバの操作

コントロールパネル上で追加した仮想サーバーを選択し、「コンソール」をクリックしてください。



コンソールをクリックすると、別ウインドウでコンソール画面が表示されます。
以下のユーザ名とパスワードを入力しログインすることができます。

- ユーザ名：vyos
- パスワード：[サーバー情報設定]で設定した root パスワードを入力してください



ログインすると各種 VyOS の設定が可能になります。VyOS の操作方法については次項から記載していますのでご参照ください。

VyOS 基本コマンド

VyOS を設定するための基本コマンドを以下に記載します。

- 操作方法について

  作成した仮想サーバー(VyOS)を操作する方法として、前述したコントロールパネルからコンソール接続する方法と、リモートマシンから SSH 接続で操作する方法があります。

- 操作モードについて

  VyOS には 2 種類の操作モードがあり、それぞれ実行できるコマンドが異なります。
  ログイン直後は一般モードでの操作になります。

モード名	プロンプト	用途
一般	vyos@vyos:~$	動作状態や設定状態を確認することができます
設定	vyos@vyos#	vyos の設定変更を行うことができます

一般モードと設定モードの遷移方法は以下になります。

```
vyos@vyos:~$ config  ← 一般モードから設定モードへ移行
vyos@vyos# exit  ← 設定モードから一般モードへ戻る
exit
vyos@vyos:~$
```

- 設定の保存について

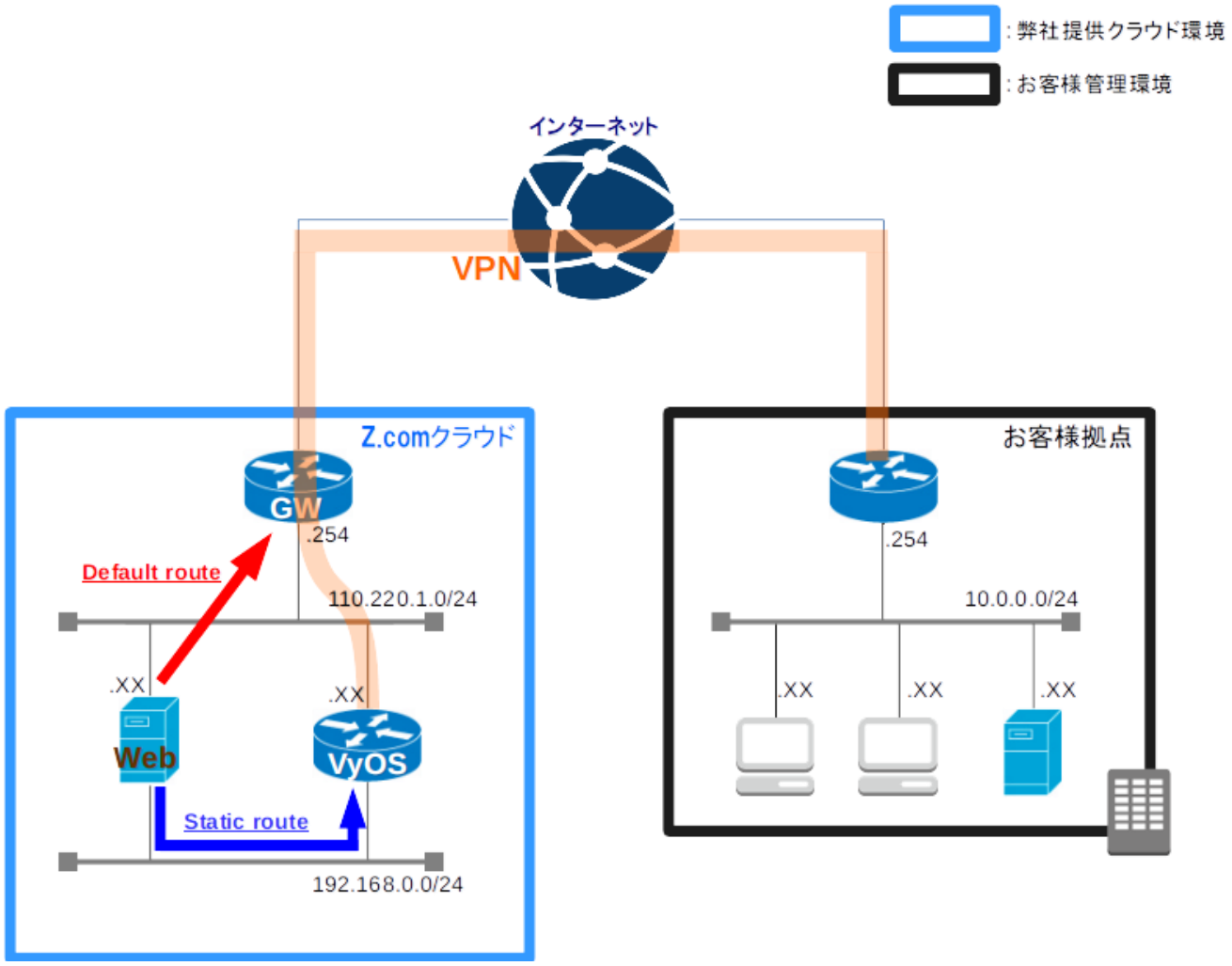
VyOS では設定変更のコマンドを投入しただけでは設定が反映されません。また、設定保存コマンドを実行していない場合は再起動時に設定が消えてしまいます。

```
vyos@vyos# commit  ← 設定の反映コマンド
vyos@vyos# save  ← 設定の保存コマンド
```

