AWS上での監視サーバー(Zabbix)構築【5.AWSとCMLのVPN接続】

2021.09.11　2021.09.05

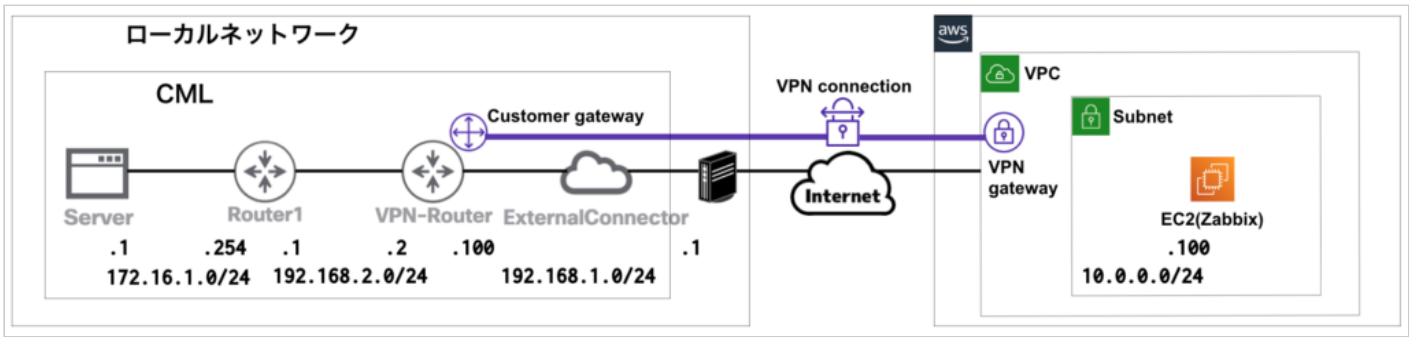
監視サーバーをAWS上で構築し、CML上のネットワーク機器/サーバーを監視します。監視ソフトウェアはZabbixを利用します。

【前回】AWS上での監視サーバー(Zabbix)構築【4.Zabbixのインストールと設定】
【次回】AWS上での監視サーバー(Zabbix)構築【6.監視登録(ICMPノード監視)】

ネットワーク構成

下記のネットワーク環境を構築し、AWS上のEC2(Zabbixサーバー)から、CML上のネットワーク機器/サーバーを監視できるようにしていきます。

【参考】AWSサイト間VPNの構築（1.AWSの基本設定）



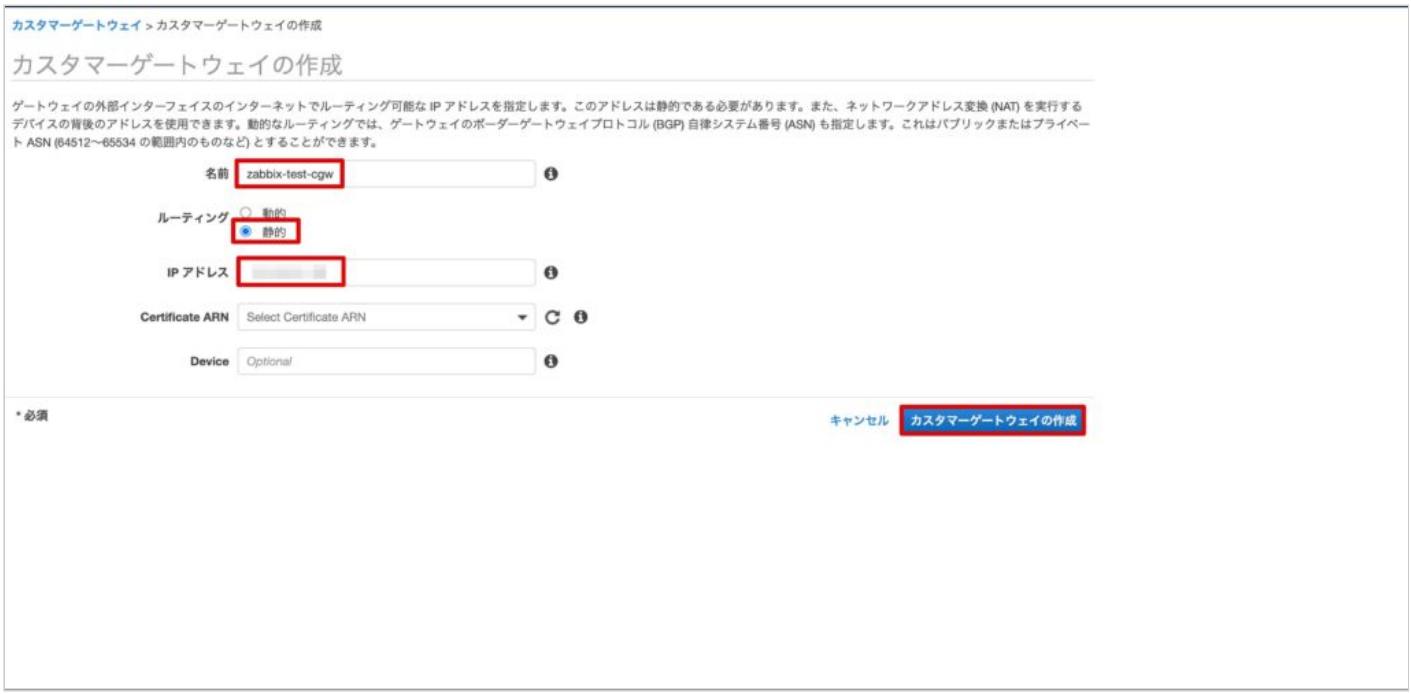
AWSのVPN構築

カスタマーゲートウェイの作成

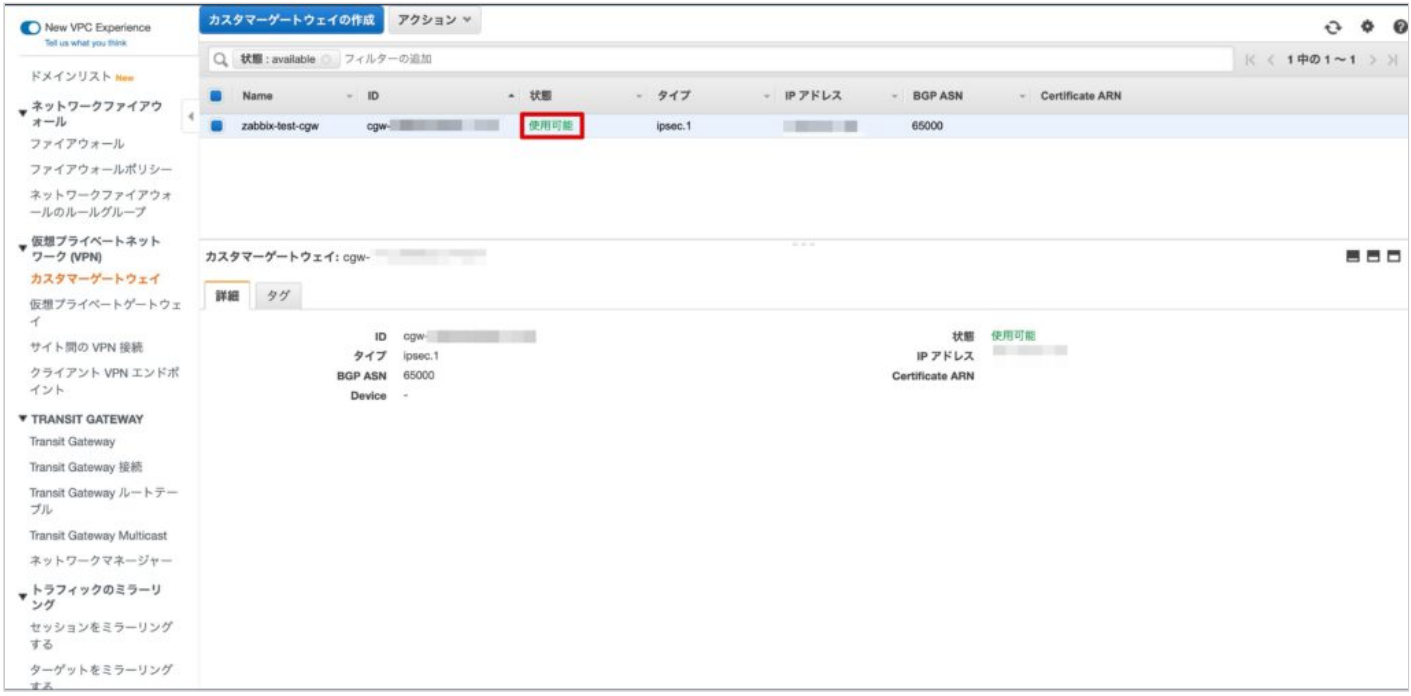
ローカルネットワーク側のVPNの起点となるカスタマーゲートウェイを作成します。まず、自身が利用しているグローバルIPアドレスを確認します。ここではCMANのIPアドレス確認ページで確認しています。

