

AR4000S-Cloud on Amazon Web Services (AWS) Installation Guide

Installation Guide

Introduction

The AR4000S-Cloud is a virtual router appliance product that provides functions such as VPN and firewall.

This installation guide enables you to install and configure your AR4000S-Cloud in an Amazon Web Services (AWS) cloud environment.

Amazon Web Services (AWS)

The system requirements for the AWS environment are as follows:

- Supported platforms: Amazon Elastic Compute Cloud (Amazon EC2)
- Supported virtualization type: Hardware Virtual Machine (HVM)
- Supported instance type: t3.medium or higher (vCPU: 1 or higher, memory: 4GB or higher)
- Virtual disk size: 20GB or more

Note: This document contains a lot of AWS-specific terminology. For more detailed information about AWS terms and concepts, please refer to the AWS documentation. Also, the screenshots shown were current at the time of creation, but are subject to change.

Contents

Introduction	1
Amazon Web Services (AWS)	1
Procedure overview	3
Create an Amazon Machine Image	4
Prerequisites	4
Create an API key	4
Install required packages	7
Preparing the VHD image file and the Python script file	7
Upload VHD image file and create AMI	8
Create an instance	10
Prerequisites	10
Create VPC	11
Create instance	14
Create and configure an internet gateway	25
Create a route table	27
SSH connection settings	33
SSH key pair	33
Accessing this product via SSH using "PuTTY"	34
SSH connection to this product using SSH client of Ubuntu (Linux)	39
Connecting to your local network	41
How to use the VPN function of AR4000S-Cloud	41
How to use AWS (VPC) VPN function	45
Licensing	59
Accessing the Web GUI and Installing Licenses	59
Firmware update	61
Prerequisite	61
About ISO files and VHD files	61
Update procedure	61
Tips and troubleshooting	62
Lost network connection	62
When the SSH server function is disabled	62
Creating an instance snapshot	63

Procedure overview

The general procedure for setting up this product on AWS is as follows:

1. [“Create an Amazon Machine Image”](#)

Upload the VHD image file of this product to Amazon EC2 to create an Amazon Machine Image (AMI).

2. [“Create an instance”](#)

Create an instance (virtual machine) of this product from the AMI created in Step 1.

3. [“SSH connection settings”](#)

Access the instance using an SSH client (for example, PuTTY).

4. [“Connecting to your local network”](#)

Create an IPsec VPN with the local network to enable secure communication between AWS and devices on the local network.

Create an Amazon Machine Image

To create an instance (virtual machine) of this product on AWS, you need to create an Amazon Machine Image (AMI), which is a virtual machine template. This section explains how to upload the VHD image file to AWS and create an AMI.

Note: This process is only required the first time you install. After initial setup, you can use the **software-upgrade** command to update the firmware (see the [“Firmware update”](#) section).

Prerequisites

To create an AMI, you need:

- A computer that can connect to the Internet running Linux (Ubuntu or Debian).

Note: Windows is not supported.

- An AWS API key (AKID and SAK, ID and password to use the API) with full access permissions for Amazon EC2 and Amazon S3.

Note: Creating this key is described in the [“Create an API key”](#) section.

- The .vhd disk image file.
- The .py Python upload script file.

Note: These files are available from the Software Download Centre.

- The Amazon EC2 API tool (a tool for performing various operations on EC2 from the command line). Please refer to the [AWS CLI installation documentation](#) for details.