各 OS の静的ルートの設定

クラウド側の各仮想マシンにおいて、VyOS までの静的ルートを設定する場合があります。静的ルートが必要な場合の構成を以下に記載します。

図中クラウド環境下の Web サーバーにて'Default route'を GW に設定し、お客様環境宛の経路情報を'Static route'で VyOS に設定することで、Web サーバーはインターネットへのアクセスとお客様環境へのアクセス、双方と通信が可能になります。



以下に OS 毎の静的ルートの設定方法を記載します。

- CentOS の場合

  下記ファイルに静的ルート情報を追記してください。

```
[root@centos ~]# vi /etc/sysconfig/network-scripts/route-eth1
10.0.0.0/24 via 192.168.10.1 ← 追加
```

  設定した静的ルートを反映されるために下記コマンドを実行してください。

```
[root@centos ~]# ifdown eth1
[root@centos ~]# ifup eth1
```

- Debian/Ubuntu の場合

  下記ファイルに静的ルート情報を追記してください。

```
root@debian :~# vi /etc/network/interfaces
up route add -net 10.0.0.0 netmask 255.255.255.0 gw 192.168.0.1 ← 追加
```

設定した静的ルートを反映されるためにマシンを再起動してください。

- Windows の場合

コマンドプロンプトを起動し下記コマンドを実行してください。オプション「-p」を指定することで再起動後も設定が有効になります。

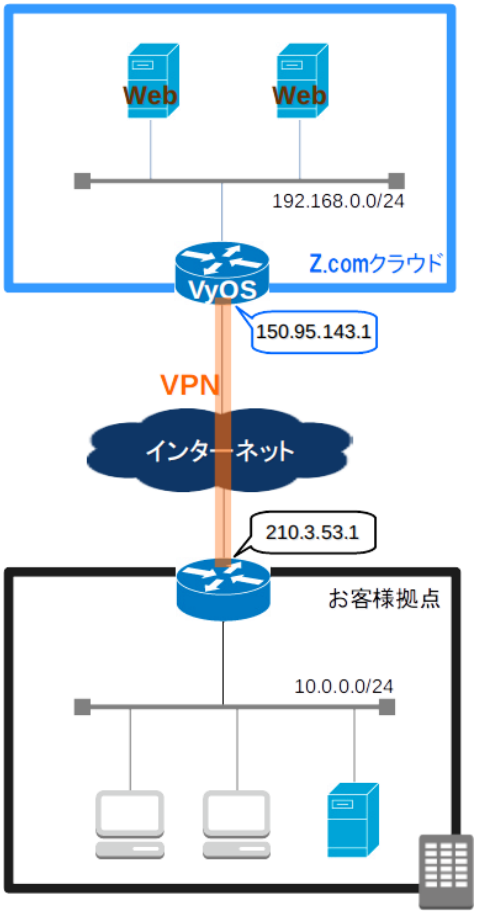
```
>route -p add 10.0.0.0/24 mask 255.255.255.0 192.168.0.1
```

