

Amazon Web Services (AWS) AR4050S, AR3050S 接続設定例

《 Static Routing 》

- ※ 当社検証結果に基づき記載していますが、全てのお客様環境の動作を保証するものではありません。
- ※ 2015年11月現在の仕様に基いて記載しています。今後の仕様変更によっては接続できない可能性があります。

アライドテレシス株式会社

目次

1. 概要
 1. 概要
 2. 設定例の構成
 3. IPsecのパラメータ
2. Amazon VPCの設定
 1. はじめに
 2. Amazon VPCの設定
3. AR4050Sの設定
 1. はじめに
 2. AR4050Sの設定
 3. 設定の確認
4. 動作確認
 1. IPsecの確認
 2. AWSの確認
 3. 通信の確認
 4. 経路冗長の確認 (参考)

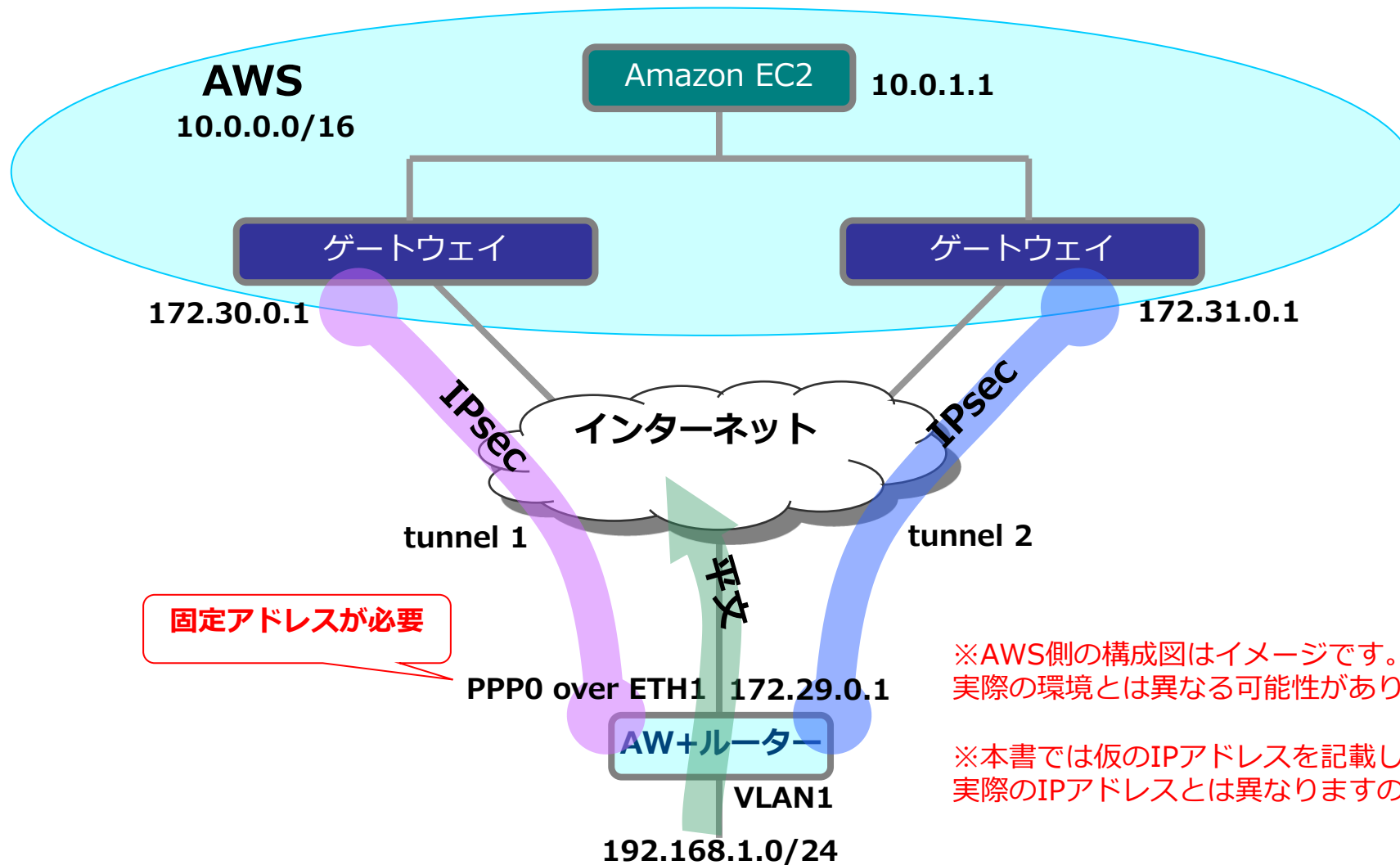
1.概要

1-1.概要

- 本書では、Amazon Web Services (以下 AWS) との接続についての設定例を説明します。以降の記述はAR4050Sを前提として説明いたします。
- Amazon Virtual Private Cloud (以下 Amazon VPC) を通じてAWSと接続します。Amazon VPCは、AWSに接続するためのVPN機能を提供しています。
- AWS側には、Amazon Elastic Compute Cloud (以下 Amazon EC2) と呼ばれる仮想サーバを用意しています。
- 本設定例では、AR4050S配下の端末からインターネット上のサーバーに直接通信（平文通信）できます。
- AR4050Sはファームウェアバージョン5.4.5-2.1以降をご利用下さい。
- Amazon VPCに関する技術情報は以下をご参照ください。
<http://aws.amazon.com/jp/vpc/>