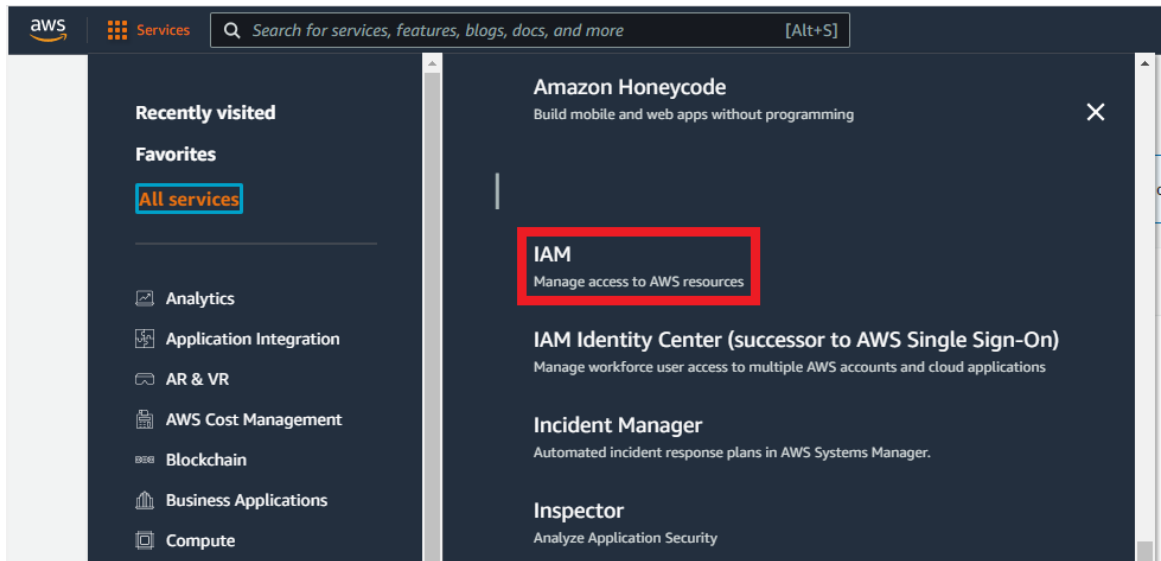
Create an API key

To create an AMI, you first need an AWS API key.

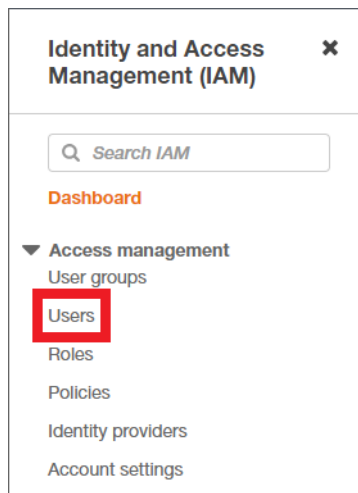
To create an API key, you must have execute permissions for the user access and encryption key management service “Identity and Access Management (IAM)”. Please refer to the [AWS Identity and Access Management documentation](#) for details.

If you are configuring Roles in the navigation pane, you must create a role named **vmimport**, specify in the trust relationship policy document that VM Import assumes this role, and attach an IAM policy to the role. Please refer to [the AWS VM Import/Export documentation](#) for details.

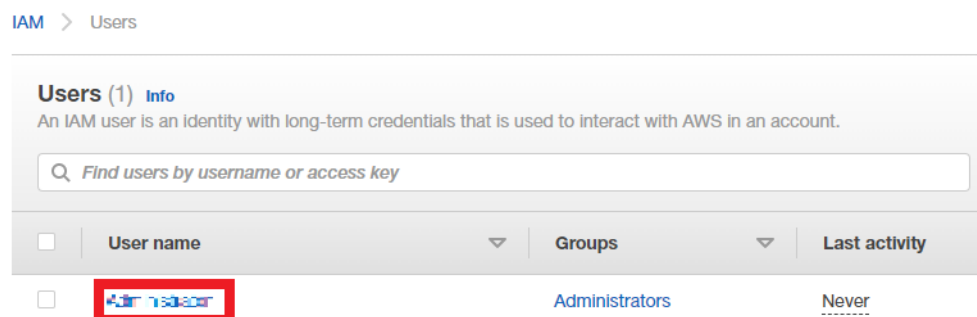
1. From the home screen of the AWS Management Console, select **Services > All Services > IAM**.



2. On the IAM dashboard screen, click **Users** under **Access Management** on the left menu.



3. Click on your IAM user-name.



- Switch to the **Security credentials** tab and click **Create Access Key**.

Summary

User ARN: [redacted]

Path: /

Creation time: 2016-12-20 17:07 UTC+1300

Permissions | Groups (1) | Tags | **Security credentials** | Access Advisor

Sign-in credentials

Summary

- Console sign-in link: [https://\[redacted\]](https://[redacted])
- Console password: Enabled (never signed in) | Manage
- Assigned MFA device: Not assigned | Manage
- Signing certificates: None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

Create access key

- The **Create access key** dialog will be displayed. Click **Download .csv file** to save the access key ID and secret access key information.