VPC→仮想プライベートネットワーク(VPN)の画面から操作します。
カスタマーゲートウェイ →「カスタマーゲートウェイの作成」をクリックします。

「zabbix-test-cgw」という名前で、ルーティングは「静的」を選択し、IPアドレスは確認した「グローバルIPアドレス」を設定します。



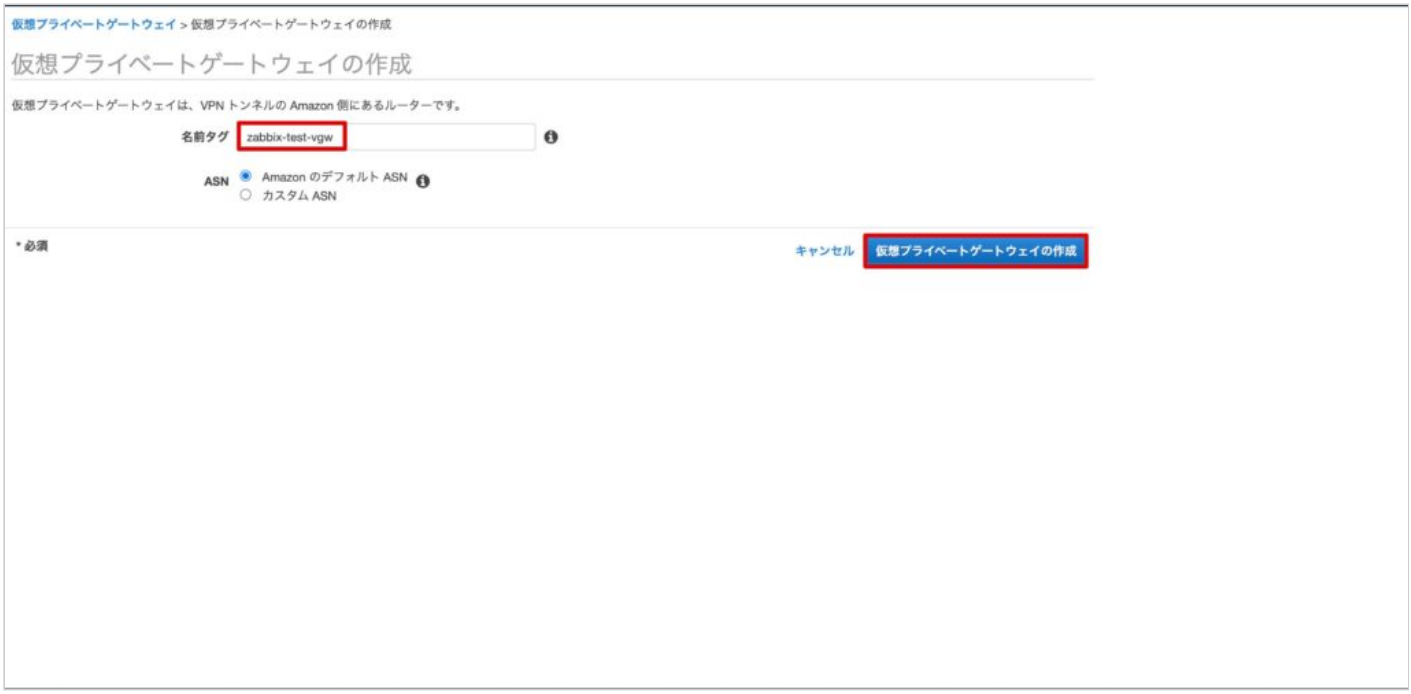
「使用可能」となれば、作成完了です。



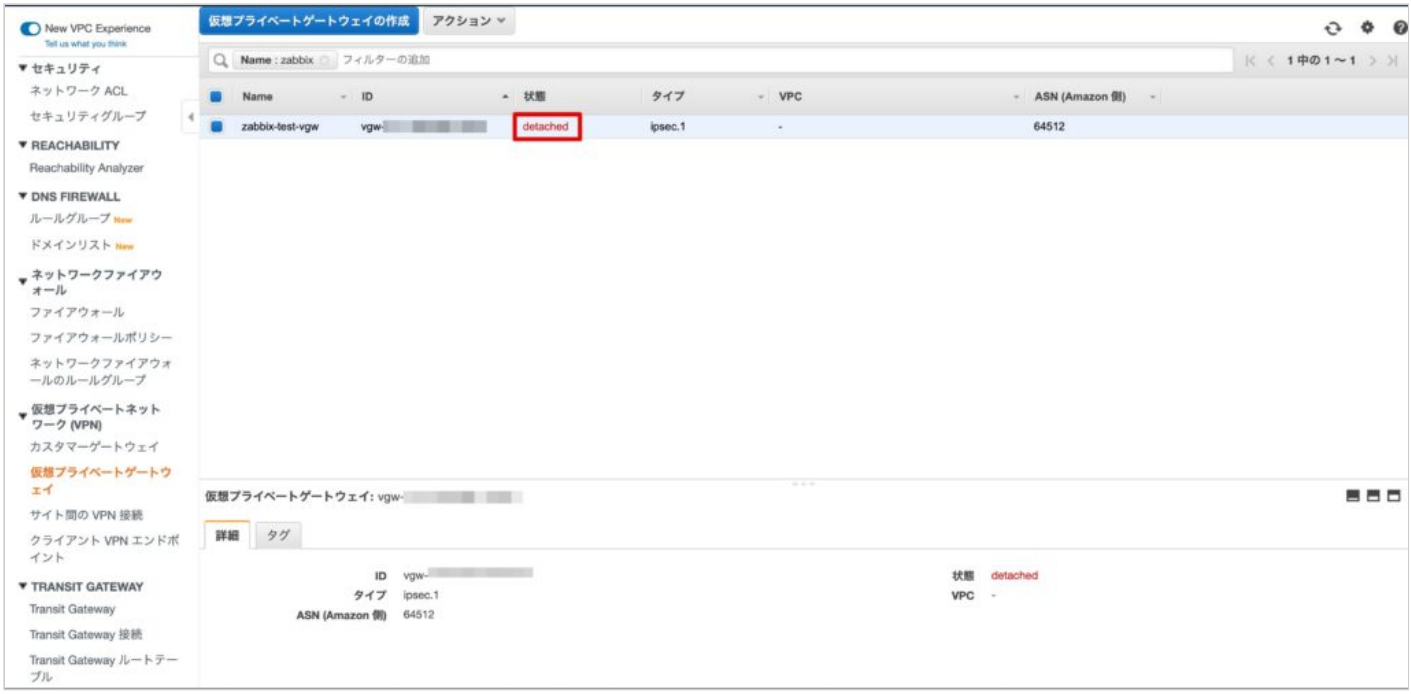
仮想プライゲートゲートウェイの作成

AWS側のVPNの起点となる仮想プライベートゲートウェイを作成します。
仮想プライベートゲートウェイ →「仮想プライベートゲートウェイの作成」をクリックします。

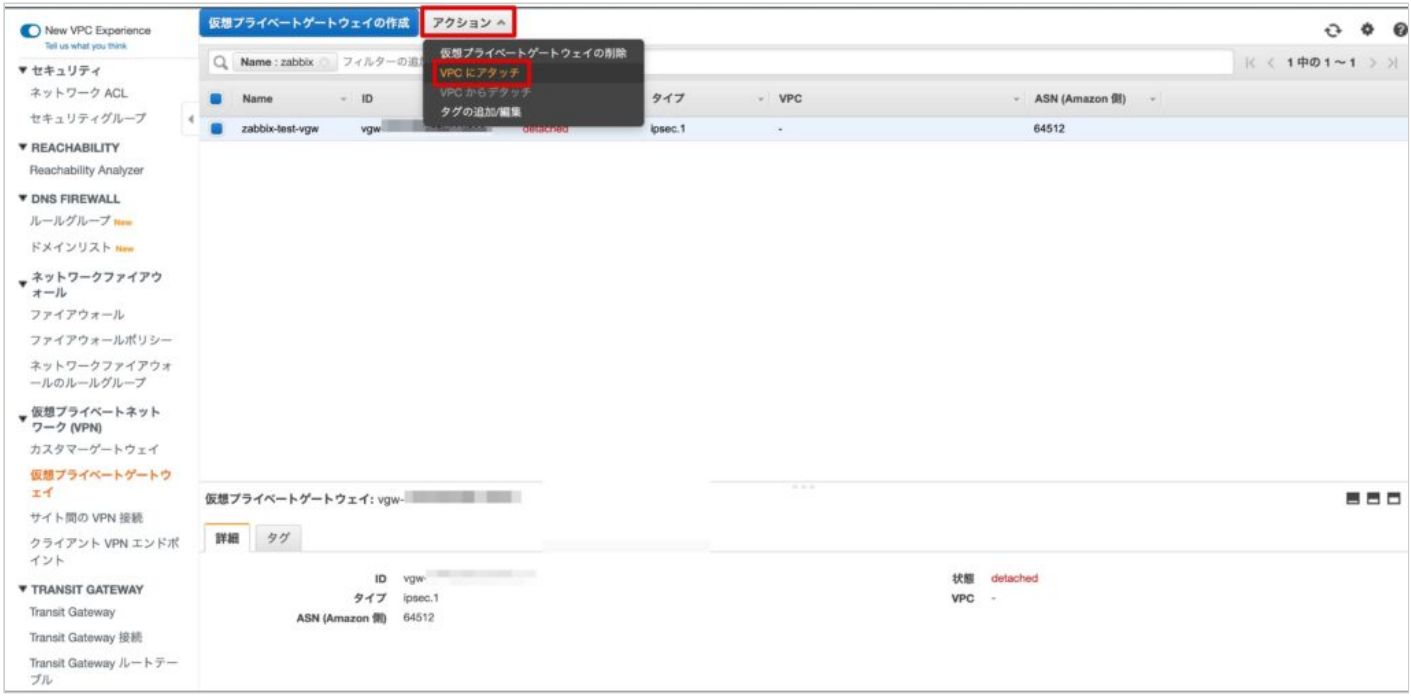