1-2.設定例の構成

- Amazon VPCでは2つのゲートウェイが用意されています。
AR4050Sは2本のIPsec (ESP) トンネルで接続します。



1-3.IPsecのパラメータ

- 下記パラメータで設定します。

IKEフェーズ1 (ISAKMP SAのネゴシエーション)

認証方式	事前共有鍵(pre-shared key)
IKE交換モード	IKEv1 Mainモード
Diffie-Hellman(Oakley)グループ	Group2(1024ビットMODP)
ISAKMPメッセージの暗号化方式	AES128
ISAKMPメッセージの認証方式	SHA-1
ISAKMP SAの有効期限(時間)	28800秒(8時間)

IKEフェーズ2 (IPsec SAのネゴシエーション)

SAモード	トンネルモード
セキュリティープロトコル	ESP(暗号化+認証)
Diffie-Hellman(Oakley)グループ	Group2(1024ビットMODP)、PFS有効
暗号化方式	AES128
認証方式	SHA-1
IPsec SAの有効期限(時間)	3600秒(1時間)

2. Amazon VPCの設定

2-1.はじめに

- Amazon VPCを設定します。
- AWSのWebサイトでアカウントを作成し、「AWS Management Console」を起動します。アカウント作成の流れについては以下をご参照ください。
<http://aws.amazon.com/jp/register-flow/>
- 次頁より主要設定を記載しますが、詳細は以下をご参照ください。
http://docs.amazonaws.com/ja_jp/AmazonVPC/latest/GettingStartedGuide/GetStarted.html
- 次頁から掲載している設定画面は2015年11月現在の情報です。今後、設定画面が変更される場合がございますのでご了承ください。

2-2. Amazon VPCの設定

- ウィザードの開始
 - 画面左上「Services」から「VPC」を選択します。
 - 「VPC Dashboard」にある「Start VPC Wizard」を押します。

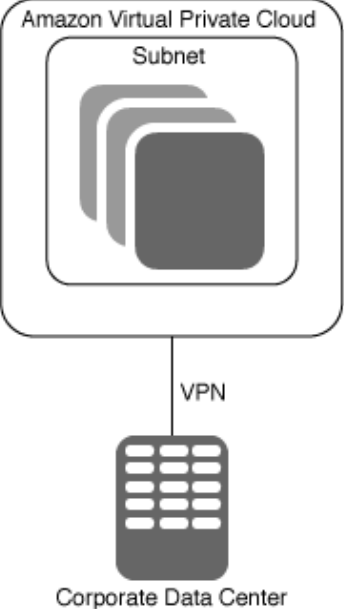
The screenshot shows the Amazon VPC Dashboard interface. The top navigation bar includes 'Services', 'Edit', a search bar, and region/region-specific options like 'Tokyo' and 'Support'. The left sidebar lists various VPC-related services such as 'Virtual Private Cloud', 'Subnets', 'Route Tables', 'Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Peering Connections', 'Security', 'Network ACLs', and 'Security Groups'. The main content area is titled 'Resources' and features two prominent buttons: 'Start VPC Wizard' (highlighted with a red box) and 'Launch EC2 Instances'. Below these buttons, a note states: 'Note: Your Instances will launch in the Asia Pacific (Tokyo) region.' The dashboard also displays a summary of resources in the Asia Pacific (Tokyo) region, including 1 VPC, 2 Subnets, 1 Network ACL, 1 Security Group, 0 VPC Peering Connections, 0 VPN Connections, 1 Internet Gateway, 1 Route Table, 0 Elastic IPs, 0 Running Instances, 0 Customer Gateways, and 0 Virtual Private Gateways. A section for 'VPN Connections' is also visible, with a table header showing 'VPN Connections', 'Customer Gateways', 'VPC ID', and 'Status', and a message indicating 'You do not have any VPNs.' A 'Create VPN Connection' button is located at the bottom of this section.

2-2. Amazon VPCの設定

- ネットワーク構成の選択

ネットワーク構成に合わせて項目を選択します。本例では、「VPC with a Private Subnet Only and Hardware VPN Access」を選び、「Select」を押します。

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet	<p>Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.</p> <p>Creates:</p> <p>A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)</p> <p>Select</p>	 <p>Amazon Virtual Private Cloud</p> <p>Subnet</p> <p>VPN</p> <p>Corporate Data Center</p>
VPC with Public and Private Subnets		
VPC with Public and Private Subnets and Hardware VPN Access		
VPC with a Private Subnet Only and Hardware VPN Access		

2-2. Amazon VPCの設定

● AWS側の設定

- AWS内で使用するサブネットを登録します。下記を参考に空欄を埋めてください。本例では、「IP CIDR block」を「10.0.0.0/16」、「Private Subnet」を「10.0.1.0/24」として登録します。
- 登録を終えたら「Next」を押します。

Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IP CIDR block:* (65531 IP addresses available) VPCで使用可能なIPアドレスの範囲を指定します。サブネットマスクは/16~/28の間で指定します。

VPC name: VPCの名称を指定します。

Private subnet:* (251 IP addresses available) 上記IP CIDR blockで指定した範囲内でプライベートサブネットを指定します。プライベートサブネットは後ほど追加することもできます。

Availability Zone:* Availability Zoneを指定します。「No Preference」にすると自動選択します。

Private subnet name: プライベートサブネットの名称を指定します。

You can add more subnets after AWS creates the VPC.

