

# AWSサイト間VPNの構築（4.CMLの構築）

AWS



## AWSサイト間VPNの構築 （4.CMLの構築）

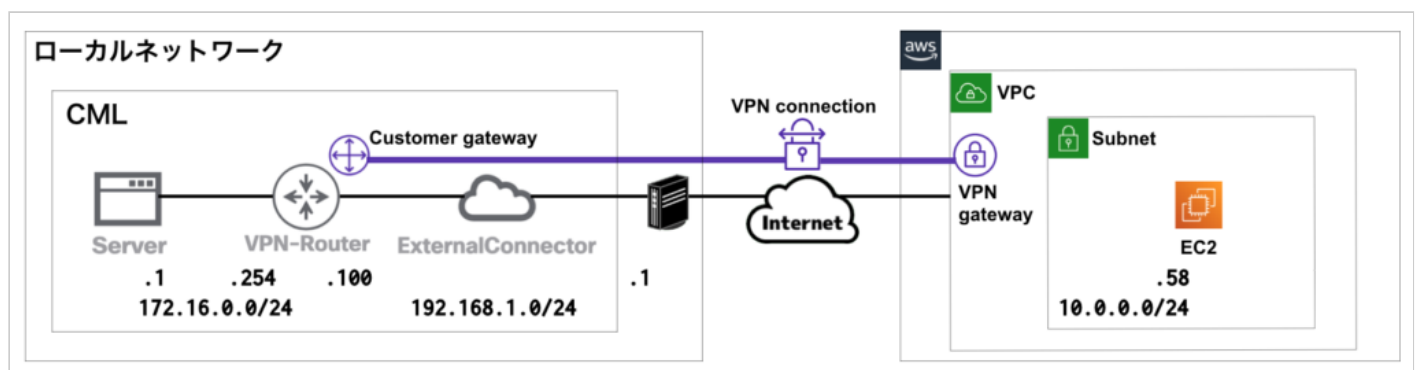
2021.09.04 2021.08.14

[【前回】AWSサイト間VPNの構築（3.AWSのVPN構築）](#)[【次回】AWSサイト間VPNの構築（5.暗号化・ハッシュアルゴリズム変更）](#)

## ネットワーク構成

下記のネットワーク構成で、CML上のLAN(172.16.0.0/24)とAWSのサブネット(10.0.0.0/24)が直接通信できるようにします。

※Server(172.16.0.1)からEC2(10.0.0.58)にPingによる疎通確認ができるようにしていきます。



## CMLの構築

AWSのサイト間VPN接続の検証のためにCMLを構築します。

## CMLの基本設定

Server、IOSv(VPN-Router)、ExternalConnectorを配置します。

RouterのGi0/0をExternalConnectorに、Gi0/1をServerに接続します。

The screenshot shows the Cisco Modeling Labs Workbench interface. At the top, there's a navigation bar with 'Cisco Modeling Labs Workbench' and 'AWS-VPN-TestLabs'. Below it, a network topology diagram shows a 'Server' connected to a 'VPN-Router' via 'Eth0' and 'G0/1', and the 'VPN-Router' connected to an 'ExternalConnector' via 'G0/0'. Below the diagram, there's a 'NODES' tab with a table listing the nodes.

Node	State	Uptime	CPU
EXTERNALCONNECTOR	CREATED	00:00:00	0.00%
VPN-ROUTER	CREATED	00:00:00	0.00%
SERVER	CREATED	00:00:00	0.00%

At the bottom, there's a status bar showing CPU usage (0.88%), MEMORY (12.36%), and DISK (18.66%).

Serverは、「EDIT CONFIG」で下記の設定を行い起動します。

```
hostname Server
ifconfig eth0 172.16.0.1 netmask 255.255.255.0 up
route add -net 0.0.0.0/0 dev eth0
```

The screenshot shows the Cisco Modeling Labs Workbench interface. At the top, the browser address is `https://192.168.1.10/lab/d89c2a`. The main workspace displays a network diagram with a 'Server' node connected to a 'VPN-Router' via 'Eth0' and 'G0/1' interfaces, and the router connected to an 'ExternalConnector' via 'G0/0'. Below the diagram, the 'EDIT CONFIG' tab is active, showing the following configuration for the 'Server' node:

```
1 hostname Server
2 ifconfig eth0 172.16.0.1 netmask 255.255.255.0 up
3 route add -net 0.0.0.0/0 dev eth0
4
```

The bottom status bar shows CPU usage at 1.57%, Memory at 12.36%, and Disk usage at 18.66%.