「zabbix-test-vgw」という名前で作成しています。



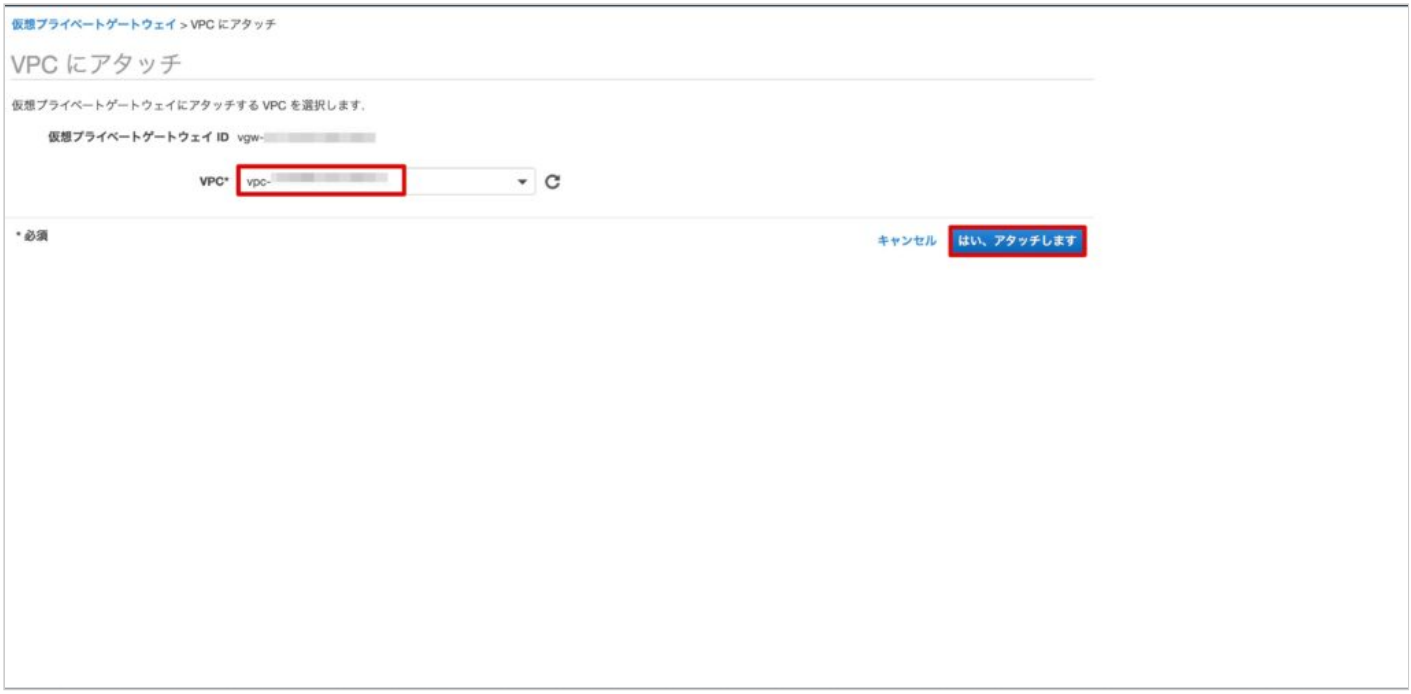
作成後は状態が「detached」となっいるため、VPCにアタッチします。



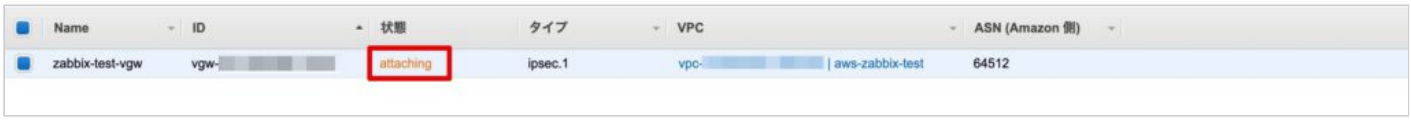
「アクション」→「VPCにアタッチ」を選択します。



VPC(aws-zabbix-test)を選択しアタッチします。



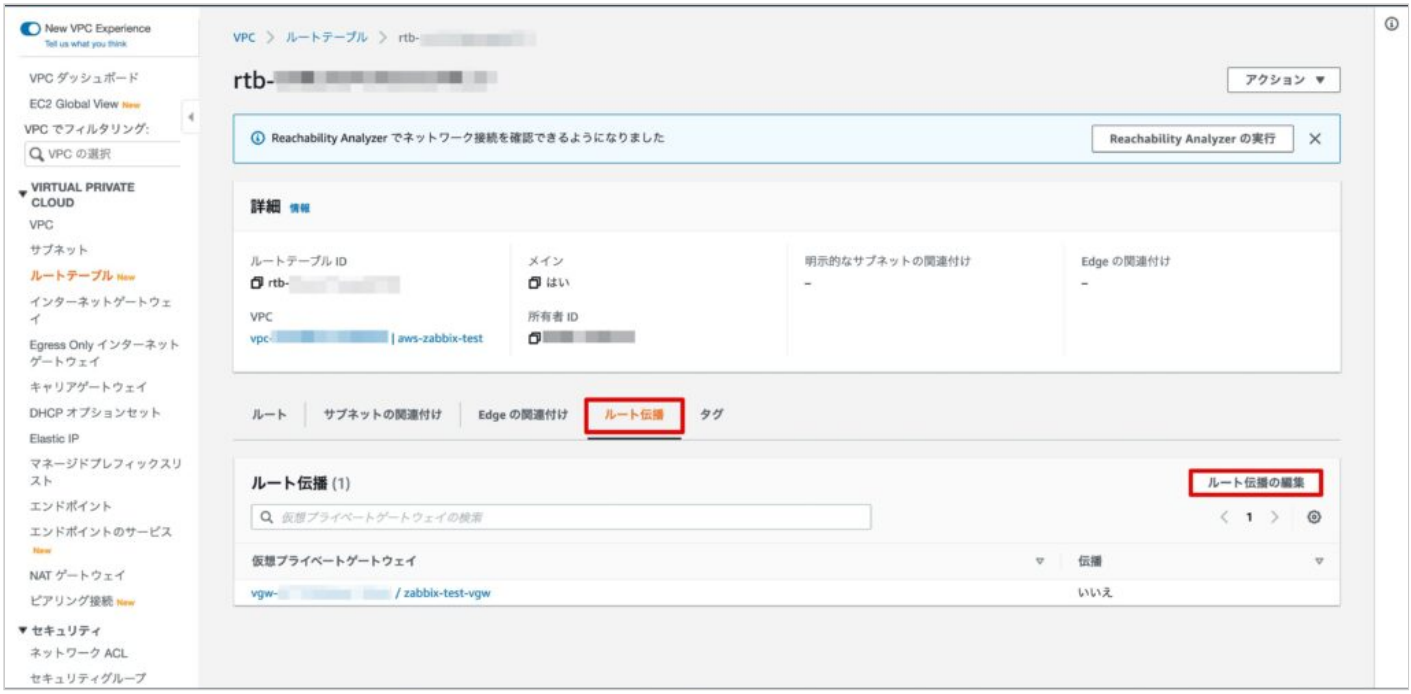
「attaching」の状態を経由し、



「attached」となれば、作成完了です。

ルートテーブルの設定

仮想プライベートゲートウェイからVPC内にルートを伝播するための設定を行います。
ルートテーブルの「ルート伝播」タブを選択し、「ルート伝播の編集」をクリックします。



