



Amazon VPC VPN 接続設定 参考資料

2015.04.16

目次

1. イントロダクション	3
1.1. 用語集.....	3
1.2. 目的	3
1.3. AWS が提供する VPN 接続.....	3
2. 事前準備	4
2.1. オンプレミス側ルータ(Customer Gateway)の準備.....	4
2.2. 設定用パラメータの準備.....	5
3. 設定手順	6
3.1. AWS マネージメントコンソールの設定.....	7
3.1.1. VPC およびサブネットの作成	8
3.1.2. <i>Virtual Private Gateway</i> の設定	10
3.1.3. <i>VPN Connection</i> の作成.....	11
3.1.4. <i>Customer Gateway</i> コンフィグレーションファイルのダウンロード.....	12
3.1.5. サブネットのルーティング設定	13
3.2. <i>Customer Gateway</i> の設定	15
3.2.1. <i>IKE</i> の設定	15
3.2.2. <i>IPsec</i> の設定.....	17
3.2.3. <i>Tunnel</i> インタフェースの設定	19
3.2.4. ルーティング設定	20
3.3. 動作確認.....	21
4. 参考情報	22

1. イントロダクション

1.1. 用語集

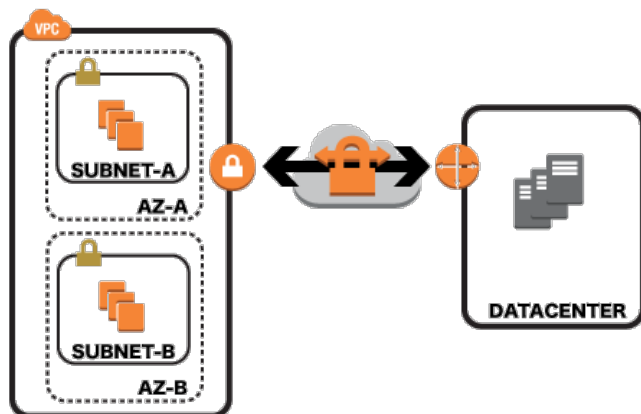
用語	説明
VPN(Virtual Private Network)	インターネット回線上に、暗号化技術を利用して専用の経路を確立する技術
Amazon VPC(Virtual Private Cloud)	AWS 上に論理的な領域を定義し、仮想ネットワークを作成することができるサービス
Customer Gateway	オンプレミスのネットワークに設置されているお客様ルータ
VGW(Virtual Private Gateway)	AWS 上で作成される仮想ルータ

1.2. 目的

本書は Amazon Web Services をご利用のお客様で、Amazon VPC(Virtual Private Cloud)とデータセンター・オフィスなどのオンプレミス拠点を VPN(Virtual Private Network) 接続するための手順について記述しています。

1.3. AWS が提供する VPN 接続

Amazon VPC の機能で提供している VPN はサイト間 VPN となります。オンプレミス環境に設置されているハードウェアルータと Amazon 側の Virtual Private Gateway 間は、インターネット経由で暗号化された通信路を確立し、拠点間通信を行います。



2. 事前準備

VPN 接続の前に、ルータ、設定パラメータの準備が必要となります。

2.1. オンプレミス側ルータ(Customer Gateway)の準備

オンプレミス側の VPN エンドポイントとなるルータ(以下、Customer Gateway)は以下の機能を利用できる必要があります。AWS で検証済のルーター一覧も以下のリンクに掲載しておりますのでご参考ください。掲載されていないルータでも、要件を満たしていればご利用いただけます。

検証済ルーター一覧 : <https://aws.amazon.com/jp/vpc/faqs/#C9>

■以下の IPsec 通信設定が可能であること

設定項目	内容
IKE (フェーズ 1) : モード	メインモード
IKE (フェーズ 1) : 暗号アルゴリズム	AES 128-bit
IKE (フェーズ 1) : 認証方式	Pre-Shared Key
IKE (フェーズ 1) : ハッシュアルゴリズム	SHA-1
IKE (フェーズ 1) : DH グループ	グループ 2
IKE (フェーズ 1) : lifetime	28800 秒
IPsec (フェーズ 2) : モード	トンネルモード
IPsec (フェーズ 2) : 暗号アルゴリズム	AES 128-bit
IPsec (フェーズ 2) : 認証アルゴリズム	HMAC
IPsec (フェーズ 2) : ハッシュアルゴリズム	SHA-1
IPsec (フェーズ 2) : PFS グループ	グループ 2
IPsec (フェーズ 2) : lifetime	3600 秒