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。

The screenshot shows the same network diagram, but now the 'ExternalConnector' node is highlighted with a red box. Below the diagram, the 'EDIT CONFIG' tab is active, and the 'Type of External Connectivity' section is visible. The 'BRIDGE' option is selected and highlighted with a red box, while 'NAT' and 'CUSTOM' are unselected.

CPU usage is now 0.75%, Memory is 12.36%, and Disk usage is 18.66%.

Routerのインターフェースを設定します。

```
int Gi0/0
ip address 192.168.1.100 255.255.255.0
no shut

int Gi0/1
ip address 172.16.0.254 255.255.255.0
no shut
```

RouterのインターフェースにIPアドレスが設定され、リンクアップしたことを確認します。

```
show ip int brief
```

The screenshot displays the Cisco Modeling Labs Workbench interface for a lab named 'AWS-VPN-TestLabs'. The topology shows a 'Server' connected to 'VPN-Router' via 'Eth0' and 'G0/1', and the 'VPN-Router' connected to an 'ExternalConnector' via 'G0/0'. The console window shows the command 'show ip int brief' being executed on the 'VPN-Router'.

Interface	IP Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.100	YES	manual	up	up
GigabitEthernet0/1	172.16.0.254	YES	manual	up	up
GigabitEthernet0/2	unassigned	no	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
SVI0	192.168.1.100	YES	unset	up	up

The console output also shows the status of other interfaces (GigabitEthernet0/2, GigabitEthernet0/3, and SVI0) and the CPU, MEMORY, and DISK usage at the bottom.

Routerのデフォルトルートを設定します。

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

※デフォルトルートのネクストホップは、自身のローカル環境のルータのIPアドレスを設定します。下記のコマンドで確認できます。

[Windowsのコマンドプロンプト]

```
route print -4
```

```
0.0.0.0          0.0.0.0          192.168.1.1
```

[Macのターミナル]

```
netstat -rn -f inet | grep default
```

```
default          192.168.1.1
```

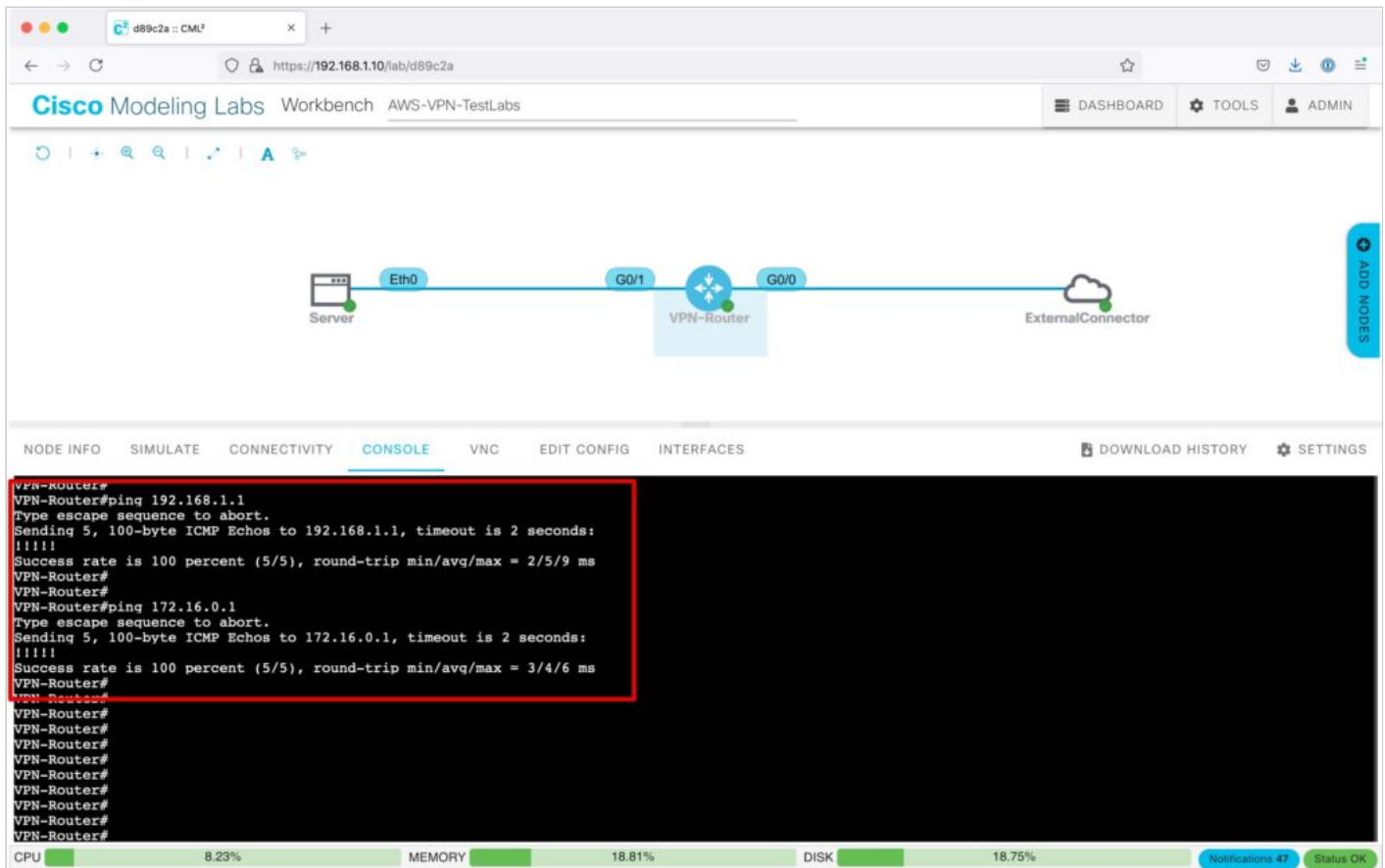
Routerのデフォルトルートが設定されたことを確認します。

```
show ip route
```