作成した仮想プライベートゲートウェイの伝播の「有効化」にチェックを入れます。

伝播が「はい」となれば、設定完了です。

サイト間のVPN接続の作成

カスタマーゲートウェイと仮想プライベートゲートウェイの間でVPNを構築するため、サイト間のVPN接続を作成します。

サイト間のVPN接続 →「VPN接続の作成」をクリックします。

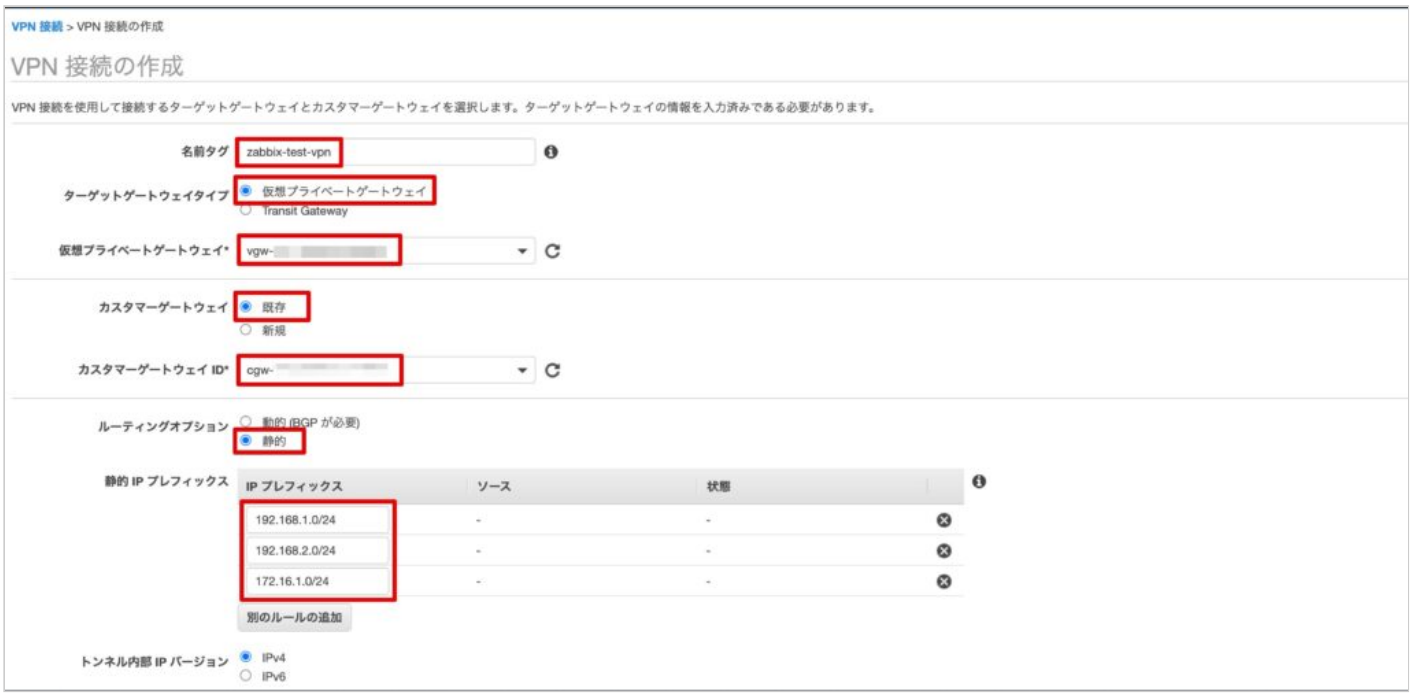
※VPN接続を作成すると利用料金が発生します※ 利用料金の説明 →こちら

下記を設定します。

名前タグ：zabbix-test-vpn ※任意の名前
ターゲットゲートウェイタイプ：仮想プライベートゲートウェイ

仮想プライベートゲートウェイ：作成した仮想プライベートゲートウェイを選択
カスタマーゲートウェイ：既存
カスタマーゲートウェイID：作成したカスタマーゲートウェイを選択
ルーティングオプション：静的
静的IPプレフィックス：下記を追加

- 192.168.1.0/24(ローカルネットワーク)
- 192.168.2.0/24(CMLのルータ間セグメント)
- 172.16.1.0/24(サーバー接続セグメント)

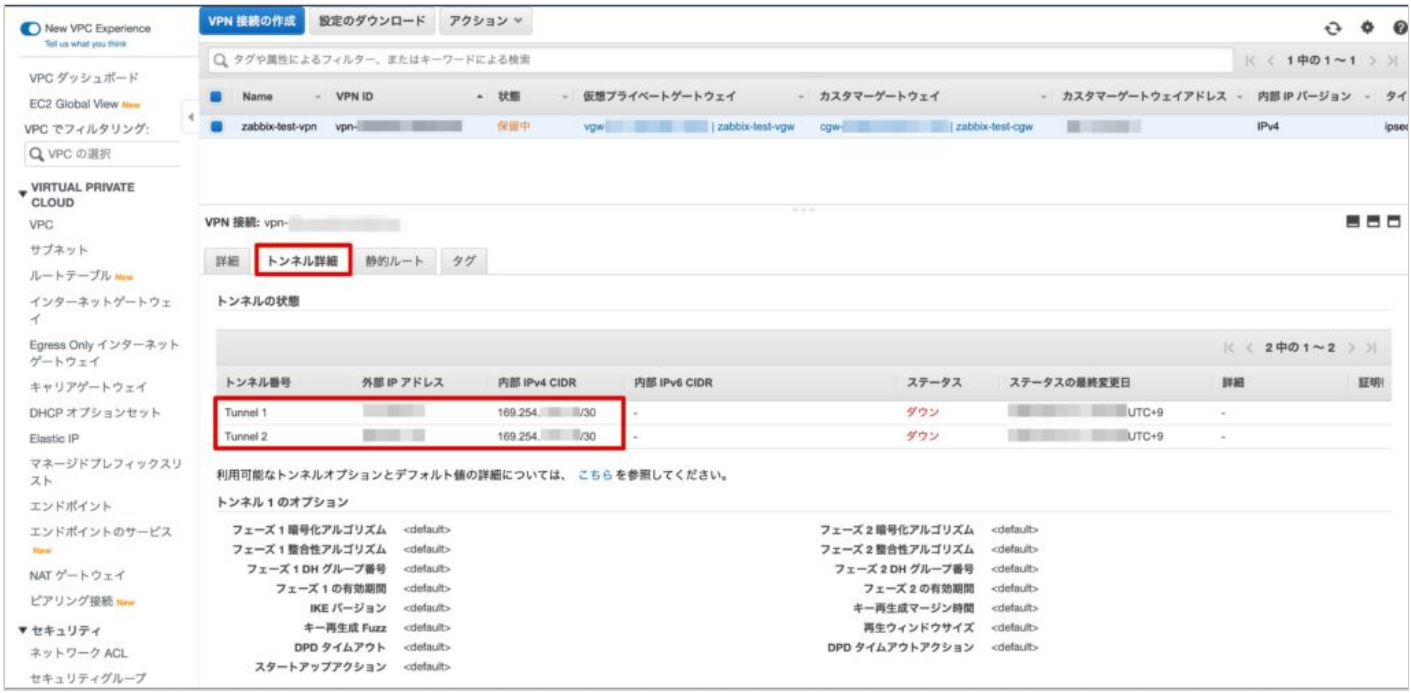


トンネルオプションは設定変更不要です。

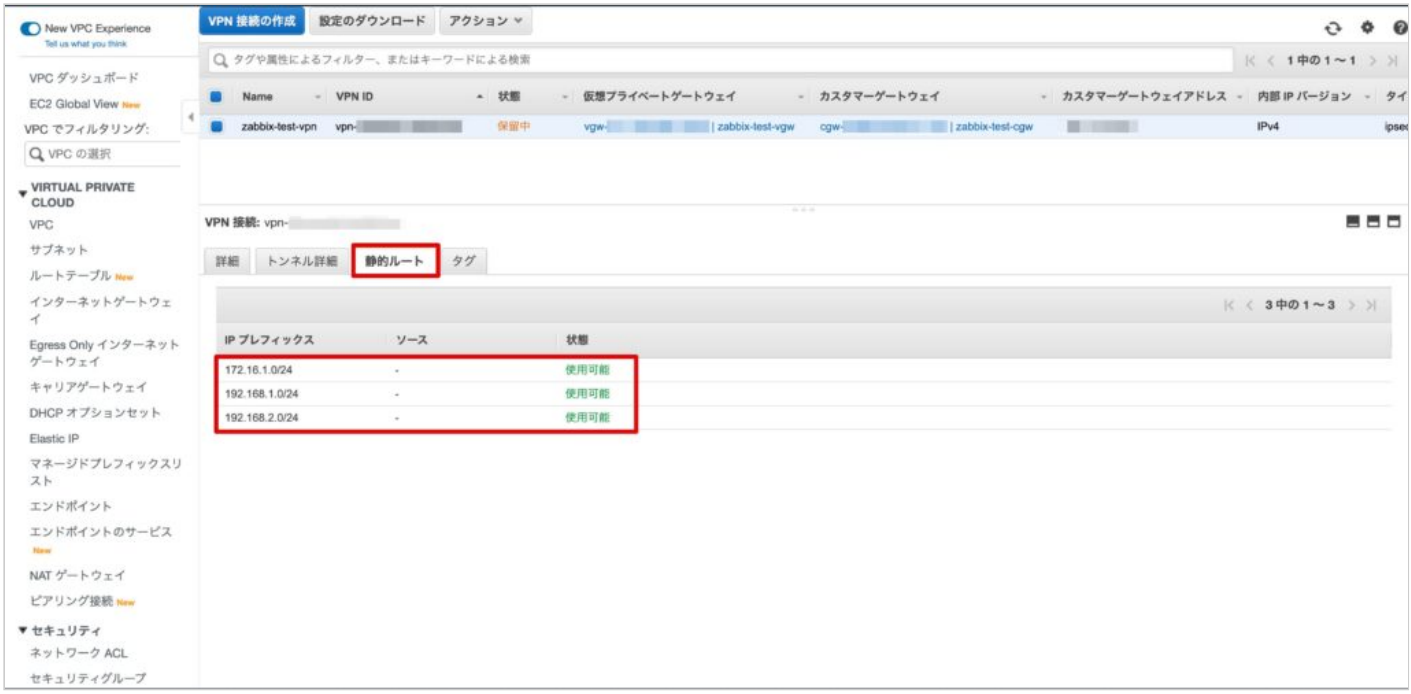
作成したVPN接続を確認します。
「詳細」タブで、「仮想プライベートゲートウェイ」と「カスタマーゲートウェイ」と「VPC」が正しく

