FITELnet を利用して、Oracle Cloud Infrastructure と VPN 接続する方法

2020 年 7 月　初版

目次

1　概要

FITELnet を利用して、Oracle Cloud Infrastructure（以下 OCI）と IPsec 接続を行う方法についてご説明します。次の 2 ケースについてご説明します。

■static に経路情報を記載した場合

■BGP を用いて dynamic に経路情報を取得した場合

2　設定手順

2.1　OCI にサインイン

OCI サインインページより、サインインしてください。

(注) OCI を利用するためのユーザ登録を、事前に実施お願いします。

2.2　仮想クラウド・ネットワーク（VCN）の作成

左上のタブから、「ネットワーキング」を選択して「仮想クラウド・ネットワーク」へ移動してください。

「仮想クラウド・ネットワークの作成」ボタンから、VCN の設定を実施ください。

＊下記入力欄の「${文字列}」の表記は、OCI の F220/F221 設定例ページで説明しているパラメータです。

入力欄	入力内容
名前	任意の名前
コンパートメントに作成	ルート
・仮想クラウド・ネットワークのみの作成 ・仮想クラウド・ネットワークおよび 関連リソースの作成	仮想クラウド・ネットワークのみの作成
CIDR ブロック：${VcnCidrBlock}	インスタンスのあるネットワークの IP アドレス
DNS 解決	指定なし

2.3　インスタンスの作成

左上のタブから、「コンピュート」を選択して「インスタンス」へ移動してください。
「インスタンスの作成」ボタンからコンピュート・インスタンスを作成してください。

入力欄	入力内容
インスタンスの命名	任意の名前
インスタンスの可用性ドメイン	可用性ドメイン 1 （他は選択不可）
オペレーティングシステム	Canonical Ubuntu 18.04
インスタンス・タイプ	仮想マシン
インスタンス・シェイプ	VM.Standard2.1 1 コア OCPU、15 GB メモリー
ブート・ボリュームの構成	（選択なし）
SSH キーの追加	下記「※SSH キー作成方法」参照

※SSH キー作成方法

Tera Term を開いて、まず「新しい接続」ウィンドウを閉じてください。その後「設定」タブ にて 「SSH 鍵生成」を選択して、下記を入力してください。

入力欄	入力内容
鍵の種類	RSA
ビット数	2048

その後、任意の鍵のパスフレーズを記載して、「公開鍵の保存」、「秘密鍵の保存」を実施ください。「SSH キーの追加」欄にて、作成した SSH キーを選択してください。

2.4　CPE の作成

左上のタブから、「ネットワーキング」を選択して「顧客構内機器」へ移動してください。
「顧客構内機器の作成」ボタンから CPE を作成してください。

＊下記入力欄の「${文字列}」の表記は、OCI の F220/F221 設定例ページで説明しているパラメータです。

入力欄	入力内容
コンパートメント	ルート
名前	任意
IP アドレス：${cpePublicIpAddress}	FITELnet(CPE)のグローバルアドレス

2.5　動的ルーティング・ゲートウェイ（DRG）の作成

左上のタブから、「ネットワーキング」を選択して「動的ルーティング・ゲートウェイ」へ移動してください。

「動的ルーティング・ゲートウェイの作成」ボタンから DRG を作成してください。

入力欄	入力内容
コンパートメント	ルート
名前	任意

2.6　DRG と VCN を紐づける

作成した DRG のページへ移動してください。

左中の「リソース」欄から「仮想クラウド・ネットワーク」へ移動してください。

「仮想クラウド・ネットワークにアタッチ」ボタンから、DRG と VCN を紐づけしてください。

入力欄	入力内容
コンパートメント	ルート
仮想クラウド・ネットワーク	作成した VCN を選択
ルート表コンパートメント	ルート
ルート表	Default Route Table for [VCN の名前]

2.7　DRG に FITELnet(CPE)の LAN 側のアドレスを記載する

(注)BGP であっても、OCI 側ではオンプレミス側経路情報（お客様構内の経路情報）をスタティックで登録する必要があります。

左上のタブから、「ネットワーキング」を選択して、「仮想クラウド・ネットワーク」へ移動してください。「デフォルト・ルート表」を選択した後、「ルート・ルール」項目から、「ルート・ルールの追加」ボタンを選択してください。

入力欄	入力内容
ターゲット・タイプ	動的ルーティング・ゲートウェイ
宛先 CIDR ブロック	FITELnet(CPE)の LAN 側ネットワーク

2.8　IPsec 接続(static)

左上のタブから、「ネットワーキング」を選択して、「IPsec 接続」へ移動してください。
「IPsec 接続の作成」ボタンから IPsec 接続のための設定をしてください。

入力欄	入力内容
コンパートメントに作成	ルート
名前	任意
顧客機構内機器コンパートメント	ルート
顧客構内機器	作成した CPE を選択
動的ルーティング・ゲートウェイ・コンパートメント	ルート
動的ルーティング・ゲートウェイ	作成した DRG を選択
静的ルート CIDR	FITELnet(CPE)の LAN 側ネットワーク