The screenshot shows the Cisco Modeling Labs Workbench interface. At the top, there's a navigation bar with 'DASHBOARD', 'TOOLS', and 'ADMIN'. Below it, a network diagram is visible, showing a 'Server' connected to a 'VPN-Router' via 'Eth0' and 'G0/1' interfaces, and the 'VPN-Router' connected to an 'ExternalConnector' via 'G0/0' interface. The main area displays the 'CONSOLE' output for the 'VPN-Router'. The output shows the command 'show ip route' and its result, which includes a list of routes and their next hops. The route 'S\* 0.0.0.0/0 [1/0] via 192.168.1.1' is highlighted with a red box. At the bottom, there's a status bar showing CPU usage (6.42%), MEMORY usage (18.81%), DISK usage (18.75%), and a 'Status OK' indicator.

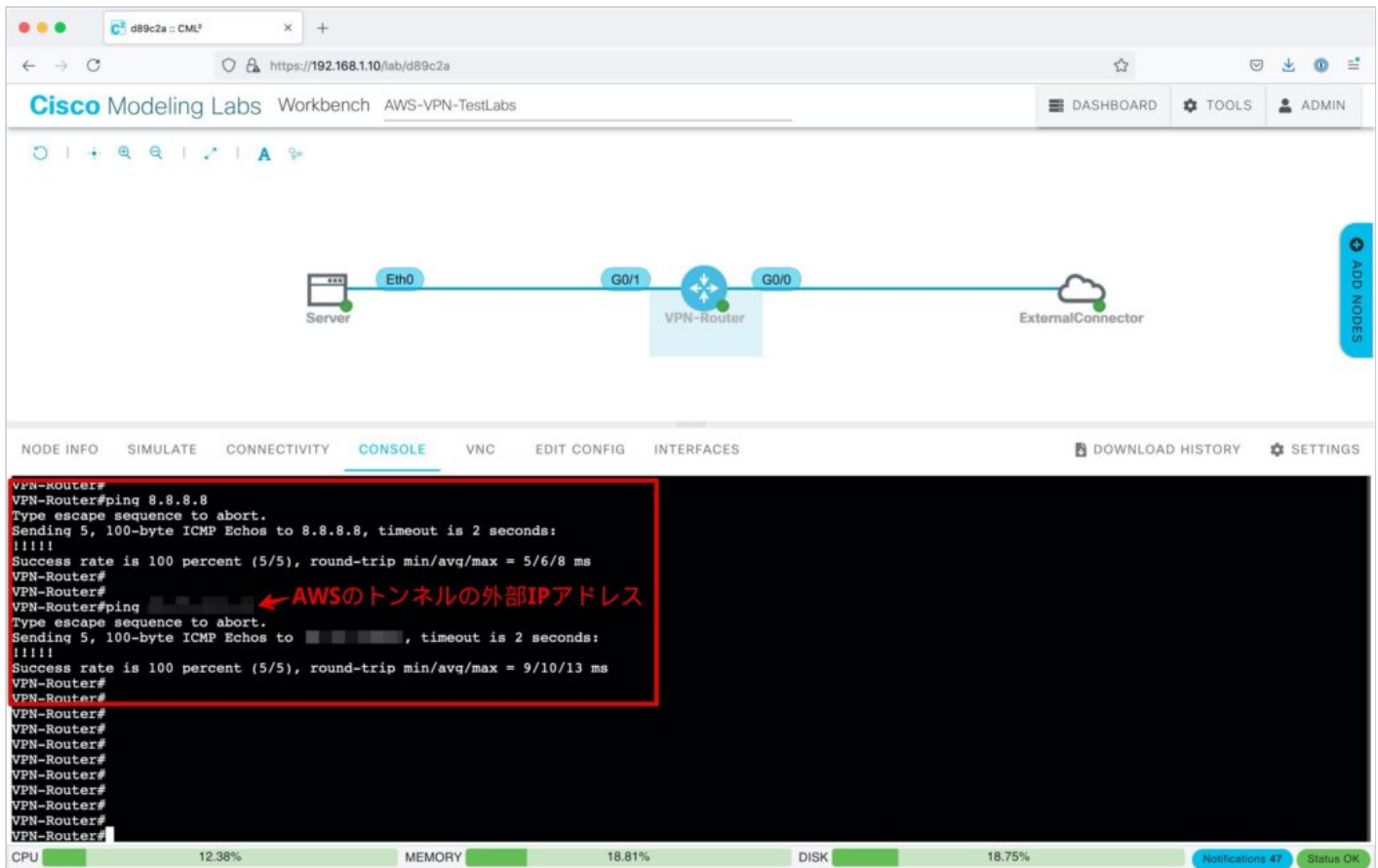
隣接機器にPingを実施し、疎通可能であることを確認します。

```
ping 192.168.1.1  
ping 172.16.0.1
```



インターネット内とAWSのトンネルインターフェースの外部IPアドレスにPingを実施し、疎通可能であることを確認します。

```
ping 8.8.8.8 ※Googleが提供している「Google Public DNS」のIPアドレス  
ping X.X.X.X ※AWSのトンネルインターフェースの外部IPアドレス
```



## CMLのVPN設定

AWSの「サイト間のVPN接続」から設定のサンプルをダウンロードできます。

「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。





ダウンロードした設定サンプルから、今回は必要最低限の下記を設定します。AWSのVPN接続は、デフォルトでトンネルインターフェースが2つ作成されますが、片方のみ接続します。

\*の部分はダウンロードしたテンプレート通りです。

```
crypto isakmp policy 200
  encryption aes 128
  authentication pre-share
  group 2
  lifetime 28800
  hash sha
exit
```

```
crypto keyring keyring-vpn-*****
  local-address 192.168.1.100 ※ここはCML上のルーターのGi0/0のアドレスを指定
  pre-shared-key address ***, ***, ***, *** key *****
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 169.254.27.178 255.255.255.252
  ip virtual-reassembly
  tunnel source 192.168.1.100 ※ここはCML上のルーターのGi0/0のアドレスを指定
  tunnel destination ***, ***, ***, ***
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-vpn-*****
  ip tcp adjust-mss 1379
  no shutdown
exit

ip route 10.0.0.0 255.255.255.0 Tunnel1
```