設定されていることを確認します。

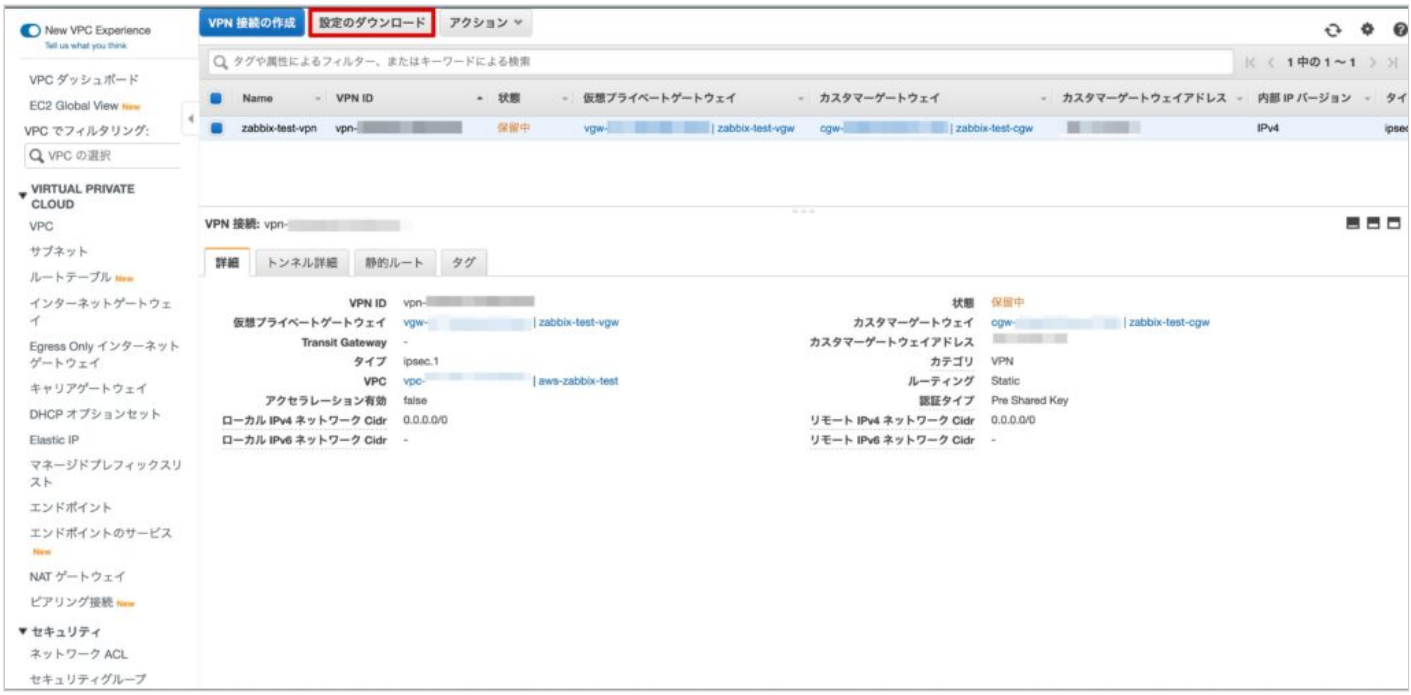
「トンネル詳細」タブで、トンネルの設定を確認します。
AWSのVPN接続では、冗長化のためにデフォルトで2つのトンネルが作成されます。
外部IPアドレスは「グローバルIPアドレス」、トンネルインターフェースのIPアドレスは「リンクローカルアドレス」が利用されます。



「静的ルート」タブで、設定したIPプレフィックスが「使用可能」となっていることを確認します。



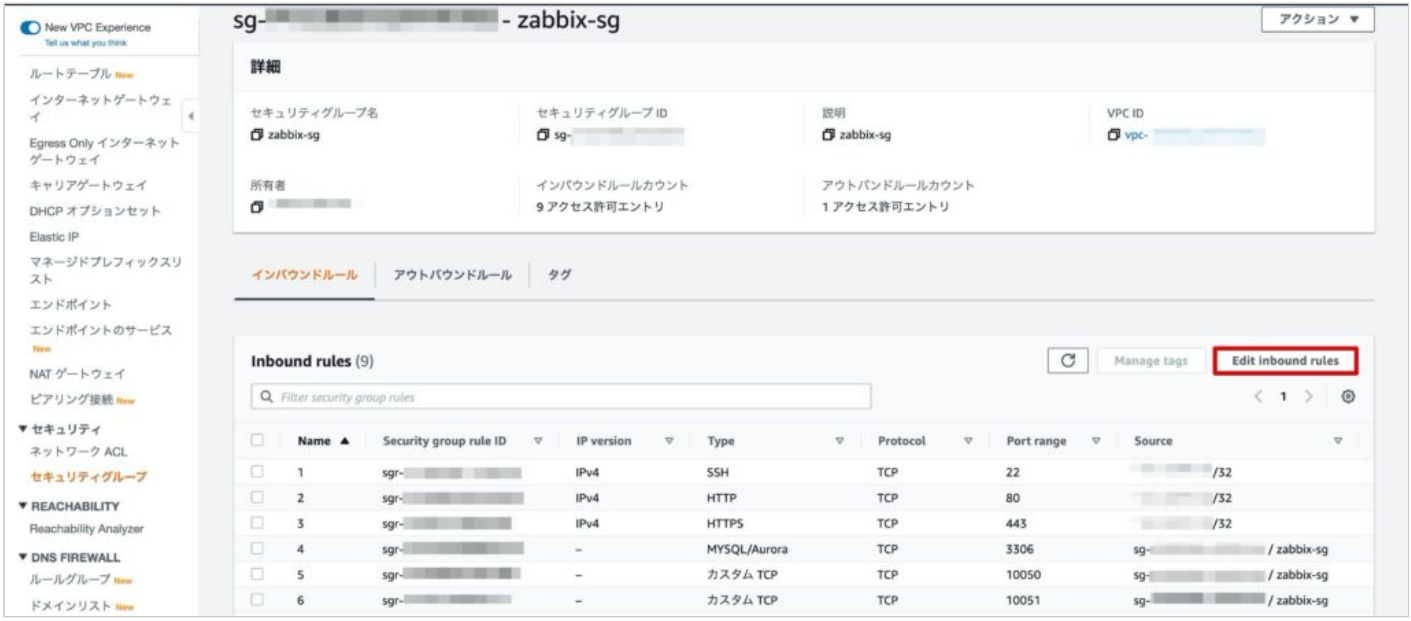
ネットワーク機器の設定サンプルをダウンロードします。
「設定のダウンロード」をクリックします。



