

Amazon VPCとのVPN接続 マニュアル

2016年7月12日

NECプラットフォームズ株式会社

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Amazon VPC とのVPN接続

「UNIVERGE WAシリーズ」を使用して、Amazon VPC（Amazon Virtual Private Cloud）とIPsec-VPNで接続する際の設定例を紹介します。

Amazon VPCを利用することにより、Amazon AWS（Amazon Web Service）上に仮想プライベートネットワークを構築することが可能です。

※本ページの設定例は、全て当社で接続を確認しておりますが、必ずしも接続性を保証するものではありません。

※当社は、Amazon VPCサービスに関連して発生した如何なる障害に対して、一切の責任を負わないものとします。

※Amazon VPCサービスをご利用になる際は、必ず本サービスの利用規約を確認し、利用規約に則った運用を行ってください。

参考資料

- Amazon VPC技術資料

<http://aws.amazon.com/jp/vpc/>

- Example: Generic Customer Gateway Using Border Gateway Protocol

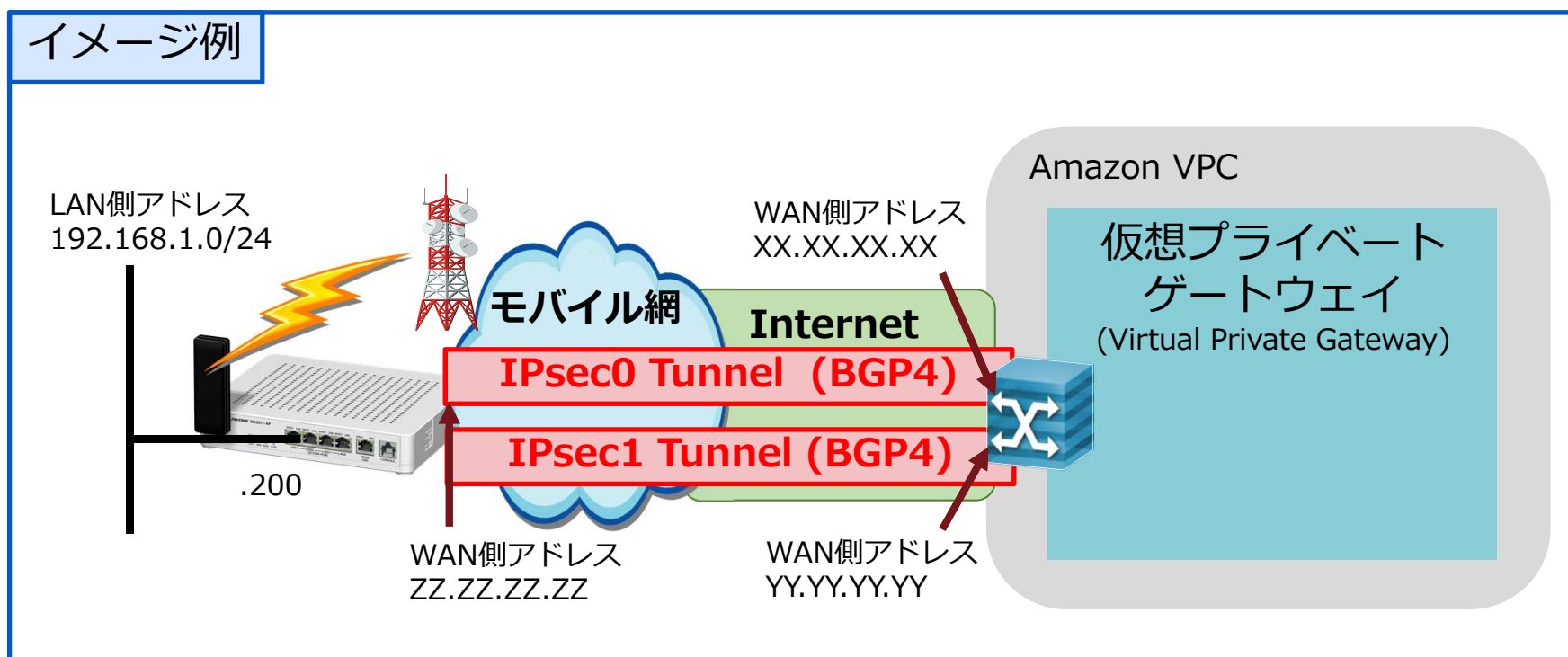
<http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/GenericConfig.html>

接続構成

この設定ガイドでは、「WA2610-AP」の**Serial0**インタフェースをWAN側インタフェース、**GE1(SW-HUB)**ポートをLAN側インタフェースとして使用します。
また、WAN側回線との接続にはデータ通信端末を使用しています。

「WA2610-AP」のIPsecの対向となる仮想プライベートゲートウェイとは、
2本のIPsecトンネルを設定し、BGPで冗長化します。

イメージ例



「WA2610-AP」の設定パラメータ確認 (AWS側)