作成した IPsec 接続のページへ移動してください。
「コンパートメント内のトンネル」欄にトンネルが新規に 2 つ生成されていることを確認した後に、上記トンネル情報から、「Oracle VPN IP アドレス」を確認してください。
生成されたトンネルのページへ移動し、「共有シークレット」欄から PSK を確認してください。
※ここでの、Oracle VPN IP アドレスと PSK は FITELnet(CPE)のコンフィグに設定する必要があります。OCI の F220/F221 設定例ページにて、Oracle VPN IP アドレスは${vpn-ip#}、PSK は${sharedSecret#}と、それぞれ記載しています（#：番号）。

FITELnet にて、以下「FITELnet のコンフィグ」の章を参考に、コンフィグを設定してください。コンフィグ設定後に、「コンパートメント内のトンネル」欄の「IPsec ステータス」が「稼働中」になっていることを確認してください。

2.9　IPsec 接続(BGP)

左上のタブから、「ネットワーキング」を選択して「IPsec 接続」へ移動してください。
「IPsec 接続の作成」ボタンから IPsec 接続のための設定を行ってください。

入力欄	入力内容
コンパートメントに作成	ルート
名前	任意
顧客機構内機器コンパートメント	ルート
顧客構内機器	作成した CPE を選択
動的ルーティング・ゲートウェイ・コンパートメント	ルート
動的ルーティング・ゲートウェイ	作成した DRG を選択
静的ルート CIDR	指定しない

BGP を使用する場合は、上記から拡張オプションを追加する必要があります。

＊下記入力欄の「${文字列}」の表記は、OCI の F220/F221 設定例ページで説明しているパラメータです。

CPE IKE 識別子	
入力欄	入力内容
CPE IKE 識別子タイプ	IP アドレス
CPE IKE 識別子：${cpePublicIpAddress}	FITELnet(CPE)のトンネル終端アドレス（グローバル IP アドレス）
トンネル 1, 2	
名前	任意
カスタム共有シークレットの指定	指定しない
ルーティングタイプ	BGP 動的ルーティング
BGP ASN：${customer-bgp-asn}	任意の番号
トンネル内インターフェース(CPE)：${customer-interface-ip#}　(#：番号)	CPE の BGP peer アドレス
トンネル内インターフェース(ORACLE)：${oracle-interface-ip#}　(#：番号)	OCI の BGP peer アドレス

作成した IPsec 接続のページへ移動してください。
「コンパートメント内のトンネル」欄にトンネルが新規に 2 つ生成されていることを確認した

後に、上記トンネル情報から、「Oracle VPN IP アドレス」を確認してください。
生成されたトンネルのページへ移動し、「共有シークレット」欄から PSK を確認してください。
※ここでの、Oracle VPN IP アドレスと PSK と BGP peer アドレスは FITELnet(CPE)のコンフィグに設定する必要があります。OCI の F220/F221 設定例ページにて、Oracle VPN IP アドレスは${vpn-ip#}、PSK は${sharedSecret#}、BGP peer アドレスは${customer-interface-ip#}と、それぞれ記載しています（#：番号）。

FITELnet にて、以下「FITELnet のコンフィグ」の章を参考に、コンフィグを設定してください。コンフィグ設定後に、「コンパートメント内のトンネル」欄の「IPsec ステータス」と「BGP ステータス」が「稼働中」になっていることを確認してください。

3　FITELnet のコンフィグ

以下に、FITELnet のコンフィグを記載します。まず、「ベースコンフィグ」と「ISAKMP と IPsec のコンフィグ」を設定してください。

その後、static に経路情報を記載する場合は「静的ルートのコンフィグ」を、BGP を用いて dynamic に経路情報を取得する場合は「BGP のコンフィグ」を、それぞれ設定してください。