設定した静的ルートが反映されていることを確認してください。固定ルートの欄に表示されていれば問題なく設定されています。

```
>netstat -r
```

VyOS 設定方法

本章では VyOS で VPN 接続を実現するための設定方法を記載していきます。設定値などは以下の構成を元に設定していますので、実際にお客様環境で利用する場合は適宜設定内容を読み替えてご利用ください。



VyOS 設定項目	設定値(例)
WAN 側インターフェース	eth0
WAN 側 IP アドレス	150.95.143.1
LAN 側ネットワーク	192.168.0.0/24
対向機器 IP アドレス	210.3.53.1
対向ネットワーク	10.0.0.0/24
ESP グループ名	ESP-test
IKE グループ名	IKE-test
事前共有鍵	vyos-vpn

IPSec の通信に用いるインターフェース設定

VPN 接続で利用する VyOS の WAN 側インターフェースを指定します。設定例では”eth0”を設定しています。

```
vyos@vyos# set vpn ipsec ipsec-interfaces interface eth0
```

NAT トラバーサル設定の有効化

NAT(NAPT)を利用している場合はこの設定を有効化してください。

```
vyos@vyos# set vpn ipsec nat-traversal enable
```

ESP グループ設定

ESP グループを設定するにあたり、以下の設定値を入力してください。

- esp-group(ESP グループ名)：[任意の名前設定可能] ESP-test
- encryption(暗号化アルゴリズム)：aes128
- hash(認証ハッシュアルゴリズム)：sha1
- lifetime(ESP の有効期限)：1800

encryption と hash は複数種類登録が可能です。proposal1 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。

```
vyos@vyos# set vpn ipsec esp-group ESP-test lifetime 1800
vyos@vyos# set vpn ipsec esp-group ESP-test proposal 1 encryption aes128
vyos@vyos# set vpn ipsec esp-group ESP-test proposal 1 hash sha1
```

IKE グループ設定

IKE グループを設定するにあたり、以下の設定値を入力してください。

- IKE-group(IKE グループ名)：[任意の名前設定可能] IKE-test
- encryption(暗号化アルゴリズム)：aes128
- hash(認証ハッシュアルゴリズム)：sha1
- lifetime(IKE の有効期限)：1800

encryption と hash は複数種類登録が可能です。proposal1 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。

```
vyos@vyos# set vpn ipsec ike-group IKE-test lifetime 3600
vyos@vyos# set vpn ipsec ike-group IKE-test proposal 1 encryption aes128
vyos@vyos# set vpn ipsec ike-group IKE-test proposal 1 hash sha1
```

VPN 接続設定方式に ESP/IKE グループを指定

本項で設定している”210.3.53.1”は VPN 接続をする対向機器の IP アドレスになります。環境に応じて適宜変更してください。

```
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 default-esp-group ESP-test
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 ike-group IKE-test
```

VPN 接続で用いる認証方式設定

拠点間で事前共有鍵を設定します。共有鍵部分は”vyos-vpn”になりますので、環境応じて適宜変更してください。

```
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 authentication mode pre-shared-secret
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 authentication pre-shared-secret vyos-vpn
```

VPN 拠点間接続の設定

VPN 拠点間の接続設定にあたり、以下の設定値を入力してください。

- local-address：150.95.143.1 [VyOS の WAN 側 IP アドレスを入力]
- local prefix：192.168.0.0/24 [VyOS の LAN 側ネットワークアドレスを入力]
- remote prefix：10.0.0.0/24 [対向拠点の LAN 側ネットワークアドレスを入力]

```
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 local-address 150.95.143.1
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 tunnel 1 local prefix 192.168.0.0/24
vyos@vyos# set vpn ipsec site-to-site peer 210.3.53.1 tunnel 1 remote prefix 10.0.0.0/24
```