Add endpoints for S3 to your subnets

Subnet:

Amazon S3 へのエンドポイントを共有するサブネットを選択します。詳細については以下をご参照ください。

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-endpoints.html

Enable DNS hostnames:* Yes No DNS名を割り当てるかどうかを選択します。

Hardware tenancy:* ハードウェア専有インスタンスの設定です。詳細については以下をご参照ください。

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/dedicated-instance.html

Cancel and Exit

Back

Next

2-2. Amazon VPCの設定

- AR4050SSのWAN側/LAN側IPアドレスの登録
 - AR4050SのWAN側IPアドレス（固定アドレス）を登録します。本例では、「172.29.0.1」を登録しています。
 - 「Routing Type」で「Static」を選択し、AR4050SのLAN側IPサブネットを登録します。本例では、「192.168.1.0/24」をLAN側サブネットとして登録しています。
 - 「Create VPC」を押します。

Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:*

Customer Gateway name:

VPN Connection name:

Note: VPN Connection rates apply.

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

Routing Type:*

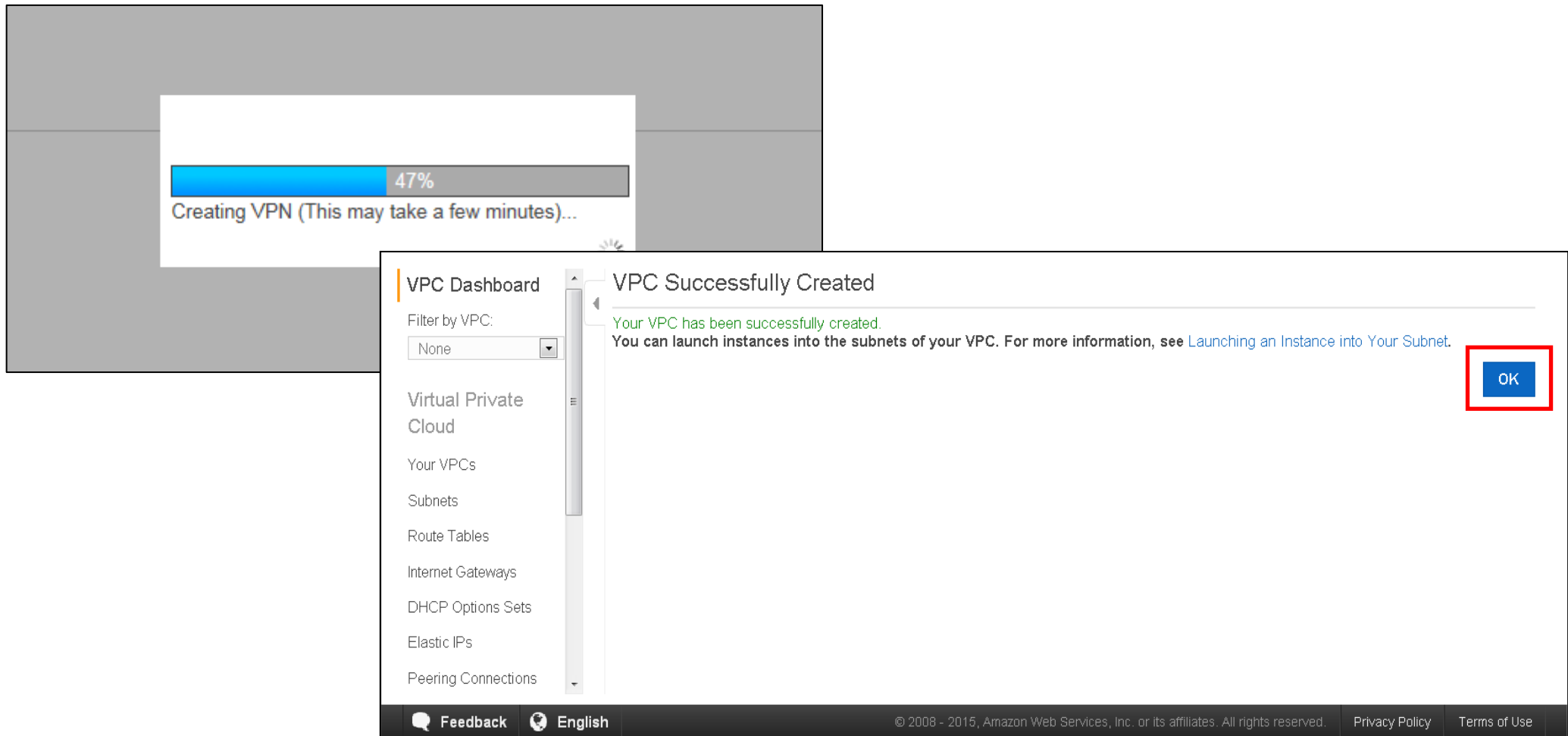
Specify the IP prefixes for the network on your side of the VPN Connection (e.g. 192.168.0.0/16)

