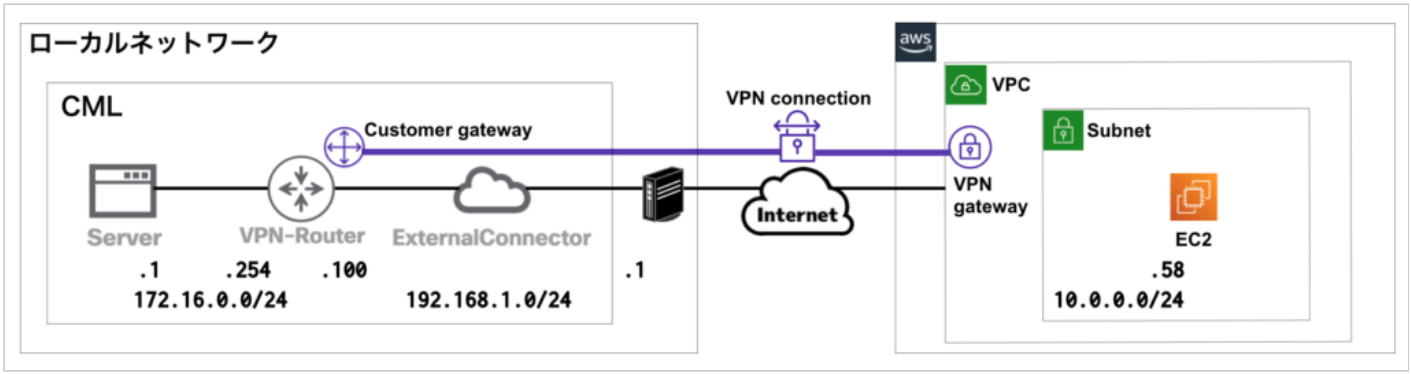
AWSサイト間VPNの構築（5.暗号化・ハッシュアルゴリズム変更）

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

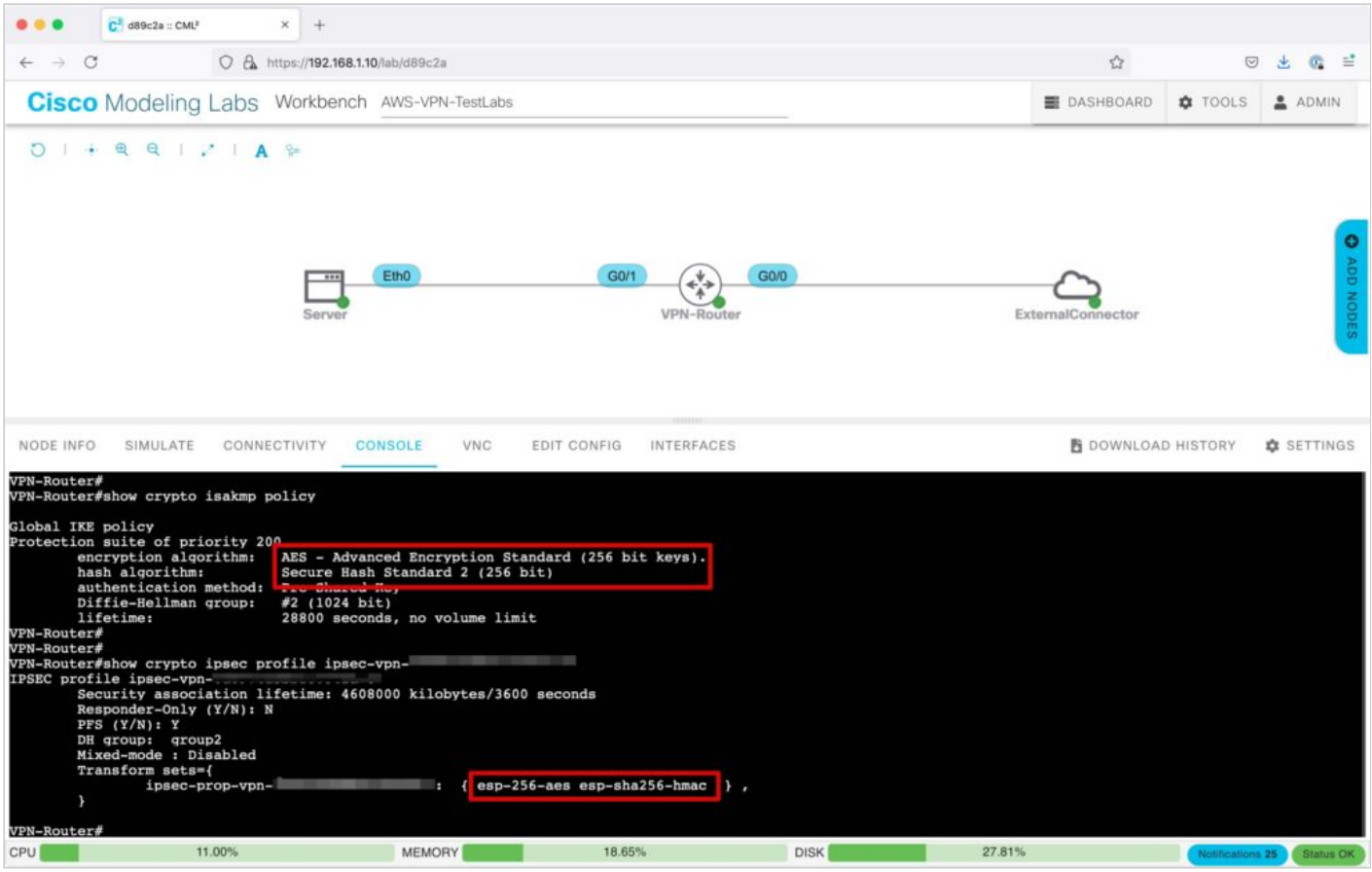
AWSの設定サンプルでは、セキュリティ強度が弱いため、下記の通りルーターの設定を変更します。

```
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
```