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
```

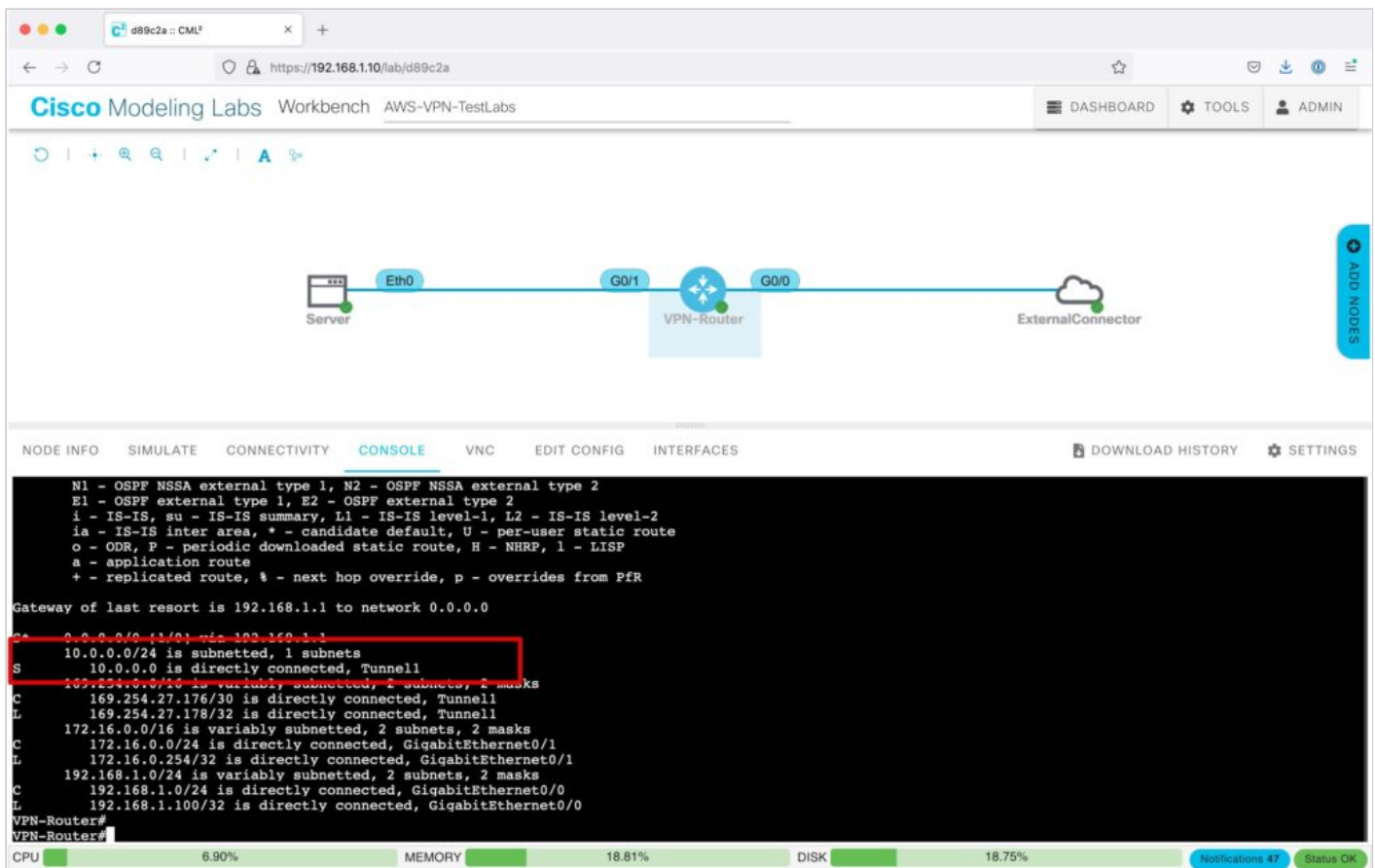
The screenshot shows the Cisco Modeling Labs Workbench interface. The topology diagram at the top shows a Server connected to a VPN-Router via Eth0 and G0/1, and the VPN-Router connected to an ExternalConnector via G0/0. The console window displays the output of the command 'show ip int brief' on the VPN-Router. The output is as follows:

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.100	YES	manual	up	up
GigabitEthernet0/1	172.16.0.254	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
Tunnel1	169.254.27.178	YES	manual	up	up