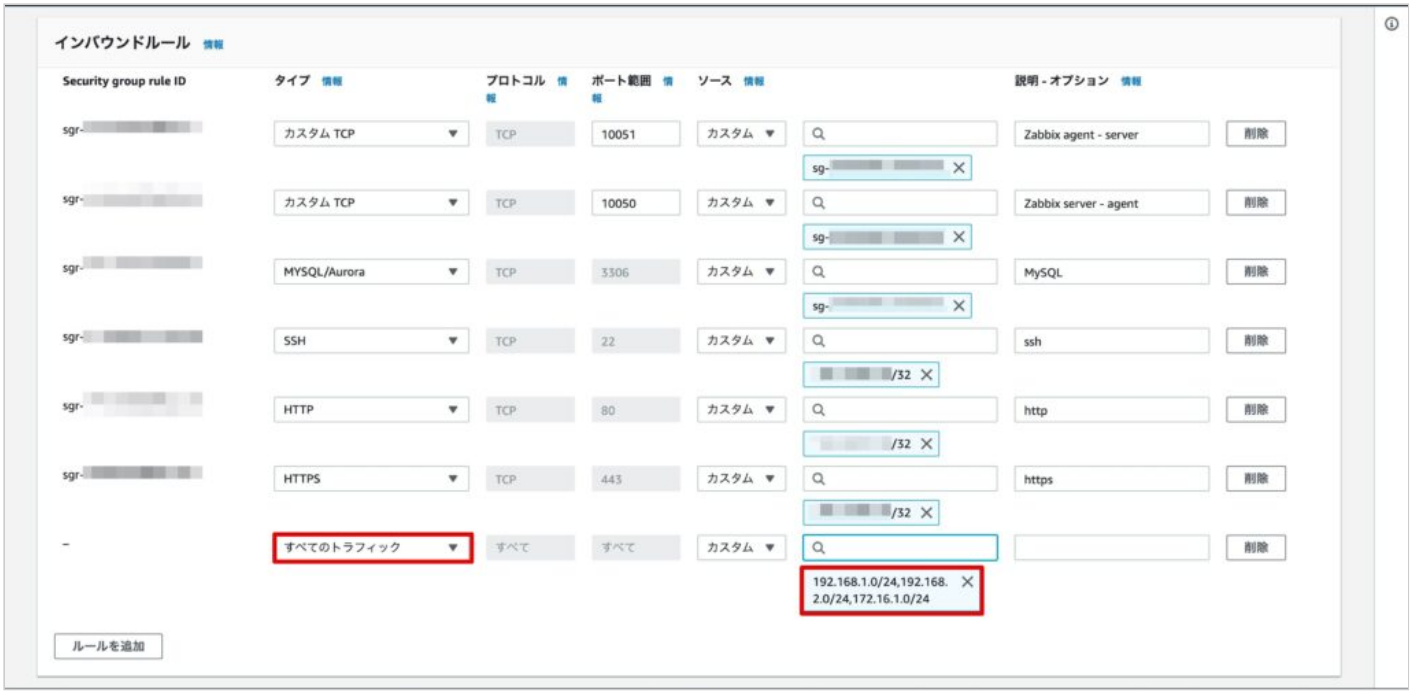
ベンダーは「Cisco Systems, Inc.」、プラットフォームは「Cisco ASR 1000」を選択し、ダウンロードをクリックします。

セキュリティグループの設定

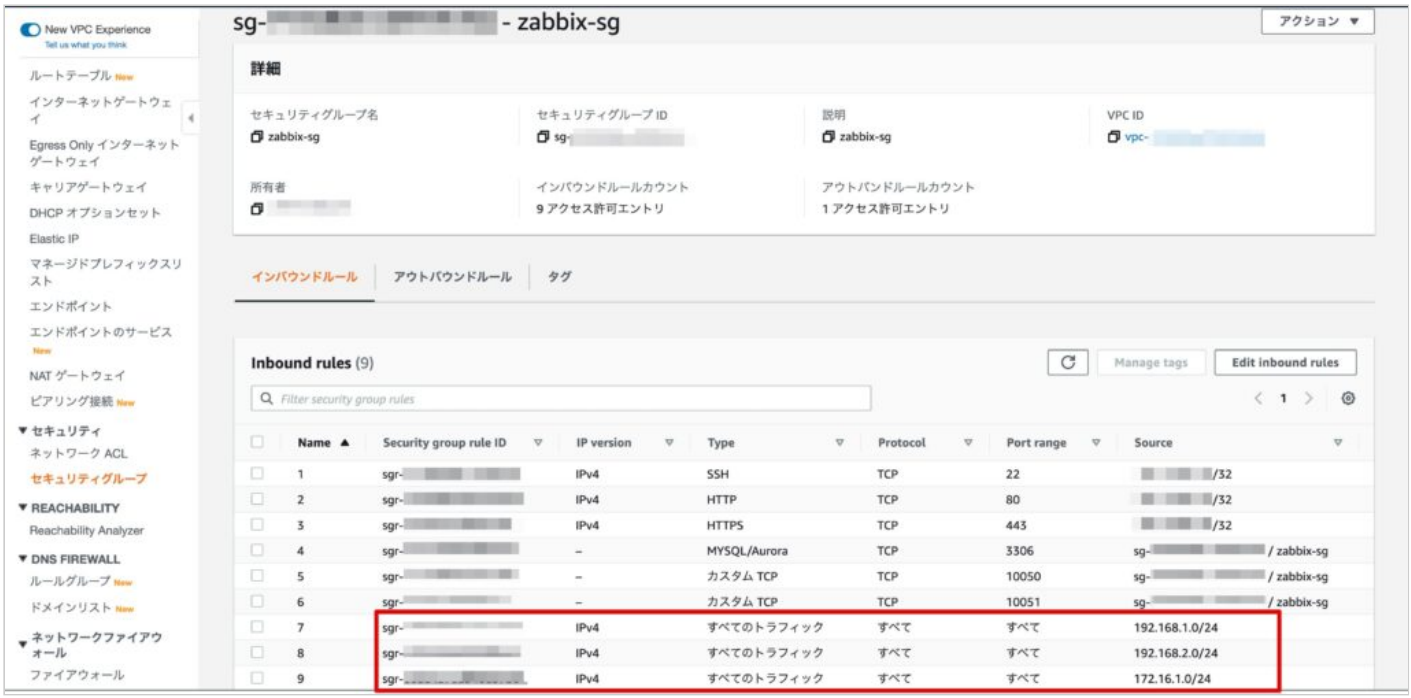
EC2に適用したセキュリティグループ(zabbix-sg)の「Edit inbound rules」をクリックします。