■暗号化処理前にフラグメント可能であること。

■論理トンネルインタフェースが作成できること。

■インターネットと直接通信可能なパブリック IP が利用できること。

NAT を利用した IPsec 通信 (NAT トラバーサル) はサポート対象外となりますのでご注意ください。

■BGP(Border Gateway Protocol)が利用できること（オプション）

Static ルートでの設定も可能ですが、BGP を利用すると障害時の経路自動変更やルーティングテーブルの動的更新などがルーティングプロトコルでサポートされているため、複雑な構成の場合は BGP のご利用をお勧めします。

■IPSec Dead Peer Detection が利用できること。（オプション）

2.2. 設定用パラメータの準備

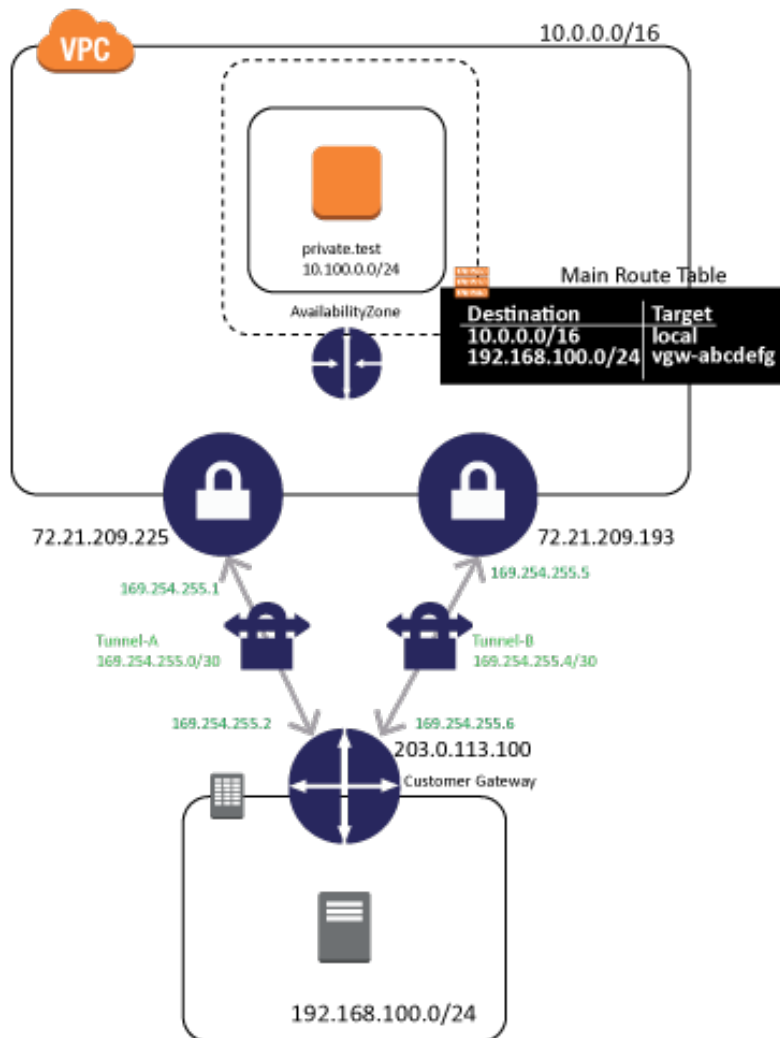
VPN 設定にあたり、お客様側で以下のパラメータをご用意いただく必要があります。

項目	内容
Customer Gateway 側 VPN エンドポイント IP アドレス	インターネットに直接通信可能な IP アドレスをご用意ください。
オンプレミス側 AS 番号(BGP の場合)	プライベート AS 64512~65534 をご利用ください。
オンプレミス側ネットワークアドレス	VPC と通信したいオンプレミスのネットワークを環境に合わせて設定してください。

