

# AWSサイト間VPNの構築（6.IKEv2の設定）

AWS



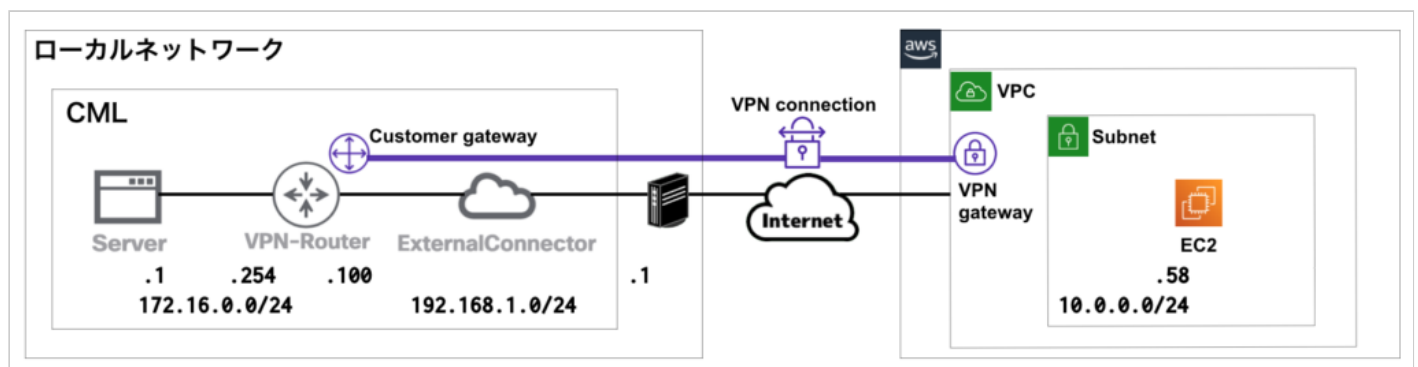
## AWSサイト間VPNの構築 （6.IKEv2の設定）

2021.09.20 2021.08.16

[【前回】 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）](#)[【次回】 AWSサイト間VPNの構築（7.AWS CLI によるVPN接続の作成）](#)

## ネットワーク構成

前回は、下記の構成でAWSのサイト間VPNを構築し、暗号化アルゴリズムとハッシュアルゴリズムを"128bit"から"256bit"に変更しました。今回は、"IKEv1"から"IKEv2"へ変更します。



## IKEv2の設定

### AWSのIKEv2への対応状況

AWSサイト間VPNは、2019年2月にIKEv2に対応しています。

[AWS サイト間 VPN が IKEv2 に対応](#)