IP Prefix	Remove
<input type="text" value="192.168.1.0/24"/>	<input type="button" value="x"/>

2-2. Amazon VPCの設定

- VPCの生成

- 処理が完了すると下のような画面が表示されます。
- 「VPC Successfully Created」と表示されたら、右側の「OK」を押します。



2-2. Amazon VPCの設定

- 設定のダウンロード

- 左側のメニューバーから「VPN Connections」を選択します。
- 作成したVPN名を選択し、「Download Configuration」を押します。

The screenshot shows the Amazon VPC console interface. On the left sidebar, the 'VPN Connections' menu item is highlighted with a red box and a circled '1'. The main content area shows a list of VPN connections. The connection 'AR4050S-to-AWS' is selected, highlighted with a red box and a circled '2'. Above the list, the 'Download Configuration' button is highlighted with a red box and a circled '3'. Below the list, the details for the selected VPN connection are shown, including a table of tunnels.

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1		DOWN	2015-11-18 11:44 UTC+9	
Tunnel 2		DOWN	2015-11-18 11:44 UTC+9	

2-2. Amazon VPCの設定

- 設定のダウンロード
 - 設定例をダウンロードします。
本例では、「Generic」を選択しています。
右下の「Yes, Download」を押します。
 - 設定例が表示されますので、ローカルディスクに保存します。
次頁の「AR4050S の設定」で使用しますので、大切に保管してください。

Download Configuration [?] [X]

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

Vendor Generic [v] [i]

Platform Generic [v] [i]

Software Vendor Agnostic [v] [i]

Cancel **Yes, Download**

3. AR4050Sの設定

3-1.はじめに

- AR4050Sの設定に必要な情報は下記です。
設定前に情報をまとめておくと便利です。

※ 「Amazon VPC Gateway address(1)(2)」、「Preshared key (1)(2)」、「Tunnel interface IP address(1)(2)」、「Tunnel peer IP Address(1)(2)」は、次頁を参考にご記入ください。

設定項目	本例	お客様情報
PPPユーザー名	user@ispA	
PPPパスワード	isppasswdA	
AR4050S ppp0 (WAN側)IPアドレス	172.29.0.1/32	
AR4050S vlan1 (LAN側)IPアドレス	192.168.1.254/24	
Amazon VPC Gateway address(1)	172.30.0.1	
Preshared key(1)	ABCDEFGHIJKLMNQRSTUWXYZ1234	
Tunnel interface IP address(1)	172.16.0.2/30	
Tunnel peer IP Address(1)	172.16.0.1	
Amazon VPC Gateway address(2)	172.31.0.1	
Preshared key(2)	1234abcdefghijklmnopqrsutvwxyz	
Tunnel interface IP address(2)	172.17.0.2/30	
Tunnel peer IP Address(2)	172.17.0.1	
LAN側ネットワークのサブネット	192.168.1.0/24	
AWS内のサブネット	10.0.0.0/16	
Tunnel Interfaceのサブネット(1)	172.16.0.0/30	
Tunnel Interfaceのサブネット(2)	172.17.0.0/30	

3-1.はじめに

- 15ページで保存した設定例をテキストエディターで開きます。
- 2本のIPSecトンネルの「Pre-Shared Key」、「Virtual Private Gateway（Outside IP Addresses）」、「Customer Gateway（Inside IP Address）」、「Virtual Private Gateway（Inside IP Addresses）」を確認します。
※ダウンロードした設定によって記載方法が異なります。下記は「Generic」の場合の例です。

```
IPSec Tunnel #1
```

```
=====
```

```
#1: Internet Key Exchange Configuration
```

```
Configure the IKE SA as follows
```

```
- Authentication Method      : Pre-Shared Key
```

```
- Pre-Shared Key             : ABCDEFGHIJKLMNOPQRSTUVWXYZ1234
```

```
:
```

```
:
```

```
Outside IP Addresses:
```

```
- Customer Gateway           : 172.29.0.1
```

```
- Virtual Private Gateway     : 172.30.0.1
```

```
Inside IP Addresses
```

```
- Customer Gateway           : 172.16.0.2/30
```

```
- Virtual Private Gateway     : 172.16.0.1/30
```

```
:
```



Preshared key(1)



Amazon VPC Gateway address(1)



Tunnel interface IP address(1)



Tunnel peer IP Address(1)

3-1.はじめに

IPSec Tunnel #2

#1: Internet Key Exchange Configuration

Configure the IKE SA as follows

- Authentication Method : Pre-Shared Key
- Pre-Shared Key : 1234abcdefghijklmnopqrstuvwxyz



Preshared key(2)

:
:

Outside IP Addresses:

- Customer Gateway : 172.29.0.1
- Virtual Private Gateway : 172.31.0.1



Amazon VPC Gateway address(2)

Inside IP Addresses

- Customer Gateway : 172.17.0.2/30
- Virtual Private Gateway : 172.17.0.1/30



Tunnel interface IP address(2)



Tunnel peer IP Address(2)

:

3-2. AR4050Sの設定

- ログイン

- AR4050Sにログインします。
工場出荷時設定のCLIの ログインID/PW は下記の通りです。

```
awplus login: manager  
Password: friend ←実際には表示されません  
Last login: Fri Nov 13 17:09:55 JST 2015 on ttyS0  
AlliedWare Plus (TM) 5.4.5 11/12/15 03:11:03  
awplus>
```

- モードの移行

- 非特権EXECモードから、特権EXECモードに移行します。

```
awplus> enable
```

- 特権EXECモードからグローバルコンフィグモードに移行します。

```
awplus# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
awplus(config)#
```

3-2. AR4050Sの設定

- スパニングツリープロトコルの無効化
 - LANポートにおいて初期状態で有効化されているスパニングツリープロトコル (RSTP) を無効化します。

```
awplus(config)# no spanning-tree rstp enable
```

- LANインターフェース設定
 - LAN側インターフェース (vlan1) にIPアドレスを設定します。

```
awplus(config)# interface vlan1  
awplus(config-if)# ip address 192.168.1.254/24  
awplus(config-if)# exit
```

- PPPインターフェース作成
 - ETH 1 インターフェース上にPPPインターフェースを作成します。

```
awplus(config)# interface eth1  
awplus(config-if)# encapsulation ppp 0
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

● PPPoEインターフェース設定

- PPPインターフェースにWAN側のIPアドレスを設定します。
- LCP EchoパケットによるPPP接続の監視を有効にします。
- ISPから通知されたPPPユーザー名やパスワードを設定します。
- PPPインターフェースを通過するTCPパケットのMSS値の自動書き換えを有効にします。

```
awplus(config)# interface ppp0
awplus(config-if)# ip address 172.29.0.1/32
awplus(config-if)# keepalive
awplus(config-if)# ppp username user@ispA
awplus(config-if)# ppp password isppasswdA
awplus(config-if)# ip tcp adjust-mss pmtu
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

● エンティティの設定

- ファイアウォールやNATのルール作成時に使うエンティティ（通信主体）を定義します。
- 内部ネットワークを表すゾーン「private」と外部ネットワークを表すゾーン「public」を作成します。

```
awplus(config)# zone private
awplus(config-zone)# network lan
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# ip subnet 10.0.0.0/16
awplus(config-network)# ip subnet 172.16.0.0/30
awplus(config-network)# ip subnet 172.17.0.0/30
```

```
awplus(config)# zone public
awplus(config-zone)# network wan
awplus(config-network)# ip subnet 0.0.0.0/0 interface ppp0
awplus(config-network)# host ppp0
awplus(config-host)# ip address 172.29.0.1
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

● アプリケーションの設定

- ファイアウォールやNATのルール作成時に通信内容を指定するために使う「アプリケーション」を定義します
- IPsecのESPパケットを表すカスタムアプリケーション「esp」を定義します。
- ISAKMPパケットを表すカスタムアプリケーション「isakmp」を定義します。
- NAT-T(NAT Traversal)パケットをカスタムアプリケーション「nat-t」を定義します

```
awplus(config)# application esp  
awplus(config-application)# protocol 50
```

```
awplus(config)# application isakmp  
awplus(config-application)# protocol udp  
awplus(config-application)# sport 500  
awplus(config-application)# dport 500
```

```
awplus(config)# application nat-t  
awplus(config-application)# protocol udp  
awplus(config-application)# sport 4500  
awplus(config-application)# dport 4500
```


3-2. AR4050Sの設定

- ファイアウォール、NATの設定
 - ISAKMPパケット、NAT-Tパケット、ESPパケットは通しつつ他の外側からの通信を遮断し、内側からの通信は自由に行えるようにファイアウォールのルールを設定します。
 - LAN側ネットワークに接続されているすべてのコンピューターがダイナミックENAT機能を使用できるように設定します。

```
awplus(config)# firewall
```

```
awplus(config-firewall)# rule 10 permit isakmp from public.wan.ppp0 to public.wan
```

```
awplus(config-firewall)# rule 20 permit isakmp from public.wan to public.wan.ppp0
```

```
awplus(config-firewall)# rule 30 permit nat-t from public.wan.ppp0 to public.wan
```

```
awplus(config-firewall)# rule 40 permit nat-t from public.wan to public.wan.ppp0
```

```
awplus(config-firewall)# rule 50 permit esp from public.wan.ppp0 to public.wan
```

```
awplus(config-firewall)# rule 60 permit esp from public.wan to public.wan.ppp0
```

```
awplus(config-firewall)# rule 70 permit any from private to private
```

```
awplus(config-firewall)# rule 80 permit any from private to public
```

```
awplus(config-firewall)# protect
```

```
awplus(config)# nat
```

```
awplus(config-nat)# rule 10 masq any from private to public
```

```
awplus(config-nat)# enable
```

3-2. AR4050Sの設定

● IPsec設定

- IKEフェーズ1のポリシー「AWS-isakmp」とフェーズ2のポリシー「AWS-ipsec」をそれぞれ作成します。

```
awplus(config)# crypto isakmp profile AWS-isakmp  
awplus(config-isakmp-profile)# version 1 mode main  
awplus(config-isakmp-profile)# lifetime 28800  
awplus(config-isakmp-profile)# transform 1 integrity sha1 encryption aes128 group 2
```