Create access key

Warning

Never post your secret access key on public platforms, such as GitHub. This can compromise your account security.

Success

This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Download .csv file

Access key ID	Secret access key
[redacted]	***** Show

Close

Alternatively, click **Show** next to the secret access key to display the key. You can then copy the access key ID and secret access key information, and save them locally.

Access key ID	Secret access key
AKIATY4WLAA45KFSSJWE	[redacted] Hide

Note: Keep your access key in a safe place. A generated key can only be downloaded once. Do not send the key by e-mail. Do not hand over the key information, even if you receive an inquiry from AWS or Amazon.com. An authorized Amazon representative will never ask you for a key.

6. You have now created your AWS API key.

Install required packages

Install the required packages on your Linux (Ubuntu or Debian) computer. The following packages are required to upload the VHD image file of this product to AWS and create an AMI:

- Python version 3.7 or later
- Ec2-api-tools
- boto3
- Python-pip

For example, to install them on Ubuntu, enter the following commands:

```
ubuntu@ubuntu-pc:~/tmp$ sudo apt-get install ec2-api-tools
ubuntu@ubuntu-pc:~/tmp$ sudo apt-get install python3.7
ubuntu@ubuntu-pc:~/tmp$ sudo apt -get install python-pip
ubuntu@ubuntu-pc:~/tmp$ sudo pip install "boto3>=1.3.0,<=1.4.4"
```

Preparing the VHD image file and the Python script file

Create a temporary folder on your computer. Copy the VHD image file “AR4000S-Cloud-X.X.X-X.X.vhd” (where X.X.X-X.X is the version you want to install) and the Python script “upload_vhd.py” to this location.

In the confirmation screen example below, it is assumed that these files are placed in the user's tmp folder directly under the home directory of the user.

```
ubuntu@ubuntu-pc:~/tmp$ ls
AR4000S-Cloud-5.5.2-1.1.vhd upload_vhd.py
```

Upload VHD image file and create AMI

Use the Python script “upload_vhd.py” to upload the VHD image file to AWS and create an AMI.

The command line format and arguments for executing the script are as follows:

```
format
python upload_vhd.py IMAGEFILE AMINAME --region NAME --bucket NAME --akid KEY
--sak KEY

argument
IMAGEFILE : VHD image file of this product to be imported (Example: AR4000S-
Cloud-5.5.2-1.1.vhd)
AMINAME : AMI name (Example: AR4000S-Cloud-5.5.2)
--region NAME : AWS region to use (e.g. ap-northeast-1)
                *For a list of region names, please refer to Amazon's user guide.
--bucket NAME : AWS S3 bucket to temporarily upload the VHD file to (e.g. AR4000S-
Cloud.upload)
                *If it does not exist, the bucket will be created automatically.
--akid KEY : API key access key ID (for access to EC2 and S3) (e.g. AKIDABCDF)
--sak KEY : API key secret key (for access to EC2 and S3) (e.g. SAKABCDF)
```

The VHD image file is temporarily uploaded to your AWS S3 bucket.

Note: Please refer to Amazon's user guide for charges incurred by using S3. Bucket names must be unique across S3 (you cannot use a bucket name used by another S3 user). Refer to Amazon's user guide for bucket naming conventions.

An execution example is shown below:

```
ubuntu@ubuntu-pc:~/tmp$ python upload_vhd.py AR4000S-Cloud-5.5.2-1.1.vhd
AR4000S-Cloud-5.5.2 --region ap-northeast-1 --bucket AR4000S-Cloud.upload -- akid
AKIDABCDF --sak SAKABCDF
upload_image: Creating Bucket
upload_image: Uploading disk image
upload_image: 10% (12MB/120MB)
upload_image: 20% (24MB/120MB)
upload_image: 30% (36MB/120MB)
upload_image: 40% (48MB/120MB)
upload_image: 50% (60MB/120MB)
upload_image: 60% (72MB/120MB)
upload_image: 70% (84MB/120MB)
upload_image: 80% (96MB/120MB)
upload_image: 90% (108MB/120MB)
import_snapshot: Converting disk image to EBS snapshot
import_snapshot: ImportTaskId=import-snap-0153ad4f76fb9e4bb
import_snapshot: 2%
import_snapshot: 43%
import_snapshot: 100%
import_snapshot: Snapshot created snap-0a20e8cb894a2f65d
import_snapshot: Deleting disk image from S3
register_image: Creating AMIs
register_image: AMI created ami-038777b2b30e26eb6
```