3. 設定手順

具体的な設定を元に手順について記載します。

説明で利用する構成は、1 台の Customer Gateway から VPC へ接続する一般的な構成とします。



本ドキュメントで利用する設定情報はこちらです。お客様にご準備いただいた設定以外に、AWS から割当てられる設定があります。

項目	内容	補足
AWS 側 VPN エンドポイント #A	72.21.209.225	AWS から割り当てられるものです。変更はできません。また、こちらのアドレスはサンプルであり、実際の環境では異なる IP アドレスとなる場合があります。
AWS 側 VPN エンドポイント #B	72.21.209.193	
Customer Gateway 側	203.0.113.100	実際の環境ではお客様にてご用意いただきます。
トンネル A ネットワークアドレス	169.254.255.0/30	AWS から割り当てられるものです。変更はできません。また、こちらのアドレスはサンプルであり、実際の環境では異なる IP アドレスとなる場合があります。
AWS 側トンネル A アドレス	169.254.255.1	
Customer Gateway 側 トンネル A アドレス	169.264.255.2	
トンネル B ネットワークアドレス	169.254.255.4/30	
AWS 側トンネル B アドレス	169.254.255.5	
Customer Gateway 側 トンネル B アドレス	169.254.255.6	
オンプレミス側 AS 番号	65001	お客様側でプライベート AS 64512~65534 をご利用ください。
オンプレミス側 ネットワークアドレス	192.168.10.0/24	実際の環境ではお客様にてご用意いただきます。

3.1. AWS マネージメントコンソールの設定

AWS マネージメントコンソールでは、以下の順序で設定を行います。

①VPC、サブネットの作成

通信したい AWS のリソースが稼働するためのネットワークを作成します。

②VGW(Virtual Gateway)の設定

AWS 側での VPN エンドポイントとなる Virtual Gateway を作成し、利用したい VPC へのアタッチを行います。

③ オンプレミス側のルータ (Customer Gateway) の登録

オンプレミス側の VPN エンドポイントとなる Customer Gateway の設定を行います。本解説ではシスコシステムズ社のルータを設定例として取り上げます。

④ VPN Connection の作成

①、②で設定したそれぞれの VPN エンドポイント間の VPN 接続を設定します。

⑤ サブネットのルーティングテーブル設定

オンプレミスに対するトラフィックが VGW を経由するように、サブネットで利用しているルーティングテーブルを設定します。

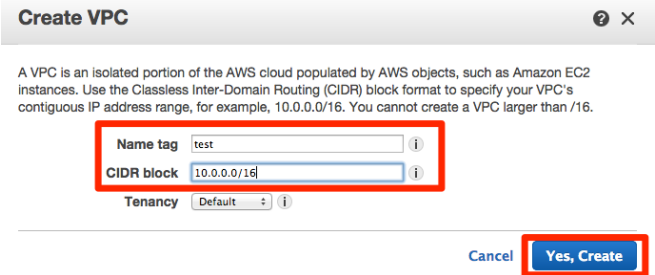
それぞれの手順について解説します。

3.1.1. VPC およびサブネットの作成

マネージメントから、[Services]-[VPC]を選択し、“VPC Dashboard”を開きます。メイン画面の“Create VPC”を選択します。



“Create VPC”画面で、“Name tag”に VPC 名、“CIDR block”に VPC で利用するネットワークアドレスを入力してください。このネットワークアドレスの中からサブネットを切り出していくことになるため、大きめのネットワークで設定することをおすすめします。また、作成後の変更はできません。



リストに作成された VPC が表示されます。

<input type="checkbox"/>	Name	VPC ID	State	VPC CIDR	DH
<input type="checkbox"/>	DEFAULT	vpc-████████	available	172.31.0.0/16	do
<input checked="" type="checkbox"/>	test	vpc-████████	available	10.0.0.0/16	dc

次に、サブネットの作成をします。“VPC Dashboard”のメニューから“Subnets”をクリックします。次に、“Create Subnet”ボタンをクリックします。



“Create subnet”画面で、
 “Name tag”に VPC 名、
 “VPC”のプルダウンメニューから該当の VPC を選択、
 “Availability Zone”を指定する場合はプルダウンメニューから選択、
 “CIDR block”にサブネットで利用するネットワークアドレス(VPC で指定したアドレスの範囲内である必要があります。)
 を入力し、“Yes, Create”をクリックします。

Create Subnet ? X

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag ⓘ

VPC ⓘ

Availability Zone ⓘ

CIDR block ⓘ

Cancel Yes, Create

リストに作成されたサブネットが表示されます。

<input checked="" type="checkbox"/>	private.test	subnet-████████	available	vpc-████████ (10.0.0.0/16) ..
<input type="checkbox"/>	DEFAULT	subnet-████████	available	vpc-████████ (172.31.0.0/16...
<input type="checkbox"/>	DEFAULT	subnet-████████	available	vpc-████████ (172.31.0.0/16...

