

# 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）

AWS



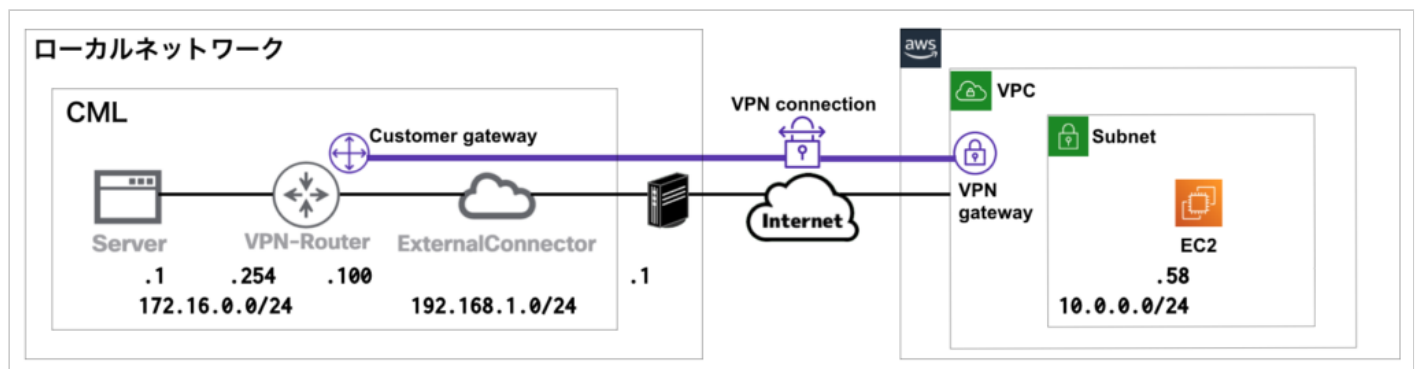
## AWSサイト間VPNの構築 (5.暗号化・ハッシュアルゴリズム変更)

2021.08.16 2021.08.15

[【前回】AWSサイト間VPNの構築（4.CMLの構築）](#)[【次回】AWSサイト間VPNの構築（6.IKEv2の設定）](#)

## ネットワーク構成

前回までで、下記の構成でAWSのサイト間VPNを構築し、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なりました。



## 暗号化アルゴリズム・ハッシュアルゴリズムの変更

### ルーターの設定変更

AWSの設定サンプルでは、セキュリティ強度が弱いため、下記の通りルーターの設定を変更します。

### ISAKMPの暗号化・ハッシュアルゴリズム

#### [AWSサンプル]

```
crypto isakmp policy 200
  encr aes 128
  hash sha
exit
```

#### [セキュリティ強化(256bitへ変更)]

```
crypto isakmp policy 200
  encr aes 256
  hash sha256
exit
```

### IPSECの暗号化・ハッシュアルゴリズム

#### [AWSサンプル]

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

#### [セキュリティ強化(256bitへ変更)]

```
crypto ipsec transform-set ipsec-prop-vpn-***** esp-aes 256 esp-sha256-
hmac
mode tunnel
exit
```