```
awplus(config)# crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.30.0.1  
awplus(config)# crypto isakmp key 1234abcdefghijklmnopqrstvwxyz address 172.31.0.1  
awplus(config)# crypto isakmp peer address 172.30.0.1 profile AWS-isakmp  
awplus(config)# crypto isakmp peer address 172.31.0.1 profile AWS-isakmp
```

```
awplus(config)# crypto ipsec profile AWS-ipsec  
awplus(config-ipsec-profile)# lifetime seconds 3600  
awplus(config-ipsec-profile)# transform 1 protocol esp integrity sha1 encryption aes128  
awplus(config-ipsec-profile)# pfs 2
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

- トンネルインターフェース設定
 - IPsecトンネルインターフェースtunnel0、tunnel1を作成します。
 - MTUの設定をします。
 - IPsecトンネルの始点(自装置)と終点(仮想ネットワークゲートウェイ)を指定します。
 - IKEフェーズ2で使用するポリシーを指定します。
 - トンネリング方式を指定します。
 - 通知されたトンネルインターフェースのIPを設定します。
 - トンネルインターフェースを通過するTCPパケットのMSS値の書き換えを有効にします。

```
awplus(config)# int tunnel0
awplus(config-if)# mtu 1436
awplus(config-if)# tunnel source ppp0
awplus(config-if)# tunnel destination 172.30.0.1
awplus(config-if)# tunnel protection ipsec profile AWS-ipsec
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# ip address 172.16.0.2/30
awplus(config-if)# ip tcp adjust-mss 1387
```

```
awplus(config)# int tunnel1
awplus(config-if)# mtu 1436
awplus(config-if)# tunnel source ppp0
awplus(config-if)# tunnel destination 172.31.0.1
awplus(config-if)# tunnel protection ipsec profile AWS-ipsec
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# ip address 172.17.0.2/30
awplus(config-if)# ip tcp adjust-mss 1387
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

● トリガーの設定

- メインで使用しているトンネルで通信断が発生した際、もう片方のトンネルに自動で切り替わるようトリガーの設定を行います。
- tunnel0の通信断を検知した際にルートの削除を行うスクリプトtunnel0_down.scpと、トンネルが再び通信可能になった際にルートの追加を行うtunnel0_up.scpをそれぞれルーターのフラッシュ上に保存します。

- tunnel0_down.scp

```
enable
configure terminal
no ip route 10.0.0.0/16 tunnel0
```

- tunnel0_up.scp

```
enable
configure terminal
ip route 10.0.0.0/16 tunnel0
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

- トンネルインターフェースtunnel0の接続性を監視するPingポーリング「1」を作成します。
- Pingポーリングトリガーを作成します。

```
awplus(config)#ping-poll 1  
awplus(config-ping-poll)#ip 172.16.0.1  
awplus(config-ping-poll)#normal-interval 25  
awplus(config-ping-poll)#active
```

```
awplus(config)#trigger 1  
awplus(config-trigger)# type ping-poll 1 down  
awplus(config-trigger)# script 1 flash:/tunnel0_down.scp
```

```
awplus(config)#trigger 2  
awplus(config-trigger)# type ping-poll 1 up  
awplus(config-trigger)# script 1 flash:/tunnel0_down.up
```

赤字には17ページのお客様情報を入力ください。

3-2. AR4050Sの設定

● ルート設定

- デフォルトルートを設定します。
- AWS宛の通信がIPsecトンネルを経由するよう設定します。
ここでは2本のトンネルの内、tunnel0を優先して使用するようになっています。
またIPsecトンネルが確立するまでは、このルートを使用できないよう設定します。

```
awplus(config)# ip route 0.0.0.0/0 ppp0  
awplus(config)# ip route 10.0.0.0/16 tunnel0  
awplus(config)# ip route 10.0.0.0/16 tunnel1 10  
awplus(config)# ip route 10.0.0.0/16 null 254
```

● コンフィグの保存、確認

- 設定は以上となります。
- 現在の設定内容を起動時コンフィグとして保存します。
- 設定（ランニングコンフィグ）を表示します。
- 次頁の「入力コマンド一覧(1)(2)」を参考に、設定に誤りが無いかご確認ください。

```
awplus# copy running-config startup-config  
awplus# show running-config
```

赤字には17ページのお客様情報を入力ください。

3-3. 設定の確認

● 入力コマンド一覧(1)

- 「show running-config」で設定を確認できます。下記のコマンドが表示されているかご確認ください。

```
!  
no spanning-tree rstp enable  
!  
interface eth1  
  encapsulation ppp 0  
!  
interface vlan1  
  ip address 192.168.1.254/24  
!  
interface ppp0  
  keepalive  
  ppp username user@ispA  
  ppp password isppasswdA  
  ip address 172.29.0.1/32  
  ip tcp adjust-mss pmtu  
!  
zone private  
  network lan  
  ip subnet 10.0.0.0/16  
  ip subnet 192.168.1.0/24  
  ip subnet 172.16.0.0/30  
  ip subnet 172.17.0.0/30  
!  
zone public  
  network wan  
  ip subnet 0.0.0.0/0 interface ppp0  
  host ppp0  
  ip address 172.29.0.1  
!  
application esp  
protocol 50
```

```
!  
application isakmp  
  protocol udp  
  sport 500  
  dport 500  
!  
application nat-t  
  protocol udp  
  sport 4500  
  dport 4500  
!  
firewall  
  rule 10 permit isakmp from public.wan.ppp0 to public.wan  
  rule 20 permit isakmp from public.wan to public.wan.ppp0  
  rule 30 permit nat-t from public.wan.ppp0 to public.wan  
  rule 40 permit nat-t from public.wan to public.wan.ppp0  
  rule 50 permit esp from public.wan.ppp0 to public.wan  
  rule 60 permit esp from public.wan to public.wan.ppp0  
  rule 70 permit any from private to private  
  rule 80 permit any from private to public  
  protect  
!  
nat  
  rule 10 masq any from private to public  
enable
```