VPN接続の作成時にトンネルの詳細オプションを確認すると、デフォルトで"IKEv1"と"IKEv2"の双方に対応していることが分かります。

トンネル 1 の詳細オプション ☐ デフォルトオプションを使用  
☒ トンネル 1 オプションを編集

フェーズ 1 暗号化アルゴリズム ☒ AES128 ☒ AES256 ☒ AES128-GCM-16 ☒ AES256-GCM-16

フェーズ 2 暗号化アルゴリズム ☒ AES128 ☒ AES256 ☒ AES128-GCM-16 ☒ AES256-GCM-16

フェーズ 1 整合性アルゴリズム ☒ SHA1 ☒ SHA2-256 ☒ SHA2-384 ☒ SHA2-512

フェーズ 2 整合性アルゴリズム ☒ SHA1 ☒ SHA2-256 ☒ SHA2-384 ☒ SHA2-512

フェーズ 1 DH グループ番号 ☒ 2 ☒ 14 ☒ 15 ☒ 16 ☒ 17 ☒ 18 ☒ 19 ☒ 20 ☒ 21 ☒ 22 ☒ 23 ☒ 24

フェーズ 2 DH グループ番号 ☒ 2 ☒ 5 ☒ 14 ☒ 15 ☒ 16 ☒ 17 ☒ 18 ☒ 19 ☒ 20 ☒ 21 ☒ 22 ☒ 23 ☒ 24

IkeVersion ☒ ikev1 ☒ ikev2

## ルーターの設定変更

下記の通り、IKEv2のパラメーターを設定します。

\*の部分はダウンロードしたテンプレートから事前共有キー (Pre-Shared Key) を設定します。

```
crypto ikev2 proposal IKEV2-PROP
  encryption aes-cbc-256
  integrity sha256
  group 2
```

```
crypto ikev2 policy IKEV2-POL
  proposal IKEV2-PROP
```

```
crypto ikev2 keyring IKEV2-KEY
  peer peer1
    address XXX.XXX.XXX.XXX ※ここはAWS側のグローバルアドレスを指定
    pre-shared-key local *****
    pre-shared-key remote *****
```

```
crypto ikev2 profile IKEV2-PROF
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local IKEV2-KEY
```

```
lifetime 21600

crypto ipsec transform-set IPSEC esp-aes 256 esp-sha256-hmac
mode tunnel

crypto ipsec profile IPSEC-PROFILE
set transform-set IPSEC
set pfs group2
set ikev2-profile IKEV2-PROF

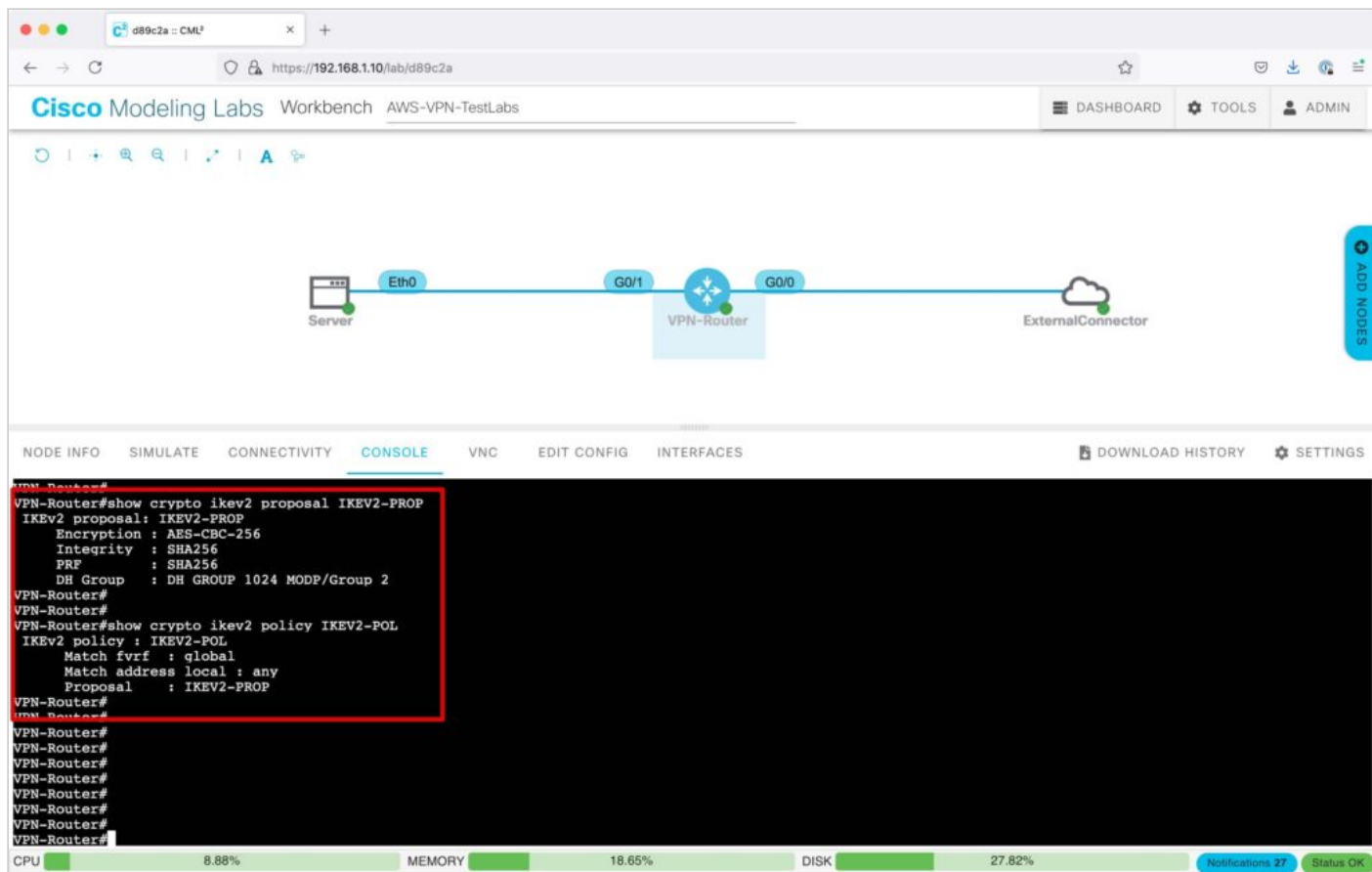
interface Tunnel1
ip address 169.254.27.178 255.255.255.252
ip virtual-reassembly in
ip tcp adjust-mss 1379
tunnel source 192.168.1.100 ※ここはCML上のルーターのGi0/0のアドレスを指定
tunnel mode ipsec ipv4
tunnel destination XXX.XXX.XXX.XXX ※ここはAWS側のグローバルアドレスを指定
tunnel protection ipsec profile IPSEC-PROFILE

ip route 10.0.0.0 255.255.255.0 Tunnel1
```