The Tunnel1 interface is highlighted with a red box. The bottom status bar shows CPU usage at 11.88%, MEMORY at 18.81%, and DISK at 18.75%.

AWSのEC2を配置したサブネット(10.0.0.0/24)向けのルーティングが追加されていることを確認します。

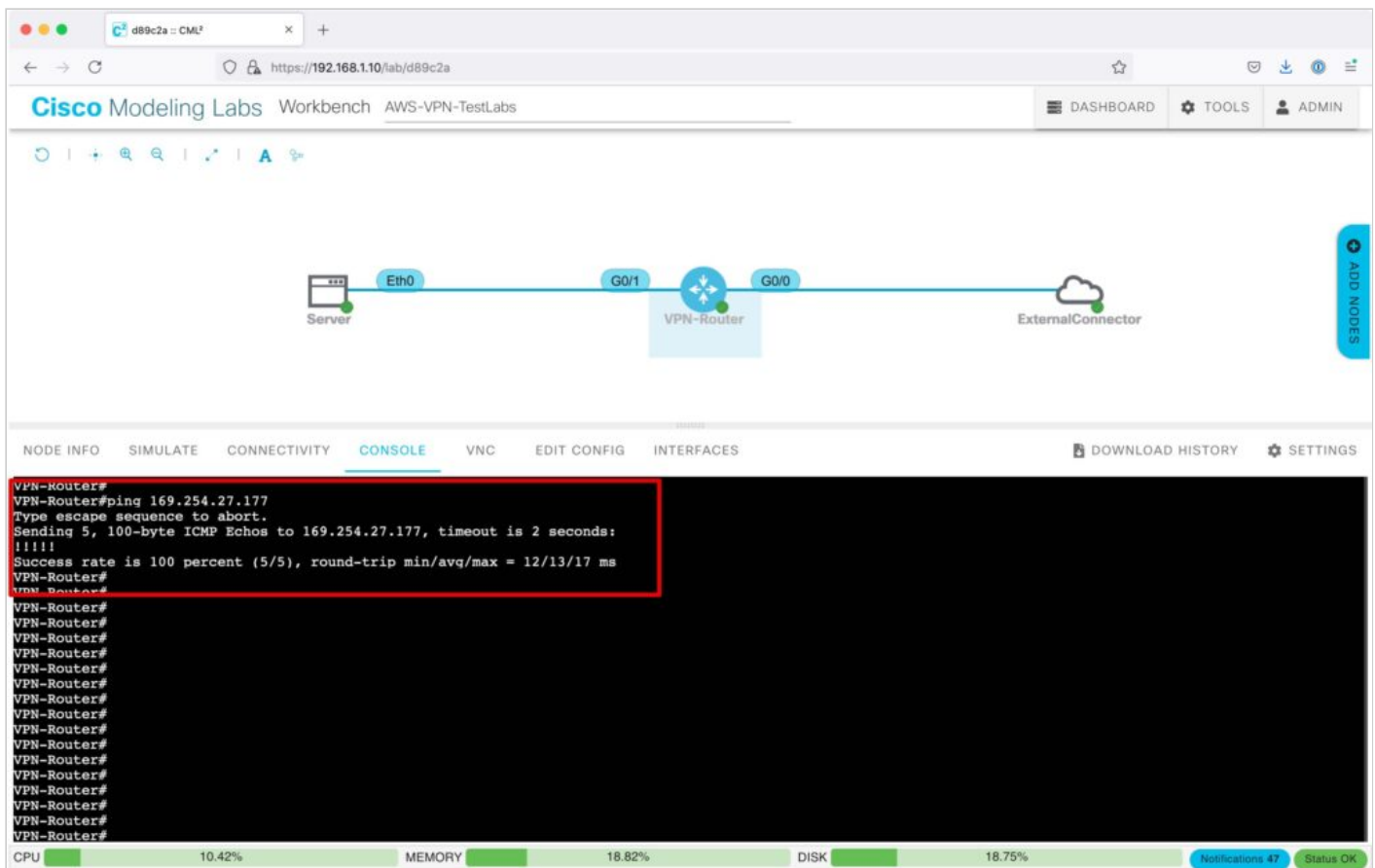
```
show ip route
```



AWSのVPN接続のトンネルインターフェースにPingを実施し、疎通可能であることを確認します。  
トンネルインターフェースのセグメント「169.254.27.176/30」は下記のようにアドレスがアサインされます。

- 169.254.27.176 ネットワークアドレス
- 169.254.27.177 AWS側のトンネルインターフェース
- 169.254.27.178 カスタマー側のトンネルインターフェース
- 169.254.27.179 ブroadcastアドレス

ping 169.254.27.177



AWSのVPN接続の「トンネル詳細」を確認すると、Tunnel1のステータスが「アップ」になり、VPN接続が確立されています。



## 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 10.0.0.58
```