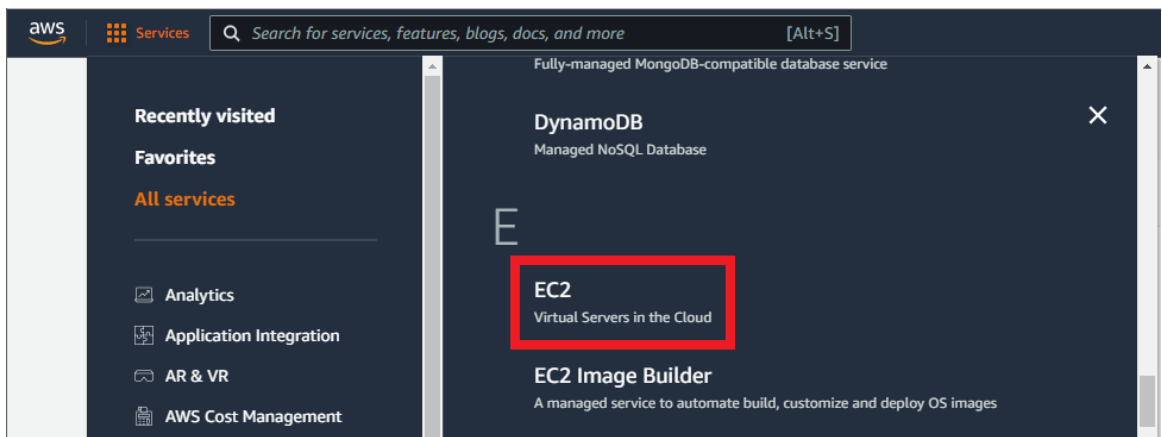

Note: The content displayed when the script is executed is an example. The displayed contents may differ depending on the settings in AWS.

When this product is successfully uploaded to AWS, the following message will be displayed. XXXXXXXXX is automatically generated during the process.

```
register_image: AMI created ami-XXXXXXX
```

You can also check the AMI in the EC2 dashboard.

1. From the home screen of the AWS Management Console, select **Services > All Services > EC2**.



2. On the EC2 dashboard screen, click **AMI** under **Image** on the left menu.

Amazon Machine Images (AMIs) (1/2) Info

Owned by me Find AMI by attribute or tag

Name	AMI ID	AMI name	Source	Owner	Visibility	Status
-	ami-057fa2afd74ccea6	vaa-main-20221003-2	259623944249/vaa-main-20221003-2	259623944249	Private	Available
<input checked="" type="checkbox"/>	ami-05d92637888e52c93	vaa-5.5.2-1.1	259623944249/vaa-5.5.2-1.1	259623944249	Private	Available

AMI ID: ami-05d92637888e52c93

Details Permissions Storage Tags

AMI ID ami-05d92637888e52c93	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name vaa-5.5.2-1.1	Owner account ID 259623944249	Architecture x86_64	Usage operation RunInstances
Root device name /dev/xvda	Status Available	Source 259623944249/vaa-5.5.2-1.1	Virtualization type hvm
Boot mode -	State reason -	Creation date Thu Oct 06 2022 11:12:47 GMT+1300 (New Zealand Daylight Time)	Kernel ID -
Block devices /dev/xvda=snap-0fcae78d45e6fbf61:10:true:gp2	Description -	Product codes -	RAM disk ID -