## IKEv2の設定確認

IKEv2の設定を確認します。

```
show crypto ikev2 proposal IKEV2-PROP
show crypto ikev2 policy IKEV2-POL
```



The screenshot displays the Cisco Modeling Labs Workbench interface for a VPN configuration. The topology shows a Server connected to a VPN-Router via Ethernet0, and the VPN-Router connected to an ExternalConnector via GigabitEthernet0/1 and GigabitEthernet0/0. The console window shows the configuration of IKEv2 proposal and policy.

```
VPN-Router#  
VPN-Router#show crypto ikev2 proposal IKEV2-PROP  
IKEv2 proposal: IKEV2-PROP  
Encryption : AES-CBC-256  
Integrity : SHA256  
PRF : SHA256  
DH Group : DH GROUP 1024 MODP/Group 2  
VPN-Router#  
VPN-Router#show crypto ikev2 policy IKEV2-POL  
IKEv2 policy : IKEV2-POL  
Match fvrfl : global  
Match address local : any  
Proposal : IKEV2-PROP  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#  
VPN-Router#
```

At the bottom, system resource usage is shown: CPU 8.88%, MEMORY 18.65%, DISK 27.82%. There are 27 notifications and the status is OK.

## 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 'Cisco Modeling Labs Workbench' and 'AWS-VPN-TestLabs'. 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 on the 'cisco@Server' node. The terminal shows a successful ping from the server to 10.0.0.58. At the bottom, a status bar shows CPU at 6.28%, MEMORY at 18.65%, and DISK at 27.81%.

```
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=16.659 ms
64 bytes from 10.0.0.58: seq=1 ttl=253 time=14.736 ms
64 bytes from 10.0.0.58: seq=2 ttl=253 time=18.950 ms
64 bytes from 10.0.0.58: seq=3 ttl=253 time=19.105 ms
64 bytes from 10.0.0.58: seq=4 ttl=253 time=16.721 ms
64 bytes from 10.0.0.58: seq=5 ttl=253 time=15.276 ms
64 bytes from 10.0.0.58: seq=6 ttl=253 time=15.456 ms
64 bytes from 10.0.0.58: seq=7 ttl=253 time=14.127 ms
64 bytes from 10.0.0.58: seq=8 ttl=253 time=21.642 ms
64 bytes from 10.0.0.58: seq=9 ttl=253 time=16.753 ms
^C
--- 10.0.0.58 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 14.127/16.942/21.642 ms
cisco@Server:~$
```

## ルーターのステータス確認

IKEv2のステータスを確認します。

Statusが"READY"となっていれば、IKEv2は確立されています。

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 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 on the 'VPN-Router' node. The terminal shows the output of the command 'show crypto ikev2 sa', indicating that the IKEv2 status is 'READY'. At the bottom, a status bar shows CPU at 12.13%, MEMORY at 18.65%, and DISK at 27.81%.

```
VPN-Router# show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvr/fivr Status
2 192.168.1.100/4500 /4500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 21600/2521 sec

IPv6 Crypto IKEv2 SA

VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
VPN-Router#
```