＊本章のコンフィグの「${文字列}」の表記は、オラクル殿ページ(F220/F221　設定例)で説明しているパラメータです。

3.1　ベースコンフィグ

```
!
access-list 100 permit udp ${vpn-ip1} 0.0.0.0 eq 500 any eq 500
access-list 100 permit 50 ${vpn-ip1} 0.0.0.0 any
access-list 100 permit udp ${vpn-ip2} 0.0.0.0 eq 500 any eq 500
access-list 100 permit 50 ${vpn-ip2} 0.0.0.0 any
access-list 111 deny ip any any
access-list 121 spi ip any any
!　VPN 通信とインターネットからの応答パケットのみを許可するための、フィルタ設定です。
!
ip route 0.0.0.0 0.0.0.0 tunnel 1
!
ip nat list 1 ${customer-lan-ip-wildcard}
!　VPN トンネルを使わない、インターネット向けの通信を行う場合に、送信元アドレスを
!　グローバル アドレスに変換するための nat-list です。
!　 ${customer-lan-ip-wildcard}は、LAN のネットワークアドレスに応じて設定
!　お願いします。例えば 192.168.10.0/24 であれば、“192.168.10.0 0.0.0.255”を入力ください。
!
logging level informational
!
crypto isakmp log sa
crypto isakmp log session
crypto isakmp log negotiation-fail
!
interface GigaEthernet 1/1
 vlan-id 11
 bridge-group 11
 channel-group 11
exit
```

```
!
interface GigaEthernet 2/1
 vlan-id 21
 bridge-group 21
 pppoe enable
exit
!
Interface Port-channel 11
 ip address ${customer-lan-ip}
                ※${customer-lan-ip}には LAN 側ネットワークに属するアドレスを指定ください。
exit
!
interface Tunnel 1
 ip address ${cpePublicIpAddress}
 ip access-group 100 in
 ip access-group 111 in
 ip access-group 121 out
 ip nat inside source list 1 interface
 tunnel mode pppoe profile PPPoE_PROF
 pppoe interface gigaethernet 2/1
exit
!
pppoe profile PPPoE_PROF
 account [PPP account] [pass]
exit
!
end
```

3.2 ISAKMP と IPsec のコンフィグ

```
 !
 crypto ipsec policy ${ipsecPolicy}
  set pfs group5
  set security-association transform-keysize aes 256 256 256
  set security-association transform esp-aes esp-sha-hmac
 exit
```

```
!
crypto ipsec selector ${selector}
 src 1 ipv4 any
 dst 1 ipv4 any
exit
!
crypto isakmp keepalive
!
crypto isakmp policy ${isakmpPolicy}
 authentication pre-share
 encryption aes
 encryption-keysize aes 256 256 256
 group 5
 hash sha
exit
!
crypto isakmp profile ${isakmpProfile1}
 local-address ${cpePublicIpAddress}
 set isakmp-policy ${isakmpPolicy}
 set ipsec-policy ${ipsecPolicy}
 set peer ${vpn-ip1}
 ike-version 1
 local-key ascii ${sharedSecret1}
exit
!
crypto isakmp profile ${isakmpProfile2}
 local-address ${cpePublicIpAddress}
 set isakmp-policy ${isakmpPolicy}
 set ipsec-policy ${ipsecPolicy}
 set peer ${vpn-ip2}
 ike-version 1
 local-key ascii ${sharedSecret2}
exit
!
crypto map ${map1} ipsec-isakmp
 match address ${selector}
```

```
  set isakmp-profile ${isakmpProfile1}
exit
!
crypto map ${map2} ipsec-isakmp
  match address ${selector}
  set isakmp-profile ${isakmpProfile2}
exit
!
interface Tunnel ${tunnelNumber1}
  tunnel mode ipsec map ${map1}
  ip address ${customer-interface-ip1}
exit
!
interface Tunnel ${tunnelNumber2}
  tunnel mode ipsec map ${map2}
  ip address ${customer-interface-ip2}
exit
!
```

3.3　静的ルートのコンフィグ

```
!
ip route ${vcnCidrBlock} Tunnel ${tunnelNumber1}
ip route ${vcnCidrBlock} Tunnel ${tunnelNumber2}
!
```

3.4　BGP のコンフィグ

```
!
router bgp ${customer-bgp-asn}
 bgp router-id ${router-id}
 bgp log-neighbor-changes
 neighbor ${oracle-interface-ip1} ebgp-multihop 10
 neighbor ${oracle-interface-ip1} enforce-multihop
 neighbor ${oracle-interface-ip1} remote-as ${oracle-bgp-asn1}
 neighbor ${oracle-interface-ip1} update-source tunnel ${tunnelNumber1}
 neighbor ${oracle-interface-ip2} ebgp-multihop 10
 neighbor ${oracle-interface-ip2} enforce-multihop
 neighbor ${oracle-interface-ip2} remote-as ${oracle-bgp-asn2}
 neighbor ${oracle-interface-ip2} update-source tunnel ${tunnelNumber2}
 !
 address-family ipv4 unicast
  redistribute connected
 exit
exit
!
```

4　IPsec 接続パラメータまとめ

■ISAKMP ポリシー・オプション

ISAKMP プロトコル・バージョン	バージョン 1
交換タイプ	メイン・モード
認証方式	事前共有キー
暗号化	AES-CBC/256
認証アルゴリズム	HMAC-SHA1
Diffie-Hellman Group	グループ 5
IKE セッション・キーの有効期間	28800 秒(8 時間)　※OCI の設定値で動作

■IPsec ポリシー・オプション

IPSec プロトコル	ESP, tunnel-mode
暗号化	AES-CBC/256
認証アルゴリズム	HMAC-SHA1
PFS	有効（DH グループ 5）
IPSec セッション・キーの有効期間	3600 秒(1 時間)　※OCI の設定値で動作