3.1.2. Virtual Private Gateway の設定

マネージメントコンソールから、[Services]-[VPC]を選択し、左メニューの“VPC Connection”にある“Virtual Private Gateway”をクリックし、メイン画面の“Create Virtual Private Gateway”のボタンをクリックします。

Create Virtual Private Gateway

“Create Virtual Private Gateway”の画面で“Name tag”に VGW 名を入力し、“Yes, Create”をクリックします。

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

Cancel **Yes, Create**

リストに作成した VGW が表示されます。作成した VGW を選択し、“Attach to VPC”をクリックします。

Create Virtual Private Gateway Delete Virtual Private Gateway **Attach to VPC** Detach from VPC

Search Virtual Private Gateways an X < > 1 to 3 of 3 Virtual Private G

<input type="checkbox"/>	Name	ID	State	Type
<input checked="" type="checkbox"/>	vgw.test	vgw-██████████	detached	ipsec.1

“Attach to VPC”の画面で“VPC”のプルダウンから利用したい VPC を選択し、“Yes, Attach”をクリックします。

Select the VPC to attach to the virtual private gateway

VPC

Cancel **Yes, Attach**

リスト中で、VGW の Status 欄を確認してください。操作直後は“attaching”ですが、“attached”になったら完了です。

	vgw.test	vgw-██████████	attaching
--	----------	----------------	------------------

↓



3.1.3. VPN Connection の作成

マネージメントコンソールから、[Services]-[VPC]を選択し、左メニューの“VPC Connections”にある“VPN Connections”をクリックし、メイン画面の“Create VPN Connection”のボタンをクリックします。

ルーティング設定(BGP と Static)によって、設定画面が異なります。

<BGP の場合>

“Create VPN Connection”から、“Routing Options”に“Dynamic (Requires BGP)”にチェックを入れ、“Name tag”に VPN コネクション名、“Virtual Private Gateway”に前項で作成した VGW を選択、“Customer Gateway”で“New”にチェックを入れ、“IP Address”で Customer Gateway のパブリック IP アドレスを入力、“BGP ASN”に AS 番号を入力し、“Yes Create”をクリックします。

Create VPN Connection ⓘ ×

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag ⓘ

Virtual Private Gateway

Customer Gateway Existing New

IP Address ⓘ (e.g. 192.0.2.1)

BGP ASN ⓘ

Specify the routing for the VPN Connection ([Help me choose](#))

Routing Options Dynamic (requires BGP) Static

VPN connection charges apply once this step is complete. [View Rates](#)

<Static の場合>

“Create VPN Connection”から、“Routing Options”に“Static”にチェックを入れ、“Name tag”に VPN コネクション名、“Virtual Private Gateway”に前項で作成した VGW を選択、

“Customer Gateway”で“New”にチェックを入れ、
 “IP Address”で Customer Gateway のパブリック IP アドレスを入力、
 “Static IP Prefixes”にオンプレミスで利用しているネットワークアドレスを入力、
 “Yes Create”をクリックします。

リストに作成した VPN Connection が表示されます。

Name	VPN ID	State
vpnconn.test	vpn-██████████	available

3.1.4. Customer Gateway コンフィグレーションファイルのダウンロード

Customer Gateway で利用するコンフィグレーションはマネージメントコンソールからダウンロードすることが可能です。AWS 側の VPN エンドポイントの IP アドレスや IPsec の設定内容も記載されていますので、ご利用の機種に合ったコンフィグレーションファイルをダウンロードしてください。

VPN Connection の一覧の上にある“Download Configuration”をクリックします。

“Vendor”、“Platform”、“Software”からそれぞれの環境に合わせてコンフィギュレーションをダウンロードしてください。

Download Configuration

Please choose the configuration to download based on your type of customer gateway.