## ルーターの設定確認

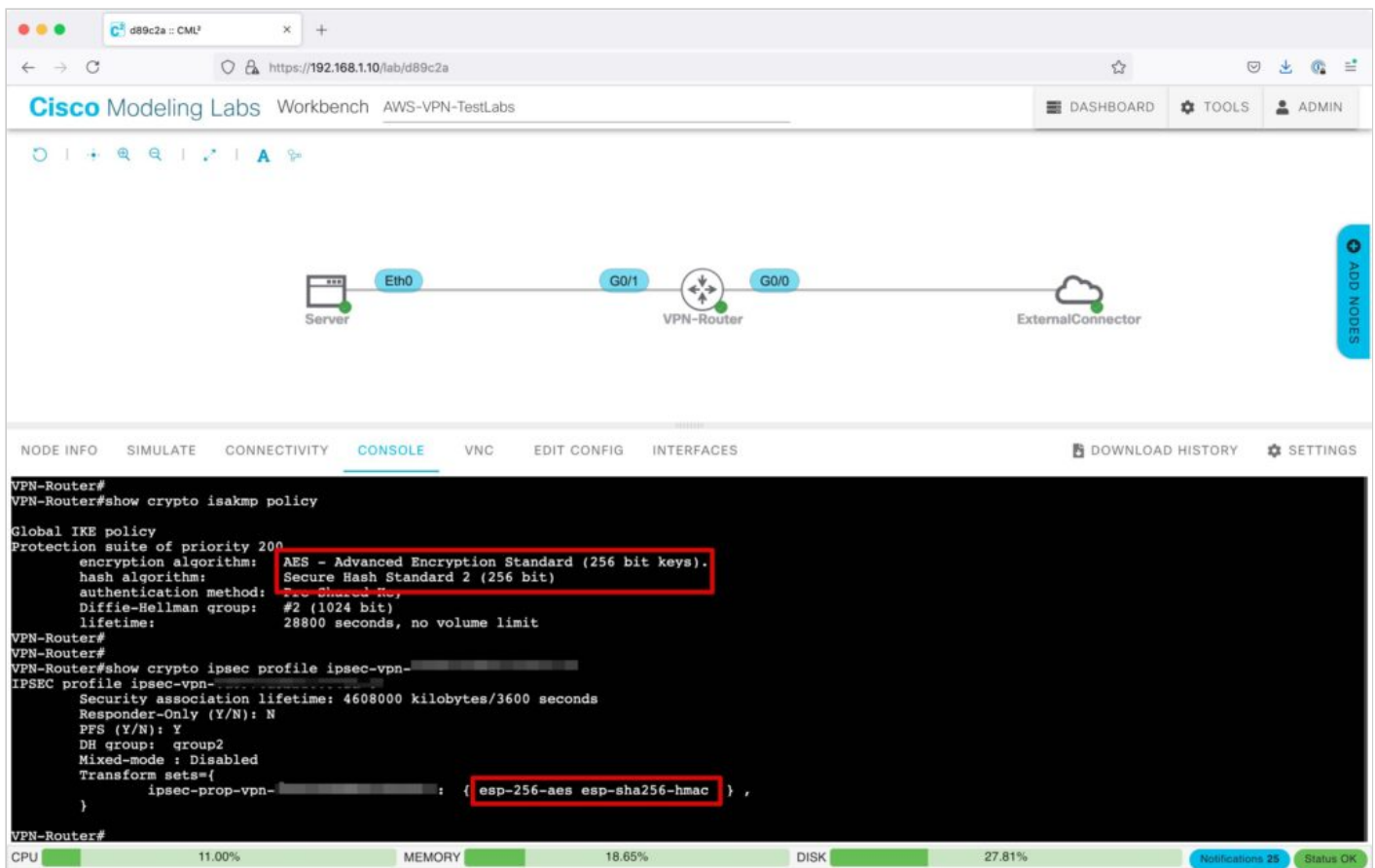
ISAKMPとIPSecの設定を確認します。それぞれ、“256bit”に変更されています。