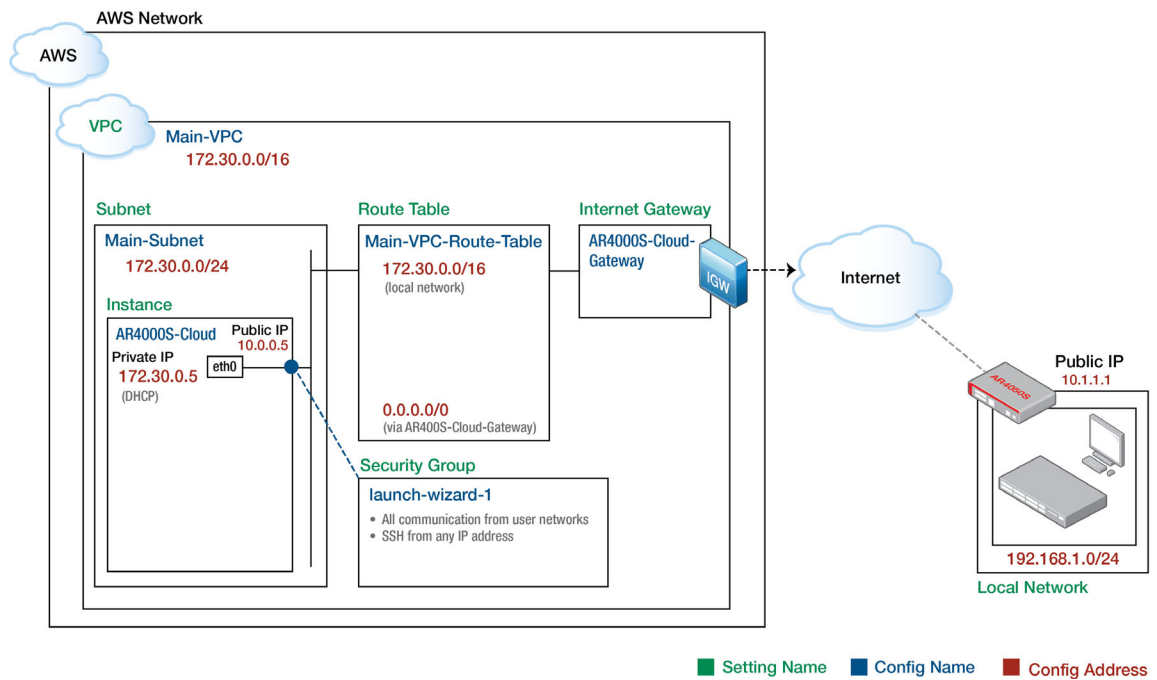
Create an instance

The next step in the process is to create an instance (virtual machine).

Prerequisites

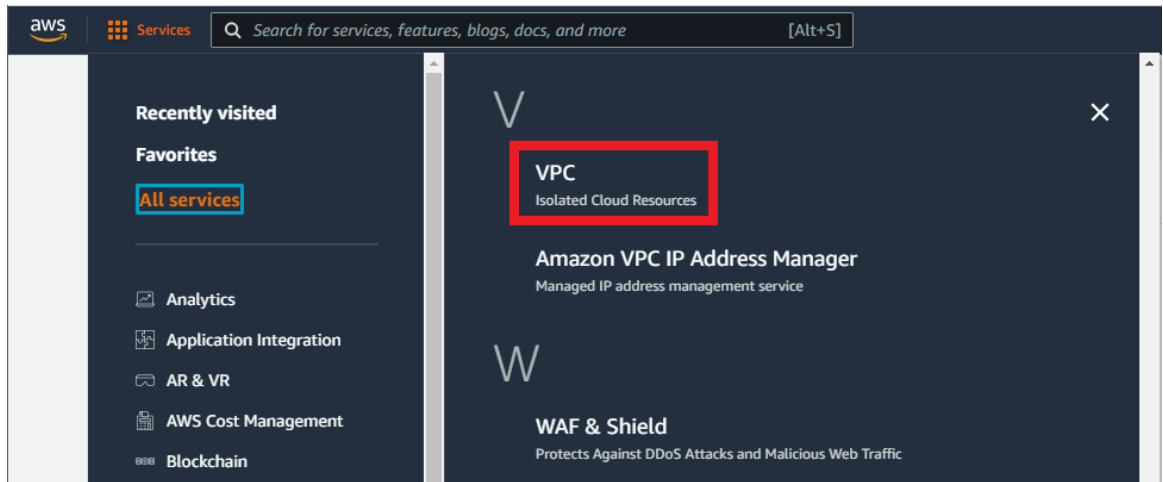
To create an instance, you need an AMI as a template. This section assumes that you have already completed the “[Create an Amazon Machine Image](#)” section.