The screenshot shows the Cisco Modeling Labs Workbench interface. At the top, there's a navigation bar with 'DASHBOARD', 'TOOLS', and 'ADMIN'. Below it, a network diagram shows a 'Server' connected to a 'VPN-Router' via 'Eth0' and 'G0/1' interfaces, and the 'VPN-Router' connected to an 'ExternalConnector' via 'G0/0'. The 'CONSOLE' tab is active, displaying a terminal session where a ping command is executed from the 'cisco@Server' prompt. The ping results show 6 packets transmitted, 6 received, and 0% packet loss. Below the console, there are status bars for CPU (8.58%), MEMORY (18.82%), and DISK (18.75%).

```
cisco@Server:~$ ping 10.0.0.58
PING 10.0.0.58 (10.0.0.58): 56 data bytes
64 bytes from 10.0.0.58: seq=0 ttl=253 time=16.408 ms
64 bytes from 10.0.0.58: seq=1 ttl=253 time=25.018 ms
64 bytes from 10.0.0.58: seq=2 ttl=253 time=19.855 ms
64 bytes from 10.0.0.58: seq=3 ttl=253 time=20.391 ms
64 bytes from 10.0.0.58: seq=4 ttl=253 time=15.246 ms
64 bytes from 10.0.0.58: seq=5 ttl=253 time=19.514 ms
^C
--- 10.0.0.58 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 15.246/19.405/25.018 ms
cisco@Server:~$
```