#### [ISAKMP]

```
show crypto isakmp policy
```

#### [IPSec]

```
show crypto ipsec profile プロファイル名
```



## VPN接続確認

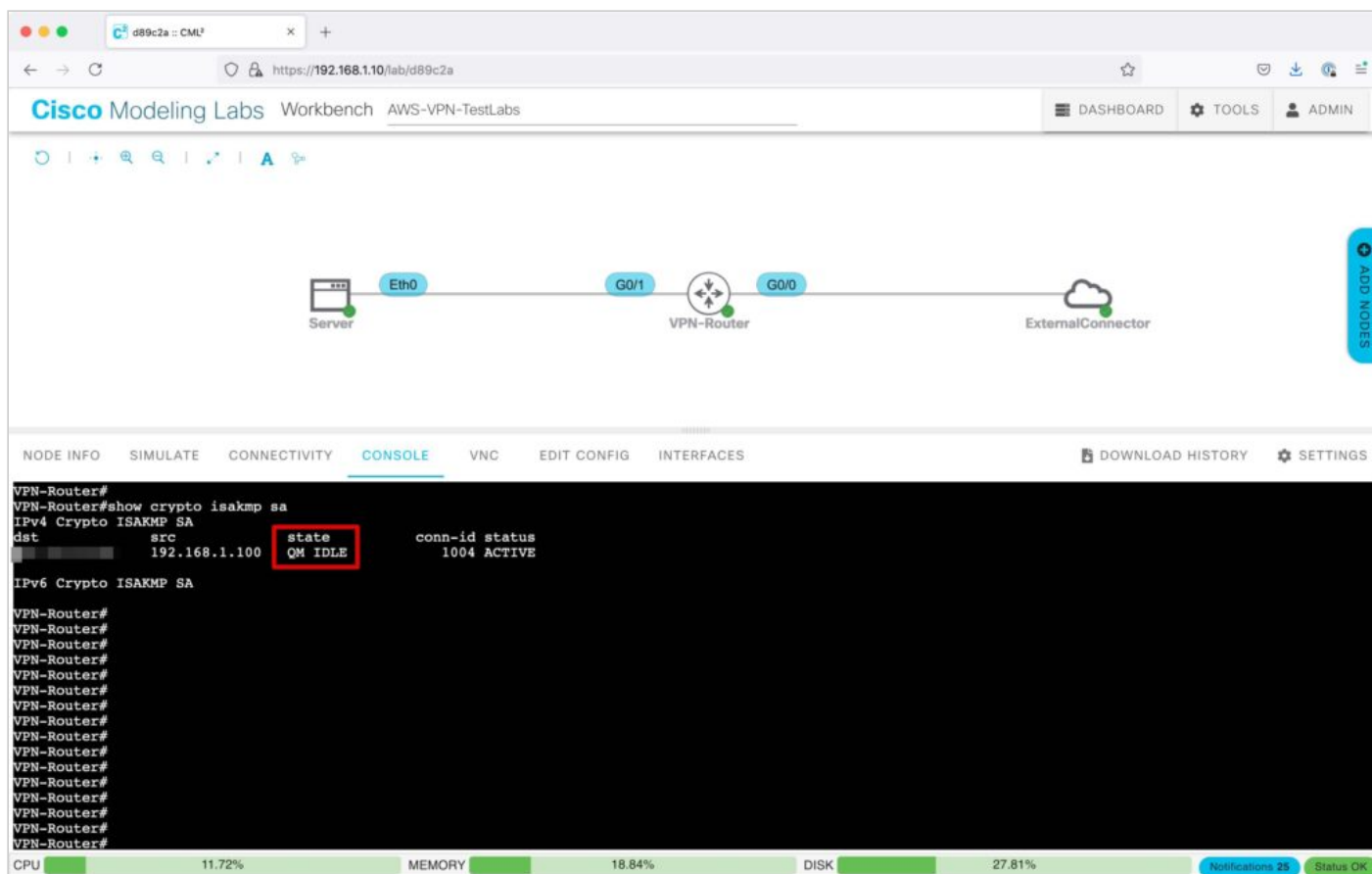
Tunnelインターフェースを一度シャットダウンし、VPNを再接続します。

```
interface Tunnel1
shutdown
no shutdown
```