状態確認

VyOS と対向拠点間で VPN 接続ができていることを確認します。State 項目が”up”になっていれば拠点間 VPN 接続が正しく設定できています。

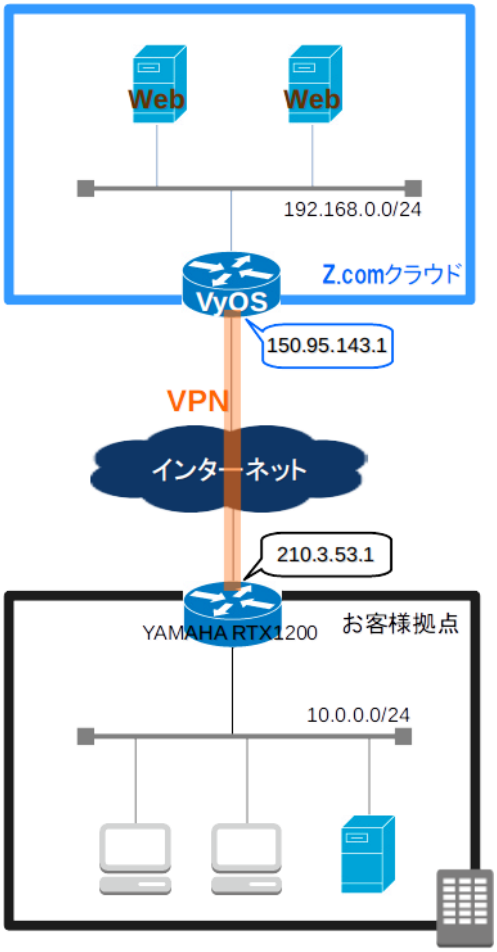
```
vyos@vyos:~$ sho vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
210.3.53.1                              150.95.143.1

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ------  -----
    1       up     0.0/0.0        aes128   sha1    no     323     1800    all
```

YAMAHA RTX1200 の設定方法

本章では YAMAHA RTX と VyOS で VPN 接続を実現するための設定方法を記載していきます。設定値などは以下の構成を元に設定していますので、実際にお客様環境で利用する場合は適宜設定内容を読み替えてご利用ください。

※VyOS の設定方法については「0 VyOS 設定方法」を参照ください



YAMAHA RTX 設定項目	設定値(例)
WAN 側インターフェース	eth0
WAN 側 IP アドレス	210.3.53.1
LAN 側ネットワーク	10.0.0.0/24
対向機器 IP アドレス	150.95.143.1
対向ネットワーク	192.168.0.0/24
事前共有鍵	vyos-vpn

IPsec の設定

IPsec の設定にあたり、以下の設定値を入力してください。

- local address：210.3.53.1
- local id：210.3.53.1
- pre-shared-key：vyos-vpn
- remote address：150.95.143.1
- remote id：150.95.143.1

```
tunnel select 1
 ipsec tunnel 101
  ipsec sa policy 101 1 esp aes-cbc sha-hmac
  ipsec ike always-on 1 on
  ipsec ike encryption 1 aes-cbc
  ipsec ike group 1 modp1024
  ipsec ike hash 1 sha
  ipsec ike keepalive use 1 on dpd 15 2
  ipsec ike local address 1 210.3.53.1
  ipsec ike local id 1 210.3.53.1
  ipsec ike pfs 1 on
  ipsec ike pre-shared-key 1 text vyos-vpn
  ipsec ike remote address 1 150.95.143.1
  ipsec ike remote id 1 150.95.143.1
  ipsec auto refresh 1 on
 ip tunnel mtu 1280
 ip tunnel tcp mss limit auto
 tunnel enable 1
```