最初に、AWSのマネジメントコンソール (AWS Management Console) を使用して、VPCと接続するためのパラメータを取得する必要があります。
マネジメントコンソールの使用方法についてはAmazon社にお問い合わせください。

■ マネジメントコンソールの情報登録

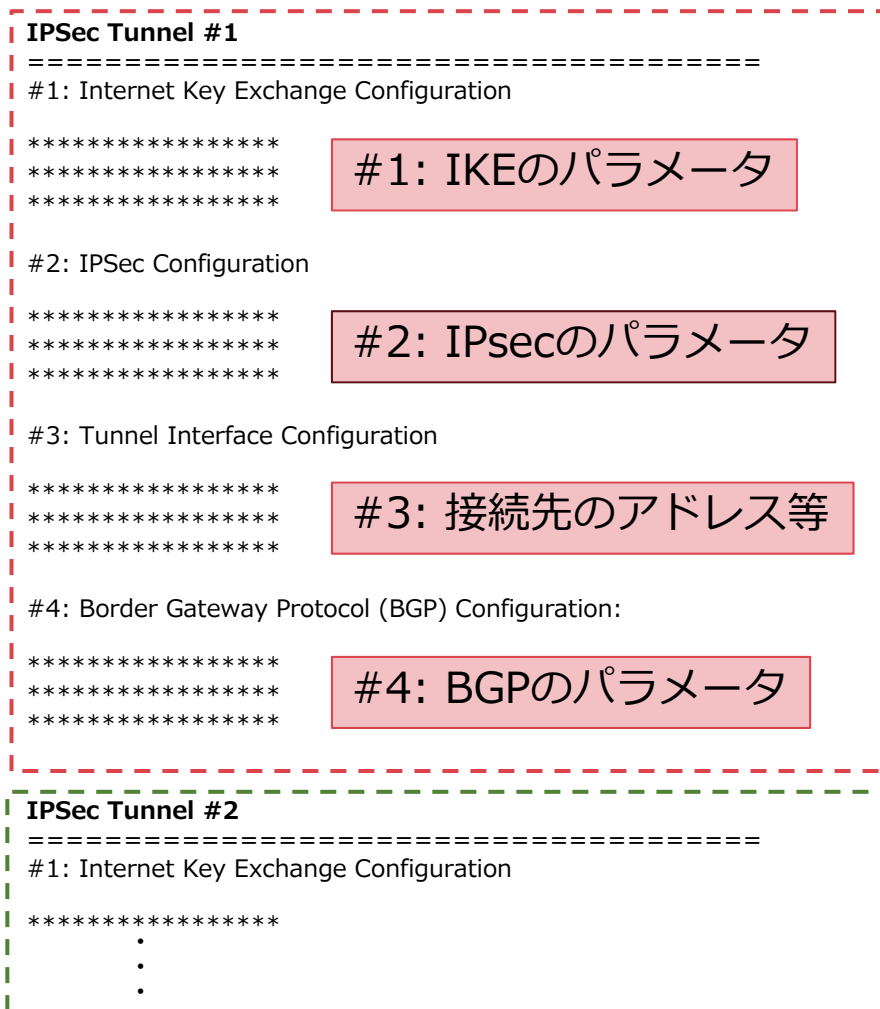
マネジメントコンソールに、今回接続する「WA2610-AP」の情報を登録し、VPCに接続するために必要となる各種パラメータを取得します。

1. 「AWS Management Console」の「VPCページ」を開きます。
2. “VPC ウィザードの開始”ボタンを押して作成を開始します。
3. “プライベートのサブネットおよびハードウェアVPNアクセスを持つVPC”シナリオを選択します。
4. “カスタマーゲートウェイIP”に「WA2610-AP」のWAN側インタフェースに付与するIPアドレスを入力します。(固定IPアドレスである必要があります)
5. “ルーティングの種類”で“動的(BGPが必要)”を選択してVPCの作成をします。
(作成に数分かかります。「VPCが正常に作成されました」と表示されます)
6. “設定のダウンロード”で、作成されたVPN接続の設定ファイルをダウンロードします。ベンダーは“Generic”にします。

6.でダウンロードした設定ファイルには、“vpn-wa2610.txt”と命名したとします。

「WA2610-AP」にパラメータを設定 (WAシリーズ側 1/5)

先程ダウンロードしたファイル(vpn-wa2610.txt)に従い、WA2610-APを設定します。



ファイル前半に記載された
「IPsec Tunnel #1」
をIPsec0トンネル用に
設定してください。

ファイル後半に記載された
「IPsec Tunnel #2」
をIPsec1トンネル用に
設定してください。

「WA2610-AP」にパラメータを設定 (WAシリーズ側 2/5)