フェーズ1(ISAKMP)のステータスを確認します。

stateが"QM IDLE"となっていれば、フェーズ1は成功しています。

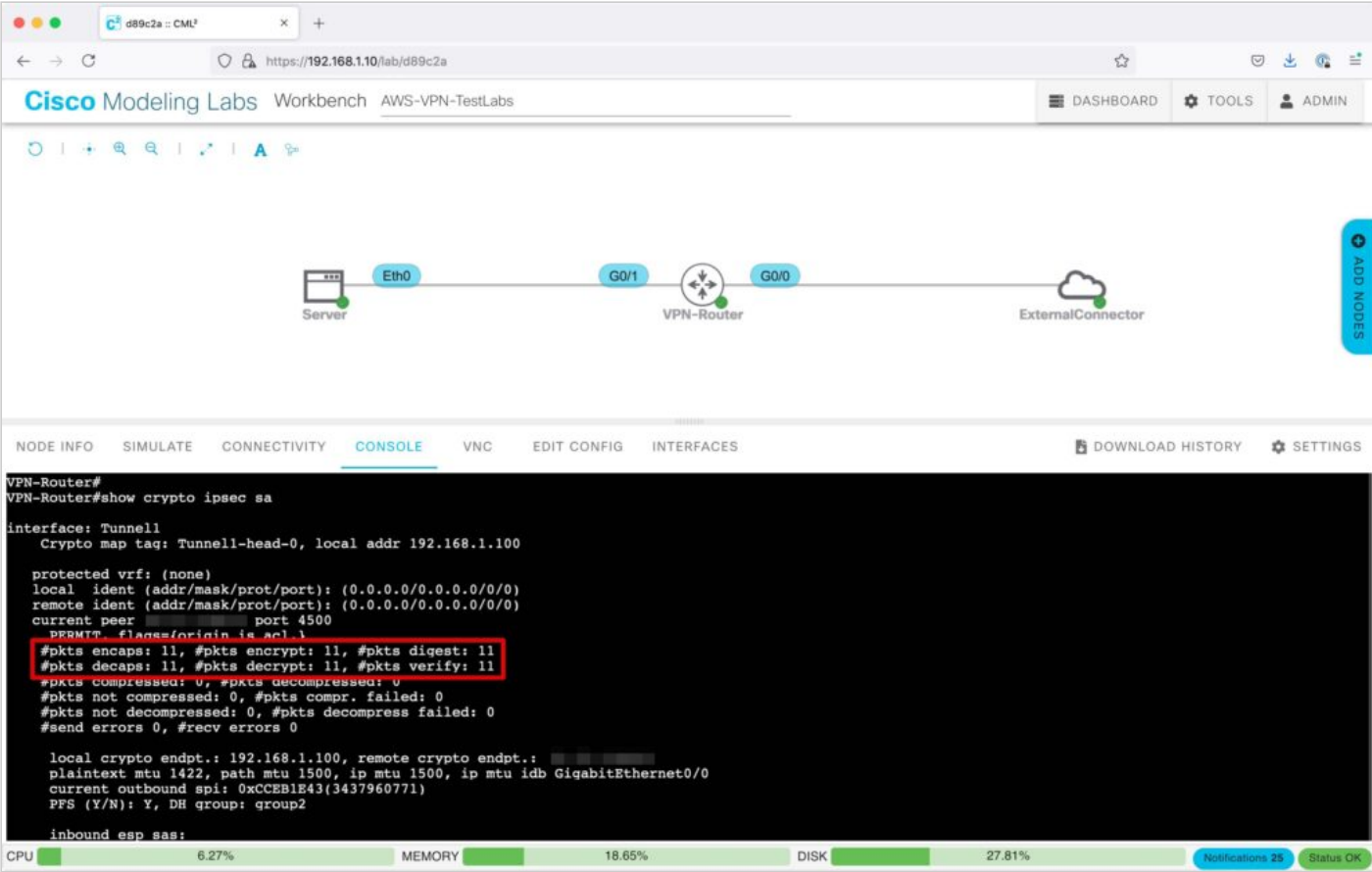
```
show crypto isakmp sa
```



フェーズ2(IPSec)のステータスを確認を確認します。

“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
```



## パケットキャプチャ確認

暗号化・ハッシュアルゴリズムが、“128bit”と“256bit”の場合の実際のパケットを比べてみます。  
“256bit”の方が、暗号化ペイロードが大きくなるため、パケット長(Length)が長くなっています。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.100	ISAKMP	206	Identity Protection (Main Mode)
2	0.116337	192.168.1.100	192.168.1.100	ISAKMP	178	Identity Protection (Main Mode)
3	0.134323	192.168.1.100	192.168.1.100	ISAKMP	326	Identity Protection (Main Mode)
4	0.143017	192.168.1.100	192.168.1.100	ISAKMP	286	Identity Protection (Main Mode)
5	0.172396	192.168.1.100	192.168.1.100	ISAKMP	154	Identity Protection (Main Mode)
6	0.180337	192.168.1.100	192.168.1.100	ISAKMP	122	Identity Protection (Main Mode)
7	0.199051	192.168.1.100	192.168.1.100	ISAKMP	362	Quick Mode
8	0.207683	192.168.1.100	192.168.1.100	ISAKMP	378	Quick Mode
9	0.281023	192.168.1.100	192.168.1.100	ISAKMP	106	Quick Mode
14	20.793054	192.168.1.100	192.168.1.100	ESP	174	ESP (SPI=0xcda29c19)
15	20.802031	192.168.1.100	192.168.1.100	ESP	174	ESP (SPI=0x4092ae41)
16	21.793485	192.168.1.100	192.168.1.100	ESP	174	ESP (SPI=0xcda29c19)
17	21.802640	192.168.1.100	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: [redacted]

▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: [redacted]

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

▼ Internet Security Association and Key Management Protocol

Initiator SPI: 3519579e596a18c3

Responder SPI: 0000000000000000

Next payload: Security Association (1)

▶ Version: 1.0

Exchange type: Identity Protection (Main Mode) (2)

▶ Flags: 0x00

Message ID: 0x00000000

Length: 164