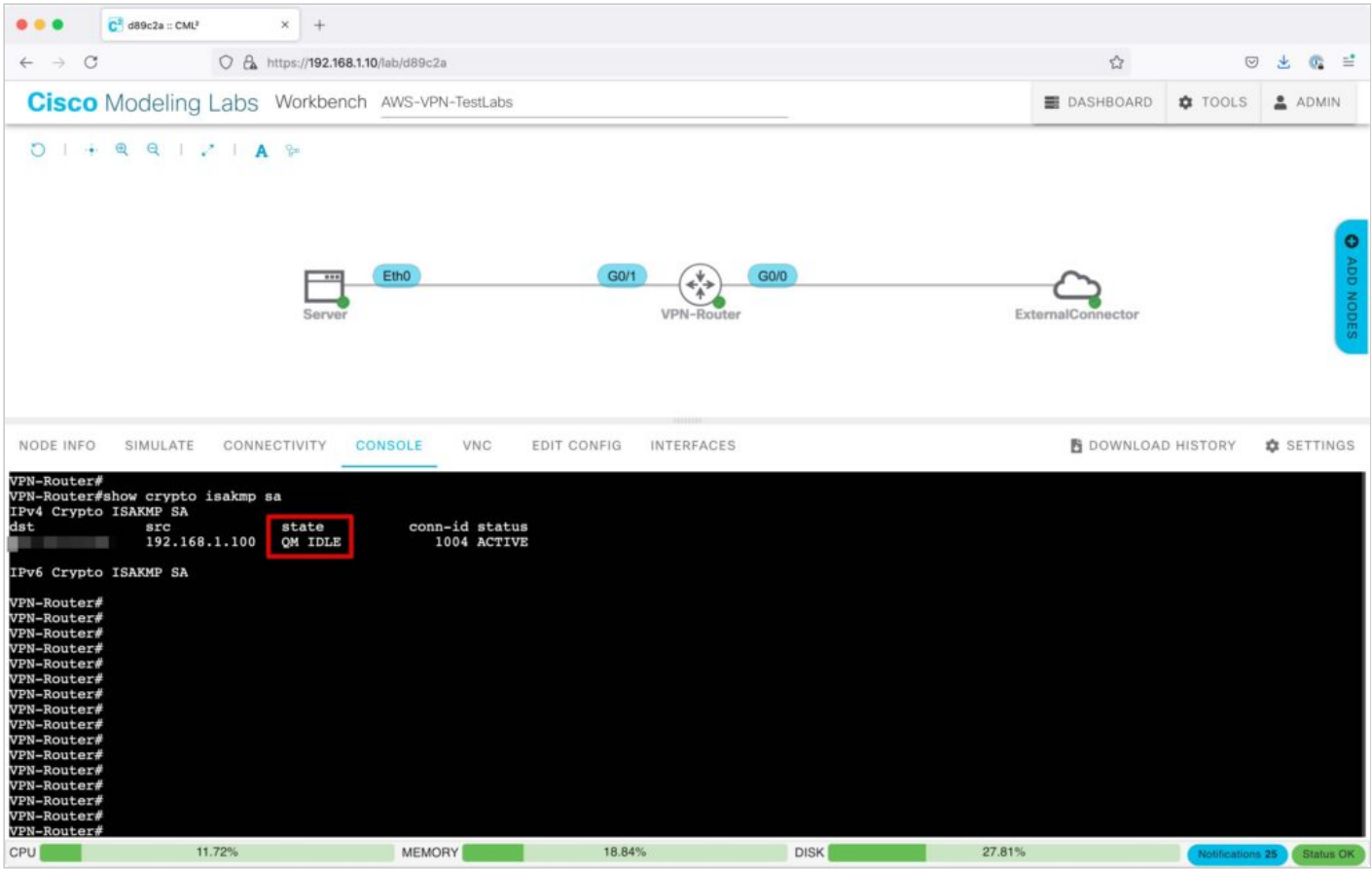
VPN接続確認

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
```