CML上のVPN-RouterのGi0/0側でキャプチャすると、暗号化されて送信されていることが分かります。

The screenshot shows the Cisco Modeling Labs Workbench interface with the 'PACKET CAPTURE' tab active. A red arrow points to the 'G0/0' interface of the 'VPN-Router' with the label 'キャプチャポイント' (Capture Point). Below the network diagram, there's a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Four packets are highlighted with a red box, showing they are all ESP (Encapsulating Security Payload) packets. To the right, the 'Packet Details' panel shows the details for the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Encapsulating Security Payload.

No.	Time	Source	Destination	Protocol	Length	Info
4	1.341558	192.168.1.100	35.72.114.41	ESP	174	ESP (SPI=0xc3fa8708)
5	1.355457	35.72.114.41	192.168.1.100	ESP	174	ESP (SPI=0xe89655eb)
6	2.339257	192.168.1.100	35.72.114.41	ESP	174	ESP (SPI=0xc3fa8708)
7	2.347395	35.72.114.41	192.168.1.100	ESP	174	ESP (SPI=0xe89655eb)

## ルーターのステータス確認

フェーズ1(ISAKMP)のステータスを確認するには下記のコマンドを実行します。

stateが"QM IDLE"となっていれば、フェーズ1は成功しています。

```
show crypto isakmp sa
```

The screenshot shows the Cisco Modeling Labs (CML) Workbench interface. At the top, there's a navigation bar with 'Cisco Modeling Labs', 'Workbench', and 'AWS-VPN-TestLabs'. Below this is a network diagram showing a 'Server' connected to a 'VPN-Router' via 'Eth0' and 'G0/1' interfaces, and the 'VPN-Router' connected to an 'ExternalConnector' via 'G0/0'. The 'CONSOLE' tab is active, displaying the output of the 'show crypto isakmp sa' command on the 'VPN-Router'. The output shows an IPv4 Crypto ISAKMP SA entry with 'src' 192.168.1.100, 'state' QM IDLE (highlighted with a red box), and 'conn-id status' 1004 ACTIVE. Below the console output, there's a status bar showing CPU usage at 8.55%, MEMORY at 18.65%, and DISK at 27.81%. There are also 'Notifications 25' and 'Status OK' indicators.

フェーズ2(IPSec)のステータスを確認するには下記のコマンドを実行します。

“pkts encrypt: ”と“pkts decrypt: ”の数値がカウントされていれば、暗号化通信が行われていることを示しています。

```
show crypto ipsec sa
```



```
VPN-Router#  
VPN-Router#show crypto ipsec sa  
  
interface: Tunnel1  
Crypto map tag: Tunnel1-head-0, local addr 192.168.1.100  
  
protected vrf: (none)  
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current peer _ port 4500  
PERMIT flags(origin is acl)  
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6  
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0  
  
local crypto endpt.: 192.168.1.100, remote crypto endpt.:  
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0  
current outbound spi: 0x0C0AC3BE(3423257534)  
PFS (Y/N): Y, DH group: group2  
  
inbound esp sas:
```