タイプは「全てのトラフィック」、ソースは「192.168.1.0/24,192.168.2.0/24,172.16.1.0/24」のルールを追加します。



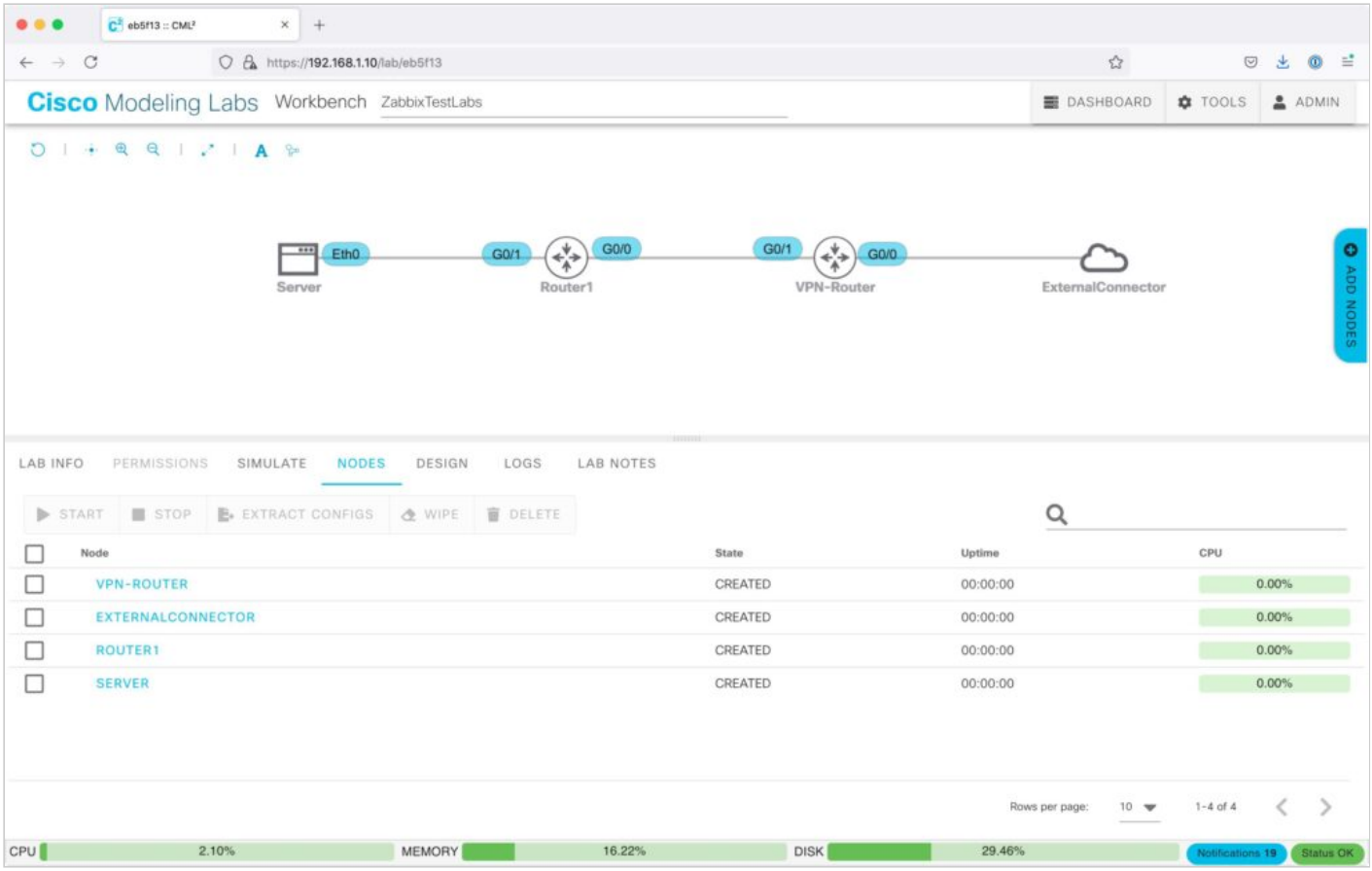
ルールが追加されていることを確認します。



CMLの構築

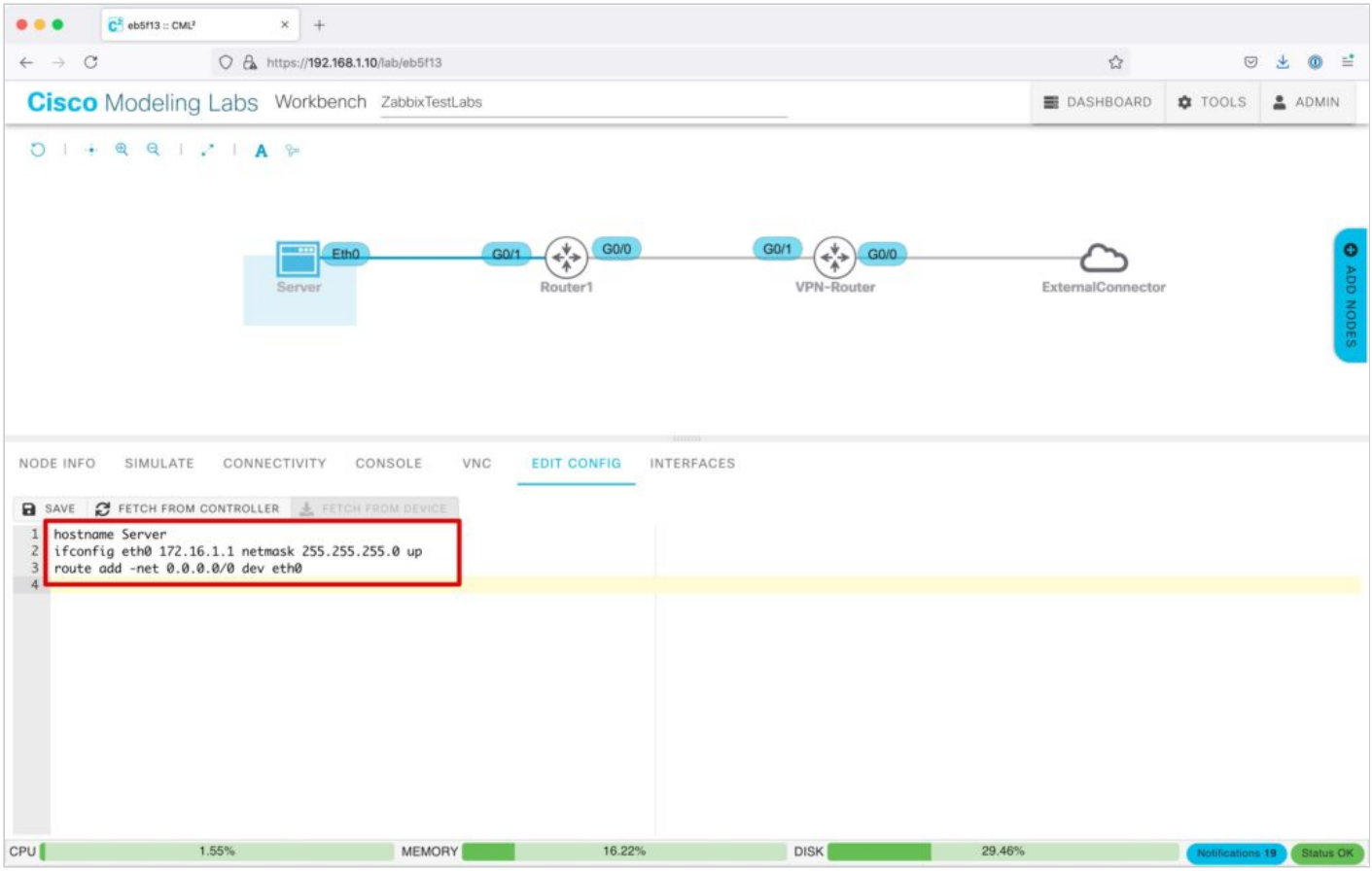
CMLの設定

Server、IOSv(VPN-Router, Router1)、ExternalConnectorを配置し、下記の通りリンクを接続します。



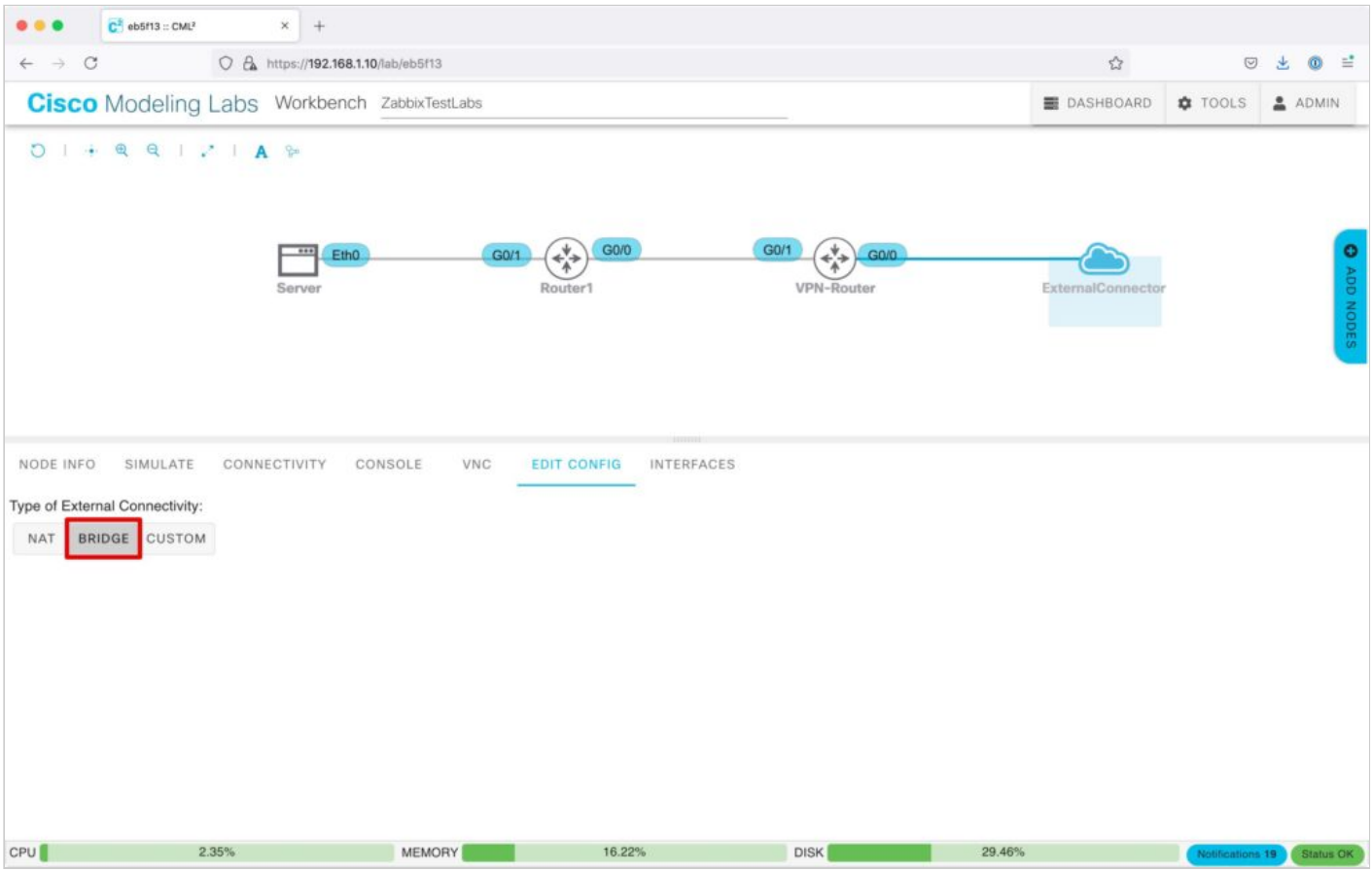
Serverは、「EDIT CONFIG」で下記の設定を行い起動します。

```
hostname Server
ifconfig eth0 172.16.1.1 netmask 255.255.255.0 up
route add -net 0.0.0.0/0 dev eth0
```



ExternalConnectorは、「EDIT CONFIG」で「BRIDGE」を選択します。

※CMLの外部ネットワーク接続の詳細はこちらで説明しています。



VPN-Routerを設定します。

*の部分はダウンロードしたテンプレート通りです。
[VPN-Router]

```
crypto keyring keyring-vpn-******************
 local-address 192.168.1.100
 pre-shared-key address ***.***.***.*** key ********************************

crypto isakmp policy 200
 encr aes
 authentication pre-share
 group 2
 lifetime 28800
exit

crypto isakmp profile isakmp-vpn-********************
 keyring keyring-vpn-********************
 match identity address ***.***.***.*** 255.255.255.255
 local-address XXX.XXX.XXX.XXX ※ここは自身のグローバルアドレスを指定
exit

crypto ipsec transform-set ipsec-prop-vpn-******************** esp-aes 128 esp-sha-
hmac
 mode tunnel
exit

crypto ipsec profile ipsec-vpn-********************
 set pfs group2
 set security-association lifetime seconds 3600
 set transform-set ipsec-prop-vpn-********************
exit

interface Tunnel1
 ip address 169.254.173.150 255.255.255.252
 ip virtual-reassembly
 tunnel source 192.168.1.100
 tunnel destination ***.***.***.***
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-vpn-********************
```