Vendor Cisco Systems, Inc. ⓘ

Platform ISR Series Routers ⓘ

Software IOS 12.4+ ⓘ

Cancel **Yes, Download**

3.1.5. サブネットのルーティング設定

マネージメントコンソールから、[Services]-[VPC]を選択し、左メニューの“Subnets”をクリックします。メイン画面のリストから作成したサブネットをクリックし、画面下のサブ画面の“Route Table”タブをクリックします。“Route Table:”の rtb- から始まるルートテーブル ID をクリックします。

The screenshot shows the AWS Management Console interface for configuring a subnet. At the top, there are buttons for "Create Subnet", "Delete Subnet", and "Modify Auto-Assign Public IP". Below this is a search bar and a table of subnets. The first row, "private.test", is highlighted with a red box. Below the table, the details for "subnet-9359b5e4 (10.0.0.0/24) | private.test" are shown. The "Route Table" tab is selected and highlighted with a red box. Below the tab, the "Route Table:" dropdown is set to "rtb-..." and highlighted with a red box. A table shows the route configuration:

Destination	Target
10.0.0.0/16	local

リストから該当のルートテーブルを選択し、画面下のサブ画面の“Routes”タブをクリックします。“Edit”をクリックします。

K < 1 to 1 of

<input type="checkbox"/>	Name	Route Table ID	Associated With	Main
<input checked="" type="checkbox"/>		rtb-	0 Subnets	Yes

rtb-27aa5242

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

“Destination”にオンプレミスのネットワークアドレス、“Target”に作成した VGW の ID を入力してください。（VGW の欄はカーソルを合わせると候補が表示されます。）その後、Save をクリックします。

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
192.168.10.0/24	vgw-	No		✖

完了後、ルーティングが登録されます。

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
192.168.10.0/24	vgw-	Active	No

3.2. Customer Gateway の設定

それぞれの項目毎の設定について記述します。こちらの設定は AWS documentation の“Amazon Virtual Private Cloud Network Administrator Guide”に記載しております。

<http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Cisco.html>

3.2.1. IKE の設定

VPN 接続における、フェーズ 1 IKE(インターネット鍵交換プロトコル)の設定を行います。

```
Tunnel #A
```

```
!  
crypto isakmp policy 200  
  encryption aes 128  
  authentication pre-share  
  group 2  
  lifetime 28800  
  hash sha  
exit  
!  
crypto keyring keyring-vpn-xxxxxxxx-0  
  pre-shared-key address 72.21.209.225 key plain-text-password1  
exit  
!  
crypto isakmp profile isakmp-vpn-xxxxxxxx-0  
  match identity address 72.21.209.225  
  keyring keyring-vpn-xxxxxxxx-0  
exit  
!
```

Tunnel #B

```
!  
crypto isakmp policy 201  
  encryption aes 128  
  authentication pre-share  
  group 2  
  lifetime 28800  
  hash sha  
exit  
!  
crypto keyring keyring-vpn-xxxxxxx-1  
  pre-shared-key address 72.21.209.193 key plain-text-password2  
exit  
!  
crypto isakmp profile isakmp-vpn-xxxxxxx-1  
  match identity address 72.21.209.193  
  keyring keyring-vpn-xxxxxxx-1  
exit  
!
```


3.2.2. IPsec の設定

次に、VPN 接続のフェーズ 2 IPsec の設定を行います。

Tunnel #A

```
!  
crypto ipsec transform-set ipsec-prop-vpn-xxxxxxx-0 esp-aes 128 esp-sha-hmac  
  mode tunnel  
exit  
!  
crypto ipsec profile ipsec-vpn-xxxxxxx-0  
  set pfs group2  
  set security-association lifetime seconds 3600  
  set transform-set ipsec-prop-vpn-xxxxxxx-0  
exit  
!  
crypto ipsec df-bit clear  
!  
crypto isakmp keepalive 10 10 on-demand  
!  
crypto ipsec security-association replay window-size 128  
!
```