ルーティングの設定

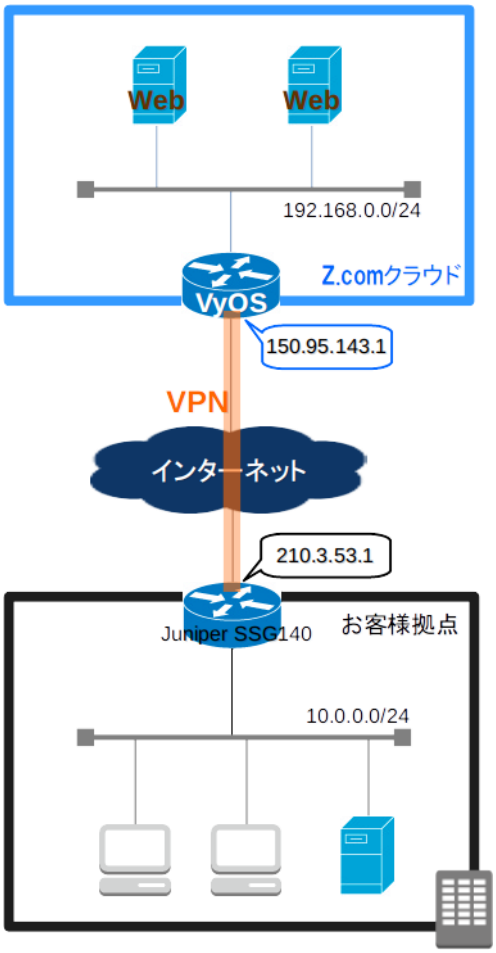
対向拠点の LAN 側ネットワークへ通信を行うために、静的ルートの設定を行います。環境に応じて対向拠点の LAN 側ネットワークアドレスを入力してください。

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

JUNIPER SSG140 の設定方法

本章では Juniper SSG と VyOS で VPN 接続を実現するための設定方法を記載していきます。設定値などは以下の構成を元に設定していますので、実際にお客様環境で利用する場合は適宜設定内容を読み替えてご利用ください。

※VyOS の設定方法については「0 VyOS 設定方法」を参照ください



JuniperSSG 設定項目	設定値(例)
WAN 側インターフェース	ethernet0/1
WAN 側 IP アドレス	210.3.53.1
LAN 側ネットワーク	10.0.0.0/24
対向機器 IP アドレス	150.95.143.1
対向ネットワーク	192.168.0.0/24
トンネルインターフェース	tunnel.1
IKE 設定名	IKE-test
事前共有鍵	vyos-vpn
VPN 設定名	SSG140-vyos
VPN 設定 ID	0x2

トンネルインターフェースと WAN 側インターフェースの関連付け

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

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"
```

IKE の設定

IKE を設定するにあたり、以下の設定値を入力してください。

- IKE 設定名：[任意の名前を設定可能] IKE-test
- 対向機器の IP アドレス：150.95.143.1
- WAN 側インターフェース：ethernet0/1
- 事前共有鍵：vyos-vpn
- 暗号化とハッシュアルゴリズム：pre-g2-aes128-sha

※下記コマンドは 1 行で入力してください

```
set ike gateway “IKE-test” address 150.95.143.1 Main outgoing-interface ″ethernet0/1″ preshare “vyos-vpn” proposal ″pre-g2-aes128-sha″
```

NAT トラバーサルの設定

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。以下の例では 5 秒間隔で実施します。

```
set ike gateway ″IKE-test″ nat-traversal
set ike gateway ″IKE-test″ nat-traversal udp-checksum
set ike gateway ″IKE-test″ nat-traversal keepalive-frequency 5
```

VPN の設定

VPN の設定をするにあたり、以下の設定値を入力してください。

- VPN 設定名：[任意の名前を設定可能] SSG140-vyos
- IKE 設定名：[任意の名前を設定可能] IKE-test
- 暗号化とハッシュアルゴリズム：pre-g2-aes128-sha

```
set vpn ″SSG140-vyos″ gateway ″IKE-test″ no-replay tunnel idletime 0 proposal ″pre-g2-aes128-sha″
```

VPN 設定をトンネルインターフェースと関連付け

VPN 設定をするにあたり、以下の設定値を入力してください。

- VPN 設定名：[任意の名前を設定可能] SSG140-vyos
- VPN 設定 ID：0x2

- トンネルインターフェース：tunnel.1
- LAN 側ネットワーク：10.0.0.0/24
- 対向ネットワーク：192.168.0.0/24

```
set vpn "SSG140-vyos" id 0x2 bind interface tunnel.1
set vpn "SSG140-vyos" proxy-id local-ip 10.0.0.0/24 remote-ip 192.168.0.0/24 "ANY"
```

ルーティングの設定

対向拠点の LAN 側ネットワークへ通信を行うために、静的ルートの設定を行います。環境に応じて対向拠点の LAN 側ネットワークアドレスを入力してください。

```
set route 192.168.0.0/24 interface tunnel.1
```