▶ Payload: Security Association (1)

▶ Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE

▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07

▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03

▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n

128bitの場合(画像クリックで拡大)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100		ISAKMP	206	Identity Protection (Main Mode)
2	0.111070		192.168.1.100	ISAKMP	178	Identity Protection (Main Mode)
3	0.125576	192.168.1.100		ISAKMP	350	Identity Protection (Main Mode)
4	0.135436		192.168.1.100	ISAKMP	310	Identity Protection (Main Mode)
5	0.158495	192.168.1.100		ISAKMP	154	Identity Protection (Main Mode)
6	0.167033		192.168.1.100	ISAKMP	138	Identity Protection (Main Mode)
7	0.185076	192.168.1.100		ISAKMP	378	Quick Mode
8	0.193377		192.168.1.100	ISAKMP	394	Quick Mode
9	0.246780	192.168.1.100		ISAKMP	122	Quick Mode
18	44.079085	192.168.1.100		ESP	178	ESP (SPI=0xc2dbb0e3)
19	44.086423		192.168.1.100	ESP	178	ESP (SPI=0x03b79f86)
20	45.077435	192.168.1.100		ESP	178	ESP (SPI=0xc2dbb0e3)
21	45.091074		192.168.1.100	ESP	178	ESP (SPI=0x03b79f86)

▶ 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  
     Initiator SPI: 9193293af5a8dbda  
     Responder SPI: 0000000000000000  
     Next payload: Security Association (1)  
     ▶ Version: 1.0  
     Exchange type: Identity Protection (Main Mode) (2)  
     ▶ Flags: 0x00  
     Message ID: 0x00000000  
     Length: 164  
     ▶ Payload: Security Association (1)  
     ▶ Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE  
     ▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07  
     ▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03  
     ▶ Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n

256bitの場合(画像クリックで拡大)

これで、AWSサイト間VPN接続の暗号化・ハッシュアルゴリズム変更は完了です！