IPSecのステータスを確認します。

“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。

The screenshot displays the Cisco Modeling Labs Workbench interface. At the top, there's a navigation bar with 'DASHBOARD', 'TOOLS', and 'ADMIN' tabs. 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 main area is the 'CONSOLE' tab, showing the command prompt for the 'VPN-Router'. The command 'show crypto ipsec sa' has been executed, and the output is displayed. The output shows details for the 'Tunnell' interface, including the 'Crypto map tag: Tunnell-head-0, local addr 192.168.1.100'. The output is as follows:

```
VPN-Router#
VPN-Router#
VPN-Router#show crypto ipsec sa
interface: Tunnell
  Crypto map tag: Tunnell-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 in acl)
  #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
  #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: 0xC6E75909(3337050377)
  PFS (Y/N): N, DH group: none
```

At the bottom of the console, there are status bars for CPU (6.22%), MEMORY (18.65%), and DISK (27.81%). There are also buttons for 'Notifications 27' and 'Status OK'.

## パケットキャプチャ確認

IKEv1と比較して、少ないやりとりでフェーズ1が完了していることが分かります。

IKE\_SA\_INITでは、UDPの500番ポートを利用しています。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100		ISAKMP	432	IKE_SA_INIT MID=00 Initiator Request
2	0.009888		192.168.1.100	ISAKMP	354	IKE_SA_INIT MID=00 Responder Response
3	0.050445	192.168.1.100		ISAKMP	622	IKE_AUTH MID=01 Initiator Request
4	0.068141		192.168.1.100	ISAKMP	270	IKE_AUTH MID=01 Responder Response
5	81.250494	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
6	81.258155		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
7	81.264838	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
8	81.272116		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
9	81.285075	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
10	81.292334		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
11	81.300456	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
12	81.307196		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)

▶ Frame 1: 432 bytes on wire (3456 bits), 432 bytes captured (3456 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: cd5067fbel3ac8fb  
Responder SPI: 0000000000000000  
Next payload: Security Association (33)

▶ Version: 2.0

Exchange type: IKE\_SA\_INIT (34)

▶ Flags: 0x08 (Initiator, No higher version, Request)  
Message ID: 0x00000000  
Length: 390

▶ Payload: Security Association (33)  
▶ Payload: Key Exchange (34)  
▶ Payload: Nonce (40)  
▶ Payload: Vendor ID (43) : Cisco Delete Reason Supported  
▶ Payload: Vendor ID (43) : Unknown Vendor ID  
▶ Payload: Vendor ID (43) : Unknown Vendor ID  
▶ Payload: Vendor ID (43) : Cisco FlexVPN Supported  
▶ Payload: Notify (41) - NAT\_DETECTION\_SOURCE\_IP  
▶ Payload: Notify (41) - NAT\_DETECTION\_DESTINATION\_IP

IKE\_AUTHでは、UDPの4500番ポートを利用しています。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100		ISAKMP	432	IKE_SA_INIT MID=00 Initiator Request
2	0.009888		192.168.1.100	ISAKMP	354	IKE_SA_INIT MID=00 Responder Response
3	0.050445	192.168.1.100		ISAKMP	622	IKE_AUTH MID=01 Initiator Request
4	0.068141		192.168.1.100	ISAKMP	270	IKE_AUTH MID=01 Responder Response
5	81.250494	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
6	81.258155		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
7	81.264838	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
8	81.272116		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
9	81.285075	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
10	81.292334		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)
11	81.300456	192.168.1.100		ESP	194	ESP (SPI=0xcb83e983)
12	81.307196		192.168.1.100	ESP	194	ESP (SPI=0x65e8707b)

▶ Frame 3: 622 bytes on wire (4976 bits), 622 bytes captured (4976 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

Initiator SPI: cd5067fbel3ac8fb  
Responder SPI: 87c9a9355ff55805  
Next payload: Encrypted and Authenticated (46)

▶ Version: 2.0

Exchange type: IKE\_AUTH (35)

▶ Flags: 0x08 (Initiator, No higher version, Request)  
Message ID: 0x00000001  
Length: 576

▶ Payload: Encrypted and Authenticated (46)

これで、AWSサイト間VPN接続のIKEv2への変更は完了です。