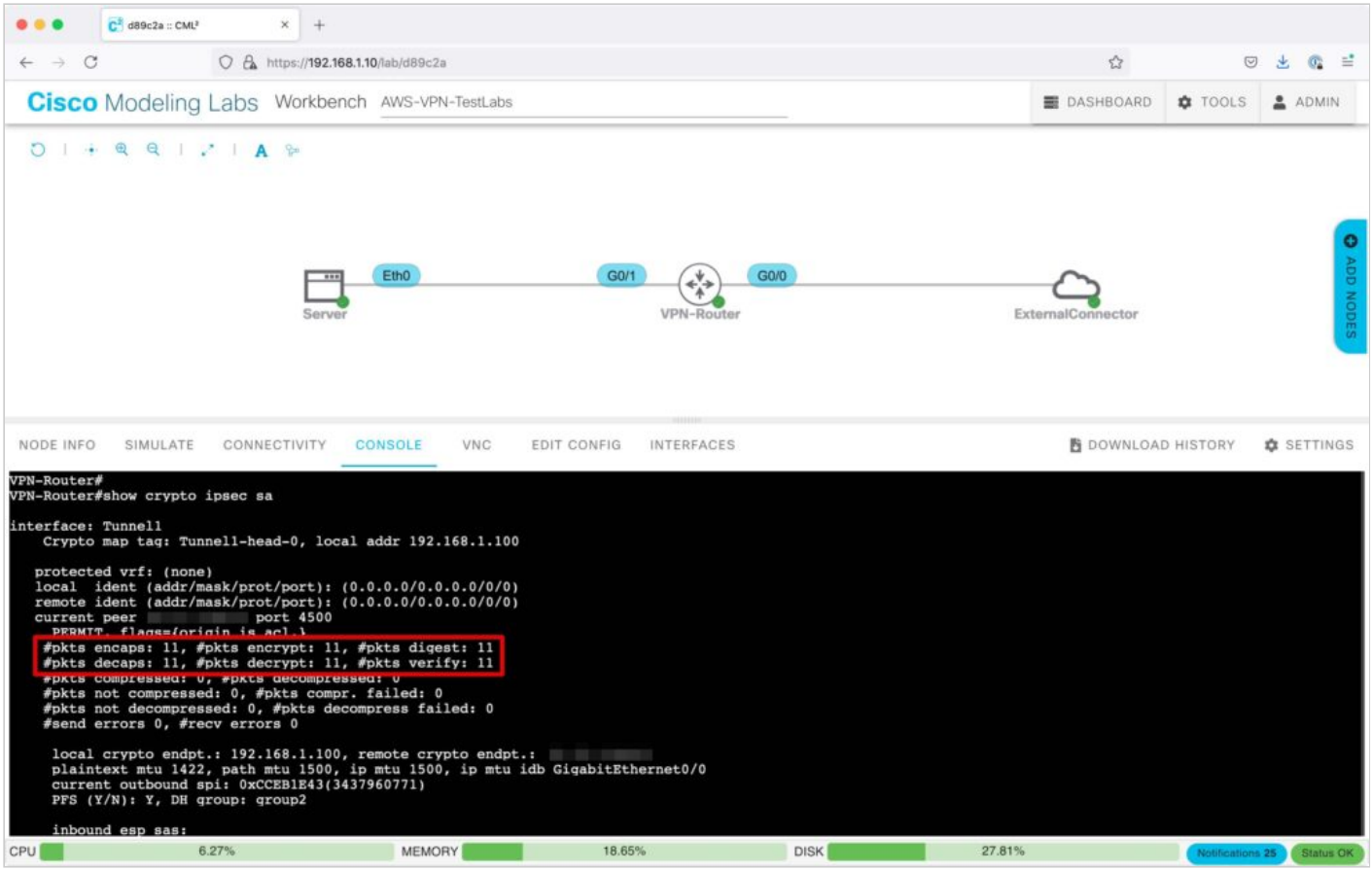
フェーズ1(ISAKMP)のステータスを確認します。
stateが”QM IDLE”となっていれば、フェーズ1は成功しています。