Tunnel #B

```
!  
crypto ipsec transform-set ipsec-prop-vpn-xxxxxxx-1 esp-aes 128 esp-sha-hmac  
  mode tunnel  
exit  
!  
crypto ipsec profile ipsec-vpn-xxxxxxx-1  
  set pfs group2  
  set security-association lifetime seconds 3600  
  set transform-set ipsec-prop-vpn-xxxxxxx-1  
exit
```

```
!  
crypto ipsec df-bit clear  
!  
crypto isakmp keepalive 10 10 on-demand  
!
```

3.2.3. Tunnel インタフェースの設定

Tunnel インタフェースに IP アドレスを設定します。実際のルーティングはこの Tunnel インタフェースを利用しています。

Tunnel #A

```
!  
interface Tunnel1  
  ip address 169.254.255.2 255.255.255.252  
  ip virtual-reassembly  
  tunnel source 203.0.113.100  
  tunnel destination 72.21.209.225  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile ipsec-vpn-xxxxxxx-0  
  ! This option causes the router to reduce the Maximum Segment Size of  
  ! TCP packets to prevent packet fragmentation.  
  ip tcp adjust-mss 1396  
  no shutdown  
exit  
!
```

Tunnel #B

```
!  
interface Tunnel2  
  ip address 169.254.255.6 255.255.255.252  
  ip virtual-reassembly  
  tunnel source 203.0.113.100  
  tunnel destination 72.21.209.193  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile ipsec-vpn-xxxxxxx-1  
  ! This option causes the router to reduce the Maximum Segment Size of  
  ! TCP packets to prevent packet fragmentation.  
  ip tcp adjust-mss 1396  
  no shutdown
```

```
!
```

3.2.4. ルーティング設定

BGP と Static で設定内容が異なりますので、ご注意ください。

<BGP の場合>

```
!  
router bgp 65001  
  neighbor 169.254.255.1 remote-as 7224  
  neighbor 169.254.255.1 activate  
  neighbor 169.254.255.1 timers 10 30 30  
  address-family ipv4 unicast  
    neighbor 169.254.255.1 remote-as 7224  
    neighbor 169.254.255.1 timers 10 30 30  
    neighbor 169.254.255.1 default-originate  
    neighbor 169.254.255.1 activate  
    neighbor 169.254.255.1 soft-reconfiguration inbound  
    network 0.0.0.0  
  exit  
exit  
!
```

<Static の場合>

```
!  
ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100  
ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200  
!  
ip sla 100  
  icmp-echo 169.254.255.1 source-interface Tunnel1  
  timeout 1000  
  frequency 5
```

```

exit
ip sla schedule 100 life forever start-time now
track 100 ip sla 100 reachability
!
ip sla 200
  icmp-echo 169.254.255.5 source-interface Tunnel2
  timeout 1000
  frequency 5
exit
ip sla schedule 200 life forever start-time now
track 200 ip sla 200 reachability
!
    
```

3.3. 動作確認

AWS マネージメントコンソール上で[VPC]-[VPN Connections]を選択し、該当の VPN 接続をクリックします。メイン画面下部の“Tunnel Dtails”をクリックし、“State”が“UP”となっていることを確認してください。

The screenshot shows the AWS Management Console interface for VPN Connections. At the top, there are buttons for 'Create VPN Connection', 'Delete', and 'Download Configuration'. Below this is a search bar and a table listing VPN connections. The table has columns for Name, VPN ID, State, and Virtual Gateway ID. One connection is listed with a state of 'available'. Below the table, the 'Tunnel Details' tab is selected, showing a table with columns for VPN Tunnel, IP Address, Status, Status Last Changed, and Details. Two tunnels are listed, both with a status of 'UP' and a last changed time of 2014-09-06 15:04 UTC+9 and 2014-09-06 15:05 UTC+9 respectively. A red box highlights this table.

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	[redacted]	UP	2014-09-06 15:04 UTC+9	
Tunnel 2	[redacted]	UP	2014-09-06 15:05 UTC+9	

4. 参考情報

VPN 設定にあたり、こちらの情報もご参考ください。

■ Amazon Virtual Private Cloud ユーザガイド

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_Introduction.html

■ Amazon Virtual Private Cloud ネットワーク管理者ガイド

<http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide>

■ AWS Black Belt Tech シリーズ Amazon VPC

<http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-tech-amazon-vpc>