## ISAKMPのポート番号

通常、ISAKMPは、UDPの500番ポートが利用されますが、途中にNAT機器を挟んだ場合は、NATトラバース用の4500番ポートに変更されます。ルーターのWAN側インターフェースでアクセスリストによる制御を行う場合は、UDPの500番ポートと4500番ポートを許可するようにしましょう。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100		ISAKMP	206	Identity Protection (Main Mode)
2	0.116337		192.168.1.100	ISAKMP	178	Identity Protection (Main Mode)
3	0.134323	192.168.1.100		ISAKMP	326	Identity Protection (Main Mode)
4	0.143017		192.168.1.100	ISAKMP	286	Identity Protection (Main Mode)
5	0.172396	192.168.1.100		ISAKMP	154	Identity Protection (Main Mode)
6	0.180337		192.168.1.100	ISAKMP	122	Identity Protection (Main Mode)
7	0.199051	192.168.1.100		ISAKMP	362	Quick Mode
8	0.207683		192.168.1.100	ISAKMP	378	Quick Mode
9	0.281023	192.168.1.100		ISAKMP	106	Quick Mode
10	10.249688		192.168.1.100	ISAKMP	138	Informational
11	10.260664	192.168.1.100		ISAKMP	138	Informational
12	20.182233		192.168.1.100	ISAKMP	138	Informational
13	20.197856	192.168.1.100		ISAKMP	138	Informational
14	20.793054	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
15	20.802031		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)
16	21.793485	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
17	21.802640		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)
18	22.795887	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
19	22.804384		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)

▶ Frame 1: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits)

▶ Ethernet II, Src: RealtekU\_02:4c:b4 (52:54:00:02:4c:b4), Dst: ( )

▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: ( )

▶ User Datagram Protocol, Src Port: 500, Dst Port: 500

▶ Internet Security Association and Key Management Protocol



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100		ISAKMP	206	Identity Protection (Main Mode)
2	0.116337		192.168.1.100	ISAKMP	178	Identity Protection (Main Mode)
3	0.134323	192.168.1.100		ISAKMP	326	Identity Protection (Main Mode)
4	0.143017		192.168.1.100	ISAKMP	286	Identity Protection (Main Mode)
5	0.172396	192.168.1.100		ISAKMP	154	Identity Protection (Main Mode)
6	0.180337		192.168.1.100	ISAKMP	122	Identity Protection (Main Mode)
7	0.199051	192.168.1.100		ISAKMP	362	Quick Mode
8	0.207683		192.168.1.100	ISAKMP	378	Quick Mode
9	0.281023	192.168.1.100		ISAKMP	106	Quick Mode
10	10.249688		192.168.1.100	ISAKMP	138	Informational
11	10.260664	192.168.1.100		ISAKMP	138	Informational
12	20.182233		192.168.1.100	ISAKMP	138	Informational
13	20.197856	192.168.1.100		ISAKMP	138	Informational
14	20.793054	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
15	20.802031		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)
16	21.793485	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
17	21.802640		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)
18	22.795887	192.168.1.100		ESP	174	ESP (SPI=0xcda29c19)
19	22.804384		192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)

- Frame 5: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
- Ethernet II, Src: RealtekU\_02:4c:b4 (52:54:00:02:4c:b4), Dst: ( )
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: ( )
- User Datagram Protocol, Src Port: 4500, Dst Port: 4500
- UDP Encapsulation of IPsec Packets
- Internet Security Association and Key Management Protocol

アクセスリスト上は、UDP/500は"isakmp"、UDP/4500は"non500-isakmp"として表示されます。(以下は例として送信元を"ANY"としていますが、実際には対向のグローバルIPアドレスを指定します。)

Screenshot of the Cisco Modeling Labs (CML) Workbench interface. The top navigation bar shows the URL `https://192.168.1.10/lab/d89c2a` and the lab name `AWS-VPN-TestLabs`. The main workspace displays a network diagram with a `Server` connected to a `VPN-Router` via `Eth0` and `G0/1` interfaces, and the `VPN-Router` connected to an `ExternalConnector` via `G0/0`. Below the diagram, the `CONSOLE` tab is active, showing the following commands and output:

```
VPN-Router(config)#
VPN-Router(config)#access-list 100 permit udp any host 192.168.1.100 eq 500
VPN-Router(config)#access-list 100 permit udp any host 192.168.1.100 eq 4500
VPN-Router(config)#
VPN-Router(config)#end
VPN-Router#
VPN-Router#show access-list
Extended IP access list 100
 10 permit udp any host 192.168.1.100 eq isakmp
 20 permit udp any host 192.168.1.100 eq non500-isakmp
VPN-Router#
```

The bottom status bar shows system metrics: CPU 8.50%, MEMORY 18.65%, DISK 27.81%, and Notifications 23.

これで、AWSサイト間VPN接続のためのCML構築は完了です！