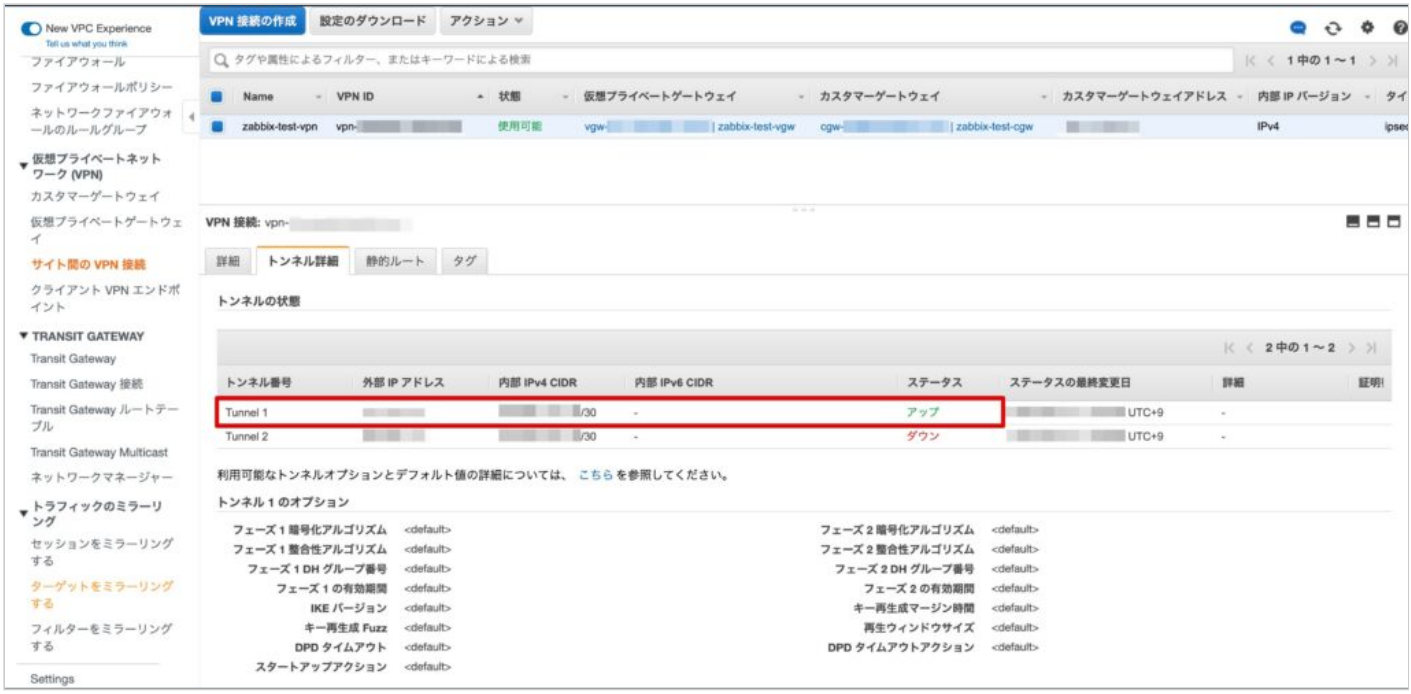
```
 ip tcp adjust-mss 1379
 no shutdown
exit

interface GigabitEthernet0/0
 ip address 192.168.1.100 255.255.255.0
 no shutdown
exit

interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.0
 no shutdown
exit

ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 10.0.0.0 255.255.255.0 Tunnel1
ip route 172.16.1.0 255.255.255.0 192.168.2.1
```

Tunnel1が作成され、リンクアップしていることを確認します。

```
show ip int brief
```

```
Router#show ip int brief
Interface                  IP-Address      OK? Method
Status         Protocol
GigabitEthernet0/0         192.168.1.100   YES manual   up
up
GigabitEthernet0/1         192.168.2.2     YES manual   up
up
Tunnel1                    169.254.173.150 YES manual   up
up
```

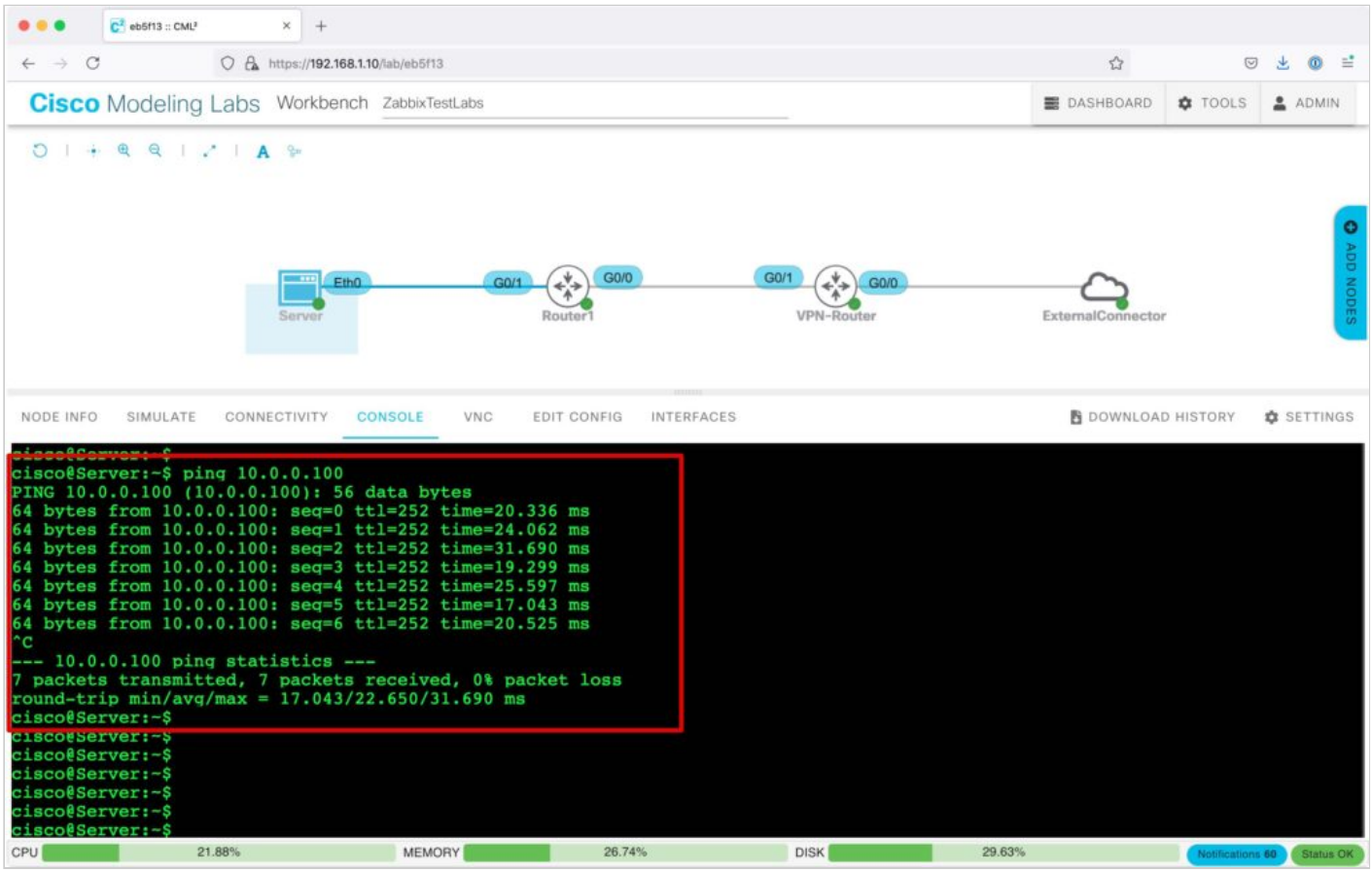
AWSのVPN接続の「トンネル詳細」で、Tunnel1のステータスが「アップ」していることを確認します。



疎通確認

ServerからEC2に向けてPingを実施し、疎通可能であることを確認します。

```
ping 10.0.0.100
```



EC2からServerに向けてPingを実施し、疎通可能であることを確認します。

```
ping 172.16.1.1
```

```
[[ec2-user@ip-10-0-0-100 ~]$
[[ec2-user@ip-10-0-0-100 ~]$ ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=62 time=17.8 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=62 time=34.1 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=62 time=59.9 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=62 time=16.3 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=62 time=16.5 ms
^C
--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 16.338/28.986/59.963/16.879 ms
[[ec2-user@ip-10-0-0-100 ~]$
```

これで、AWS上での監視サーバー(Zabbix)構築【5.AWSとCMLのVPN接続】の説明は完了です！