「IPSec Tunnel #1」のパラメータを
WA2610-APのIPsec0トンネル用に設定します。
WA2610-APの①～⑥に、#1:IKEのパラメータの①～⑥を設定します。

WA2610-APコンフィグ

```
!  
ike proposal ikeprop1  
  encryption-algorithm aes128-cbc ①  
  authentication-algorithm hmac-sha1 ②  
  lifetime 28800 ③  
  dh-group 1024-bit ④  
!  
ike policy ikepol1  
  mode main ⑤  
  dpd-keepalive enable ph1 10 3  
  proposal ikeprop1  
  pre-shared-key plain XXXX ⑥  
!
```

#1: IKEのパラメータ

#1: Internet Key Exchange Configuration

Configure the IKE SA as follows

- Authentication Method : Pre-Shared Key
- ⑥ - Pre-Shared Key : **XXXX**
- ② - Authentication Algorithm : **sha1**
- ① - Encryption Algorithm : **aes-128-cbc**
- ③ - Lifetime : **28800** seconds
- ⑤ - Phase 1 Negotiation Mode : **main**
- ④ - Perfect Forward Secrecy : **Diffie-Hellman Group 2**

「WA2610-AP」にパラメータを設定 (WAシリーズ側 3/5)

WA2610-APの①～⑦に、#2:IPsecのパラメータの①～⑦を設定します

WA2610-APコンフィグ

```
!
interface IPsec0
  mtu 1436
  ip address unnumbered
  ip forced-fragment
  ip tcp adjust-mss 1387
  ipsec map ipsecprof1
  no shutdown
!
ike policy ikepol1
  mode main
  dpd-keepalive enable ph1 10 3
  proposal ikeprop1
  pre-shared-key plain XXXX
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes128-cbc auth-algo hmac-sha1-96
  lifetime 3600
!
ipsec policy ipsecpol1
  rekey enable always
  pfs enable 1024-bit
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer XX.XX.XX.XX
!
```

#2: IPsecのパラメータ

#2: IPsec Configuration

Configure the IPsec SA as follows:

- Protocol : esp
- ④ - Authentication Algorithm : **hmac-sha1-96**
- ④ - Encryption Algorithm : **aes-128-cbc**
- ⑤ - Lifetime : **3600** seconds
- ⑦ - Mode : **tunnel**
- ⑥ - Perfect Forward Secrecy : **Diffie-Hellman Group 2**
- ③ - DPD Interval : **10**
- ③ - DPD Retries : **3**
- ② - TCP MSS Adjustment : **1387** bytes
- ① - Clear Don't Fragment Bit : **enabled**

「WA2610-AP」にパラメータを設定 (WAシリーズ側 4/5)

WA2610-APの①～④に、#3:接続先のアドレス等の①～④を設定します

WA2610-APコンフィグ

```
!  
interface Loopback0.0  
  ip address AA.AA.AA.AA/AA ①  
  no shutdown  
!  
interface IPsec0 ②  
  mtu 1436  
  ip address unnumbered  
  ip tcp adjust-mss 1387  
  ipsec map ipsecprof1  
  no shutdown  
!  
ip route BB.BB.BB.BB/BB IPsec0 ③  
!  
ipsec profile ipsecprof1  
  mode tunnel  
  ipsec policy ipsecpol1  
  ike policy ikepol1  
  peer XX.XX.XX.XX ④  
!
```

#3: 接続先のアドレス等

#3: Tunnel Interface Configuration

Outside IP Addresses:

- Customer Gateway : ZZ.ZZ.ZZ.ZZ

④ - Virtual Private Gateway : XX.XX.XX.XX

Inside IP Addresses

① - Customer Gateway : AA.AA.AA.AA/AA

③ - Virtual Private Gateway : BB.BB.BB.BB/BB

② - Tunnel interface MTU : 1436 bytes

「WA2610-AP」にパラメータを設定 (WAシリーズ側 5/5)

WA2610-APの①～④に、#4:BGPのパラメータの①～④を設定します

WA2610-APコンフィグ

```
!
router bgp MMMM ①
 neighbor CC.CC.CC.CC remote-as NNNN ②,③
 neighbor CC.CC.CC.CC timers 10 30 ②,④
 neighbor CC.CC.CC.CC update-source Loopback0.0 ②
address-family ipv4 unicast
 network 192.168.1.0/24
!
network-monitor monitor1
 event ip unreachable CC.CC.CC.CC interface IPsec0 ②
 action 10 ipsec-sa-clear ipsecprof1
!
```

#4: BGPのパラメータ

#4: Border Gateway Protocol (BGP) Configuration:

BGP Configuration Options:

① - Customer Gateway ASN	: MMMM
③ - Virtual Private Gateway ASN	: NNNN
② - Neighbor IP Address	: CC.CC.CC.CC
④ - Neighbor Hold Time	: 30