```
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。

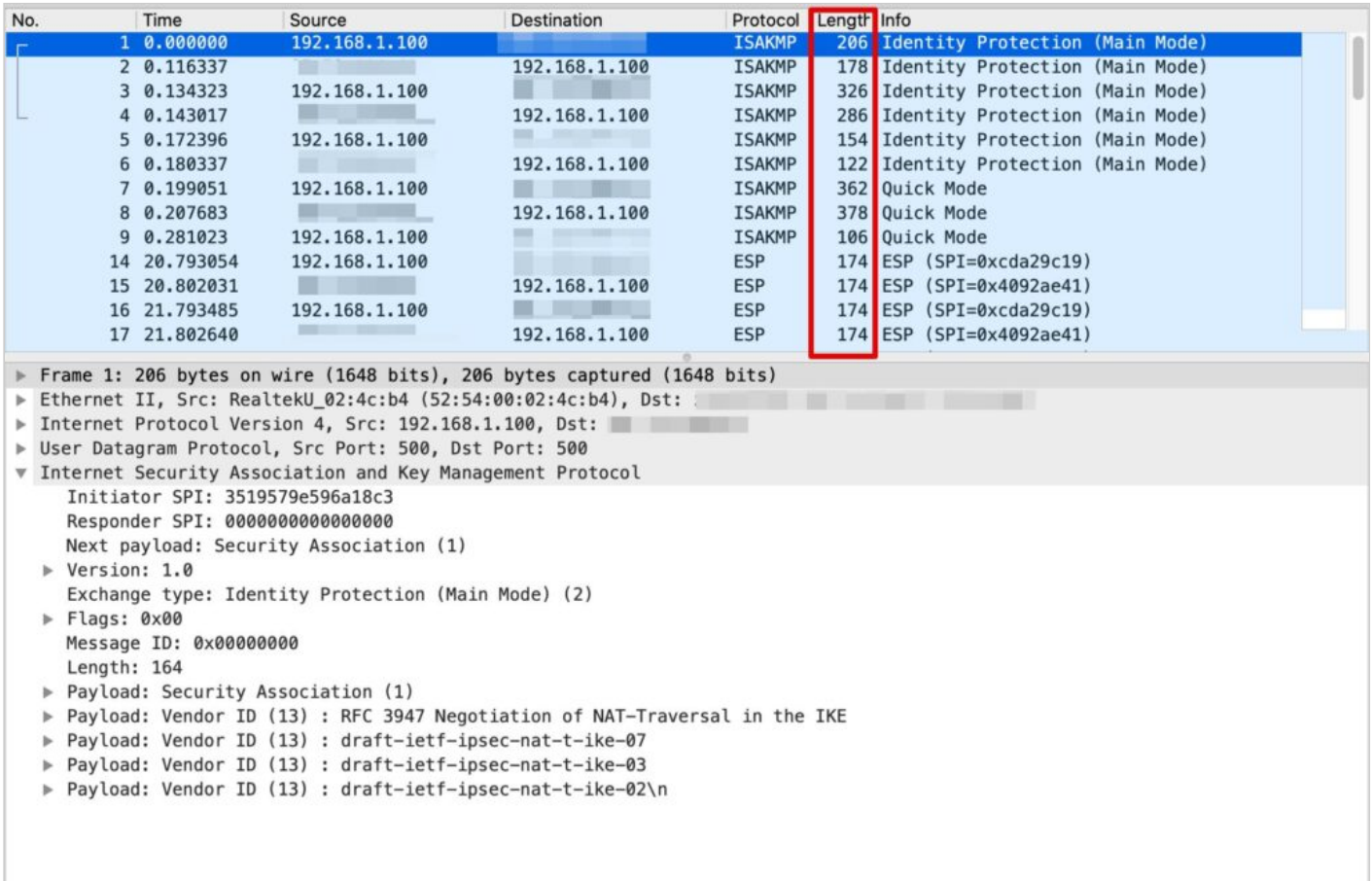
```
show crypto ipsec sa
```



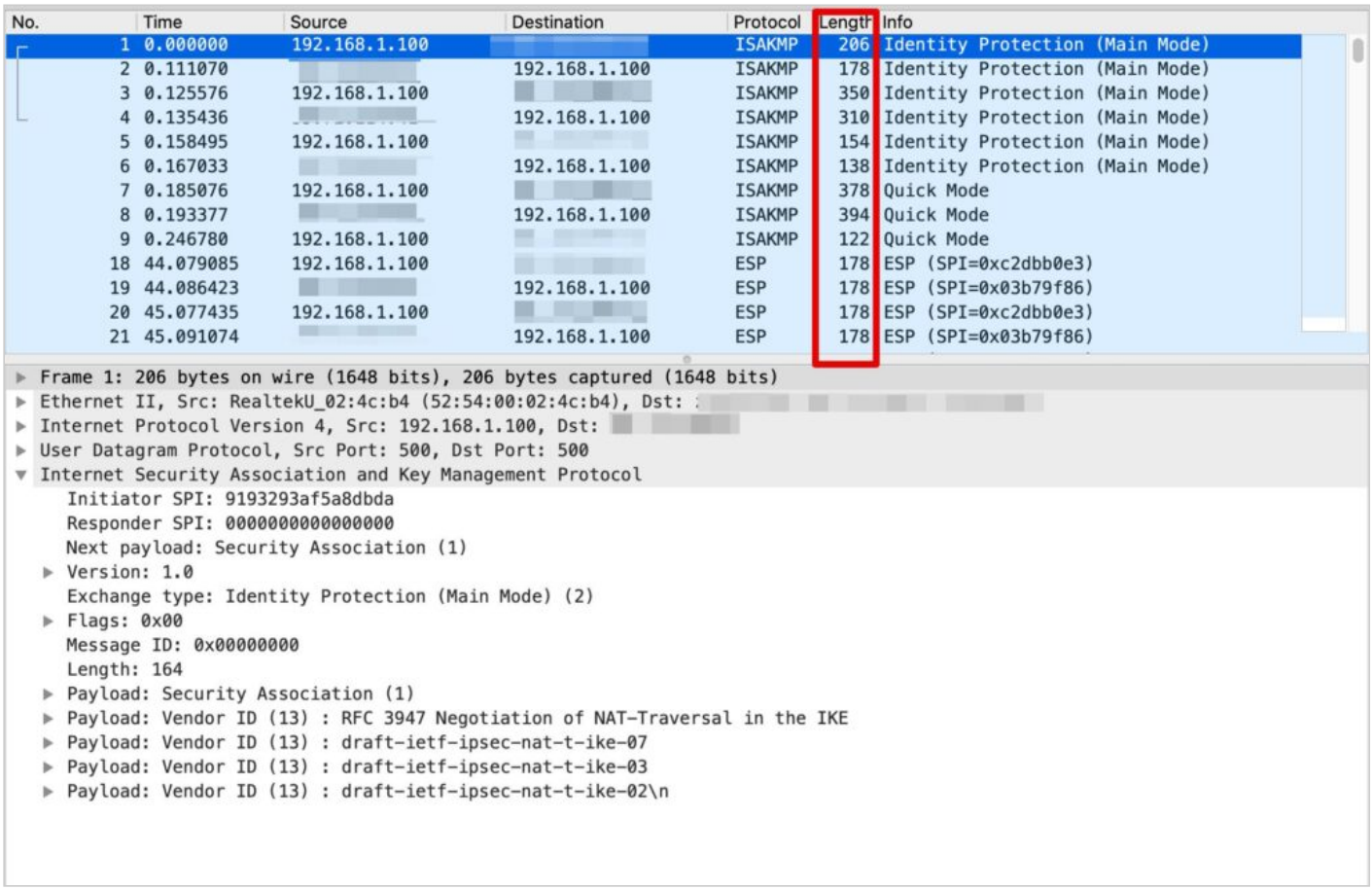
パケットキャプチャ確認

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。



128bitの場合(画像クリックで拡大)



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！