各コマンドの詳細は、コマンドリファレンスを参照ください。

http://www.allied-telesis.co.jp/support/list/router/ar3050s_ar4050s/manual.html

3-3. 設定の確認

• 入力コマンド一覧(2)

```
!  
crypto ipsec profile AWS-ipsec  
  lifetime seconds 3600  
  pfs 2  
  transform 1 protocol esp integrity SHA1 encryption AES128  
!  
crypto isakmp profile AWS-isakmp  
  version 1 mode main  
  lifetime 28800  
  transform 1 integrity SHA1 encryption AES128 group 2  
!  
crypto isakmp key ABCDEFGHIJKLMNOPQRSTUVWXYZ1234 address 172.30.0.1  
crypto isakmp key 1234abcdefghijklmnopqrsutvwxyz address 172.31.0.1  
!  
crypto isakmp peer address 172.30.0.1 profile AWS-isakmp  
crypto isakmp peer address 172.31.0.1 profile AWS-isakmp  
!  
interface tunnel0  
  mtu 1436  
  tunnel source ppp0  
  tunnel destination 172.30.0.1  
  tunnel protection ipsec profile AWS-ipsec  
  tunnel mode ipsec ipv4  
  ip address 172.16.0.2/30  
  ip tcp adjust-mss 1387  
!
```

```
!  
interface tunnel1  
  mtu 1436  
  tunnel source ppp0  
  tunnel destination 172.31.0.1  
  tunnel protection ipsec profile AWS-ipsec  
  tunnel mode ipsec ipv4  
  ip address 172.17.0.2/30  
  ip tcp adjust-mss 1387  
!  
ping-poll 1  
  ip 172.16.0.1  
  normal-interval 25  
  active  
!  
trigger 1  
  type ping-poll 1 down  
  script 1 flash:/tunnel0_down.scp  
trigger 2  
  type ping-poll 1 up  
  script 1 flash:/tunnel0_up.scp  
!  
ip route 0.0.0.0/0 ppp0  
ip route 10.0.0.0/16 tunnel0  
ip route 10.0.0.0/16 tunnel1 10  
ip route 10.0.0.0/16 Null 254  
!  
end
```

各コマンドの詳細は、コマンドリファレンスを参照ください。

http://www.allied-telesis.co.jp/support/list/router/ar3050s_ar4050s/manual.html

3-3. 設定の確認

- スクリプト

- 「show file xxxx(スクリプトファイル名)」でスクリプトの内容を確認できます。下記のコマンドが表示されているかご確認ください。

- tunnel0_down.scp

```
enable  
configure terminal  
no ip route 10.0.0.0/16 tunnel0
```

- tunnel0_up.scp

```
enable  
configure terminal  
ip route 10.0.0.0/16 tunnel0
```

各コマンドの詳細は、コマンドリファレンスを参照ください。
http://www.allied-telesys.co.jp/support/list/router/ar3050s_ar4050s/manual.html

4. 動作確認

4-1. IPsecの確認

- ISAKMP SAの確立状態

- 下記コマンドを実行し、ISAKMP SAの確立状態がEstablishであることを確認します。

```
awplus# show isakmp sa
```

Peer	Cookies (initiator:responder)			Auth	Ver	Expires
	Encryption	Integrity	Group	DPD	NATT	State
172.30.0.1	b697098bef5e159d:d53526e718174b9b			PSK	1	27461s
	AES128	SHA1	2	yes	yes	Established
172.31.0.1	1dee3c6ff657f7ca:faae8592a9465890			PSK	1	18833s
	AES128	SHA1	2	yes	yes	Established

- AR4050Sはトンネル経由の通信が行われないと、トンネルの接続を開始しません。そのため、上記のように表示されない場合は一度AWSのTunnel peer IP address宛にpingを実行してみてください。それでも上記のように表示されない場合は、ISAKMP SAの確立に失敗しています。Preshared keyやISAKMPポリシー、ISAKMP proposalが正しく設定されているかご確認ください。

4-1. IPsecの確認

- IPsec SAの確立状態

- 下記コマンドを実行し、IPsec SAが確立されていることを確認します。

```
awplus#show ipsec sa
```

Peer	SPI (in:out) Encryption	Mode Integrity	Proto PFS	Expires
172.30.0.1	cabf7c72:30b110cf AES128	tunnel SHA1	ESP 2	2170s
172.31.0.1	c4400876:a1e6e6b8 AES128	tunnel SHA1	ESP 2	231s