引き続き、
「IPSec Tunnel #2」のパラメータを
WA2610-APのIPsec1トンネル用に設定します。

「WA2610-AP」の設定例 (1/2)

赤字の箇所は、インターネット接続するための設定。AWSとは関係ありません。
青字の箇所は、“vpn-wa2610.txt”に則って設定してください。

```
ppp profile XXXX  
authentication username XXXX  
authentication password plain XXXX
```

1/4

```
!  
interface GigaEthernet1.0  
ip address 192.168.1.200/24  
ip dhcp-server binding default  
no shutdown
```

```
!  
interface Loopback0.0  
ip address AA.AA.AA.AA/AA  
no shutdown
```

```
!  
interface Loopback1.0  
ip address DD.DD.DD.DD/DD  
no shutdown
```

```
!  
interface Serial0  
ip address ipcp  
ppp profile XXXX  
ip napt enable  
ip napt reserve esp  
ip napt reserve udp 500  
mobile id XX X XXXX  
mobile number XXXX  
auto-connect  
no shutdown
```

```
!  
interface IPsec0  
mtu 1436  
ip address unnumbered  
ip forced-fragment  
ip tcp adjust-mss 1387  
ipsec map ipsecprof1  
no shutdown  
!
```

```
!  
interface IPsec1  
mtu 1436  
ip address unnumbered  
ip forced-fragment  
ip tcp adjust-mss 1387  
ipsec map ipsecprof2  
no shutdown  
!  
ip route BB.BB.BB.BB/BB IPsec0  
ip route EE.EE.EE.EE/EE IPsec1  
ip route default Serial0  
!  
router bgp MMMM  
neighbor CC.CC.CC.CC remote-as NNNN  
neighbor CC.CC.CC.CC timers 10 30  
neighbor CC.CC.CC.CC update-source Loopback0.0  
neighbor FF.FF.FF.FF remote-as NNNN  
neighbor FF.FF.FF.FF timers 10 30  
neighbor FF.FF.FF.FF update-source Loopback1.0  
address-family ipv4 unicast  
network 192.168.1.0/24  
!  
network-monitor monitor1  
event ip unreachable CC.CC.CC.CC interface IPsec0  
action 10 ipsec-sa-clear ipsecprof1  
!  
network-monitor monitor2  
event ip unreachable FF.FF.FF.FF interface IPsec1  
action 10 ipsec-sa-clear ipsecprof2  
!  
monitor-group monitor1 enable  
monitor-group monitor2 enable  
!
```

2/4

「WA2610-AP」の設定例 (2/2)

3/4

```
!
proxy-dns ip enable
proxy-dns server default Serial0 ipcp
!
ike proposal ikeprop1
  encryption-algorithm aes128-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike proposal ikeprop2
  encryption-algorithm aes128-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode main
  dpd-keepalive enable ph1 10 3
  proposal ikeprop1
  pre-shared-key plain XXXX
!
ike policy ikepol2
  mode main
  dpd-keepalive enable ph1 10 3
  proposal ikeprop2
  pre-shared-key plain XXXX
!
```

4/4

```
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes128-cbc auth-algo hmac-sha1-96
  lifetime 3600
!
ipsec proposal ipsecprop2
  protocol esp enc-algo aes128-cbc auth-algo hmac-sha1-96
  lifetime 3600
!
ipsec policy ipsecpol1
  rekey enable always
  pfs enable 1024-bit
  proposal ipsecprop1
!
ipsec policy ipsecpol2
  rekey enable always
  pfs enable 1024-bit
  proposal ipsecprop2
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer XX.XX.XX.XX
!
ipsec profile ipsecprof2
  mode tunnel
  ipsec policy ipsecpol2
  ike policy ikepol2
  peer YY.YY.YY.YY
```

状態確認

設定は、前項までとなります。

AWS側の端末に対してpingを実行し、正常に応答を受信することを確認します。

応答が無い場合、

以下の状態確認コマンドを利用して問題箇所の特定を行ってください。

■ WAシリーズの状態確認コマンド

- show ipsec sa

IPsec SAが正常に確立していることを確認するコマンドです。

SAが確立していないときは、

IPsec/IKEパラメータの設定に誤りは無いか確認してください。

- show ip bgp summary

BGPピアとの隣接関係が正常に確立していることを確認するコマンドです。

IPsec SAが正常に確立しているにも関わらず、

BGPピアが確立しない場合は（Established以外）、

BGPの設定に誤りは無いか確認してください。

UNIVERGE WAシリーズ
Amazon VPCとのVPN接続 マニュアル

GVT-009898-001-00

2016年7月 第7.2版
NECプラットフォームズ株式会社
(禁無断複製)

©NEC Corporation 2009-2016
©NEC Platforms, Ltd. 2009-2016

 **Orchestrating** a brighter world

NEC