GMO INTERNET

インターネット VPN
VyOS 接続設定ガイド

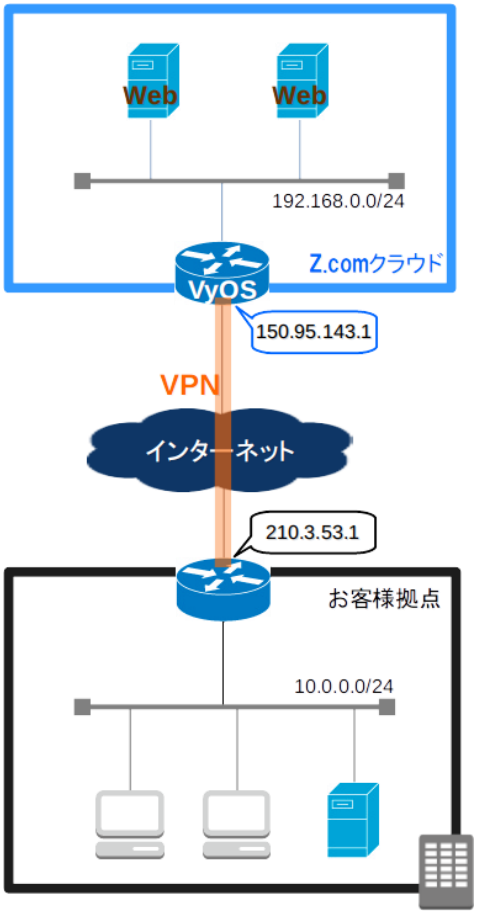
ユーザーマニュアル 1.0

2016 年 12 月 1 日

1 はじめに

2 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

2.1 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
```

2.2 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
```

2.3 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
```

2.4 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
```

2.5 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
```

2.6 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
```

2.7 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
```

2.8 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。

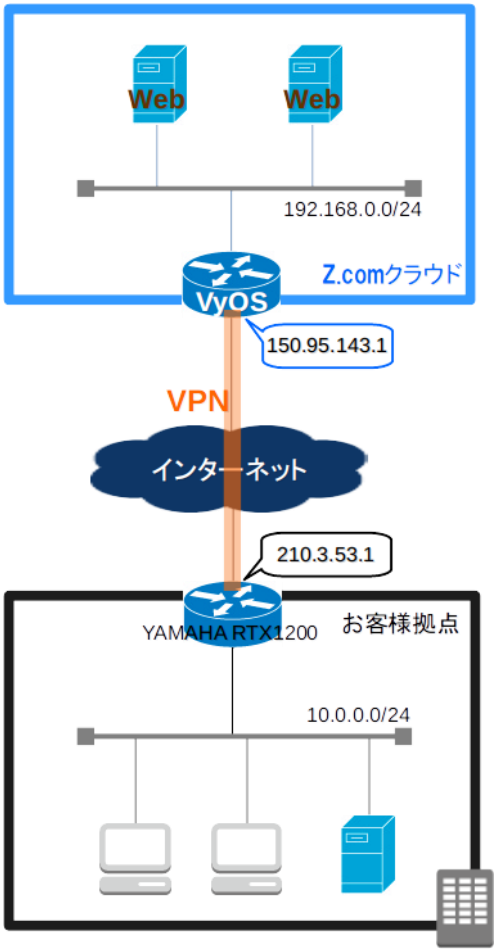
```
vyos@vyos:~$ sho vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
210.3.53.1                              150.95.143.1

    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
```

3 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「2 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

3.1 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
```

3.2 ルーティングの設定

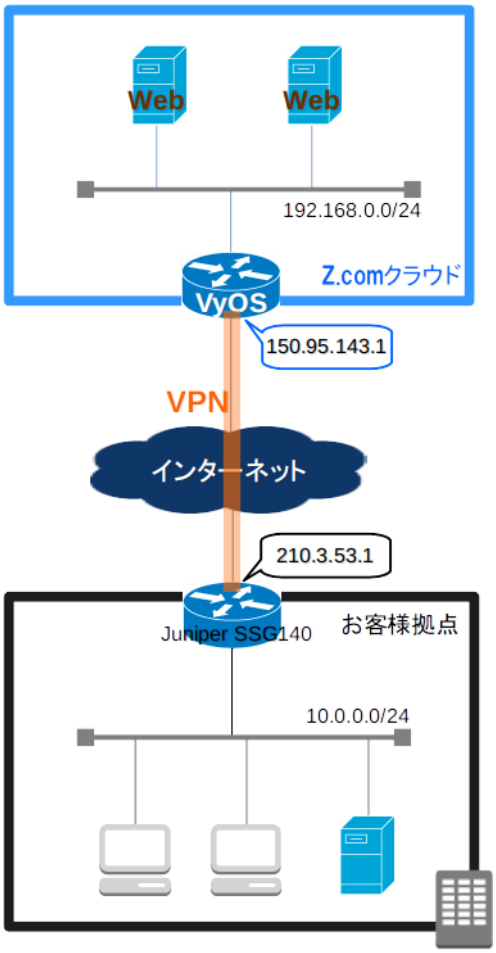
対向拠点の LAN 側ネットワークへ通信を行うために、静的ルートの設定を行います。環境に応じて対向拠点の LAN 側ネットワークアドレスを入力してください。

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

4 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「2 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

4.1 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
```

4.2 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"
```

4.3 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″
```

4.4 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
```

4.5 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″
```

4.6 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″
```

4.7 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
```