- 上記のように表示されない場合は、IPsec SAの確立に失敗しています。IPsecポリシー、IPsec proposalが正しく設定されているかご確認ください。

4-2. AWSの確認

- メニューバーの「VPN Connection」内の「Tunnel Details」タブを選択し、両方のトンネルのStatusが「UP」になっていることを確認してください。

The screenshot displays the AWS Management Console interface for VPN Connections. On the left sidebar, the 'VPN Connections' menu item is highlighted with a red box. The main content area shows a list of VPN connections with the following table:

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway
AR4050S-to-AWS	vpn-a5886dcc	available	vgw-1f8a3c1e	cgw-f776c0f6 () AR4050S

Below the list, the details for the selected connection 'vpn-a5886dcc | AR4050S-to-AWS' are shown. The 'Tunnel Details' tab is selected and highlighted with a red box. The table below shows the status of the tunnels:

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	()	UP	2015-11-18 15:52 UTC+9	
Tunnel 2	()	UP	2015-11-18 16:45 UTC+9	

The 'Status' column for both tunnels is highlighted with a red box, showing 'UP'.

4-3. 通信の確認

- Amazon EC2と通信ができることを確認します。
 - Amazon EC2の作成方法については、AWSの技術資料をご参照ください。
<http://aws.amazon.com/jp/documentation/ec2/>
 - Amazon EC2のIPアドレス（本例では「10.0.1.1」）に対してpingが通ることを確認します。
 - ルーター上でpingを実行する際は、パケットがファイアウォールによって破棄されないよう始点IPアドレスを指定してください。

```
awplus# ping 10.0.1.1 source 192.168.1.254
PING 10.0.1.1 (10.0.1.1) from 192.168.1.254 : 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_req=1 ttl=127 time=6.38 ms
64 bytes from 10.0.1.1: icmp_req=2 ttl=127 time=5.90 ms
64 bytes from 10.0.1.1: icmp_req=3 ttl=127 time=6.47 ms
64 bytes from 10.0.1.1: icmp_req=4 ttl=127 time=6.16 ms
64 bytes from 10.0.1.1: icmp_req=5 ttl=127 time=6.10 ms

--- 10.0.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 5.906/6.207/6.471/0.214 ms
```

4-5. 経路冗長の確認 (参考)

- Amazon VPCのゲートウェイの一方がダウンしたときの経路の冗長性を確認します。
 - 実際のゲートウェイのダウンを待つことはできないので、ここではtunnel 0を通るパケットを強制的にフィルタリングすることで障害をシミュレートします。
 - ファイアウォールの設定を終了したら、ファイアウォールのセッションテーブルのクリアを行ってください。

```
awplus(config)#zone AWS
awplus(config-zone)#network gateway1
awplus(config-network)# ip subnet 172.30.0.1/32
```

```
awplus(config)#firewall
awplus(config-firewall)#rule 1 deny any from AWS.gateway1 to public.wan.ppp0
awplus(config-firewall)#rule 2 deny any from public.wan.ppp0 to AWS.gateway1
```

```
awplus# awplus#clear firewall connections
```

赤字には、Amazon VPC Gateway address(1)のアドレスを入力ください。

4-4. 経路冗長の確認 (参考)

- しばらく待つとtunnel 0のIPsecが切断され、経路がtunnel 1に切替ります。
- 下記コマンドで経路の切り替わりを確認してください。

```
awplus# show ip route
```

```
Codes: C - connected, S - static, R - RIP, B - BGP
```

```
O - OSPF, D - DHCP, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
* - candidate default
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] is directly connected, ppp0
```

```
S 10.0.0.0/16 [10/0] is directly connected, tunnel1
```

```
C 172.17.0.0/30 is directly connected, tunnel1
```

```
C 172.16.0.0/30 is directly connected, tunnel0
```

```
C 192.168.1.0/24 is directly connected, vlan1
```


4-4. 経路冗長の確認（参考）

- この状態でAmazon EC2に対してpingが通ることを確認します。

```
awplus# ping 10.0.1.1 source 192.168.1.254
PING 10.0.1.1 (10.0.1.1) from 192.168.1.254 : 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_req=1 ttl=127 time=6.59 ms
64 bytes from 10.0.1.1: icmp_req=2 ttl=127 time=6.32 ms
64 bytes from 10.0.1.1: icmp_req=3 ttl=127 time=6.04 ms
64 bytes from 10.0.1.1: icmp_req=4 ttl=127 time=6.14 ms
64 bytes from 10.0.1.1: icmp_req=5 ttl=127 time=6.13 ms

--- 10.0.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 6.042/6.247/6.591/0.201 ms
```

4-4. 経路冗長の確認（参考）

- 経路の切り替わりを確認したら、先ほどのフィルタリングを消去します。

```
awplus#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
awplus(config)#firewall
```

```
awplus(config-firewall)#no rule 1
```

```
awplus(config-firewall)#no rule 2
```

- しばらく待つと、経路が再びtunnel 0に切り戻りますので、「show ip route」でご確認ください。



おかげさまで30周年

これまでも、これからも、
エンタープライズのお客様と共に。



<http://www.allied-telesis.co.jp/>
<http://www.allied-telesis.co.jp/sdn/blog.html>

Copyright© 2017 Allied Telesis K.K. All Rights Reserved.