Network configuration, SSH keys, access control, etc, also need to be planned in advance. This document assumes these have already been completed.

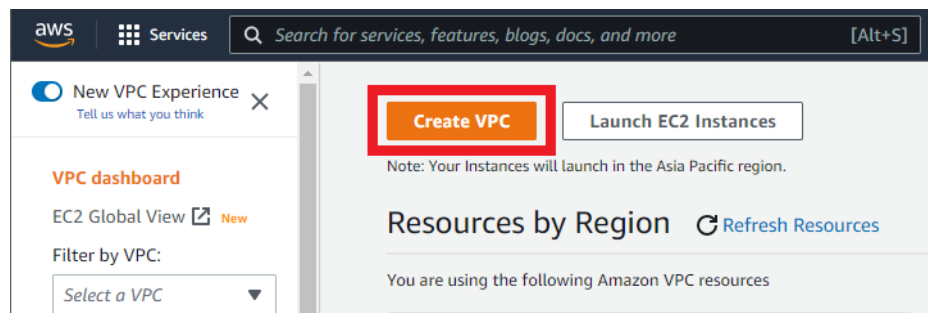


Create VPC

1. From the home screen of the AWS Management Console, select **Services** > **All Services** > **VPC**.



2. Click **Create VPC** on the VPC dashboard screen.



3. On the **Configure VPC** screen, configure the following settings and click **Create VPC**.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Main-VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR

172.30.0.0/16

IPv6 CIDR block [Info](#)

No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="Main-VPC"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

Cancel

- If the VPC is successfully created, you will see a screen like the one below.

You successfully created vpc-0d2145b3c4f0742b8 / Main-VPC

VPC > Your VPCs > vpc-0d2145b3c4f0742b8

vpc-0d2145b3c4f0742b8 / Main-VPC Actions

Details [Info](#)

VPC ID vpc-0d2145b3c4f0742b8	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-09338eccde520c074	Main route table rtb-035809a79f3d81ea4	Main network ACL acl-0ca88e6a26d2e05e7
Default VPC No	IPv4 CIDR 172.30.0.0/16	IPv6 pool -	IPv6 CIDR -
Network mapping unit metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 259623944249	

[CIDRs](#) | [Flow logs](#) | [Tags](#)

CIDRs [Info](#)

Address type	CIDR	Pool
IPv4	172.30.0.0/16	-

Create instance

1. From the **Services** menu of the AWS Management Console, select **All Services** > **EC2** to open the EC2 dashboard screen, then click **Launch Instance** > **Launch Instance**.

The screenshot shows the AWS Management Console interface for the EC2 service. The top navigation bar includes the AWS logo, a 'Services' menu, and a search bar. The left sidebar contains the 'EC2 Dashboard' with various navigation options, and the 'Launch Instance' button is highlighted with a red border. The main content area displays 'Resources' for the Asia Pacific (Sydney) region, showing a table of EC2 resources and a 'Launch instance' section with a red-bordered 'Launch instance' button.

Resource	Count
Instances (running)	0
Instances	0
Placement groups	0
Volumes	0
Dedicated Hosts	
Key pairs	
Security groups	

2. On the **Launch an instance** screen, configure the settings as follows:

- a. Name and tags

The screenshot shows the 'Launch an instance' screen in the AWS Management Console. The breadcrumb navigation shows 'EC2 > Instances > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. Below the heading is a section titled 'Name and tags' with an 'Info' link. The 'Name' field contains the text 'AR4000S-Cloud' and there is an 'Add additional tags' link.

Enter a name for your AMI.

b. Application and OS Images (Amazon Machine Image)

Click the **My AMIs** tab and the AMI you just created should be selected. If a different one is selected, select the AMI you just created from the drop-down list.

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

My AMIs Quick Start

Owned by me Shared with me

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

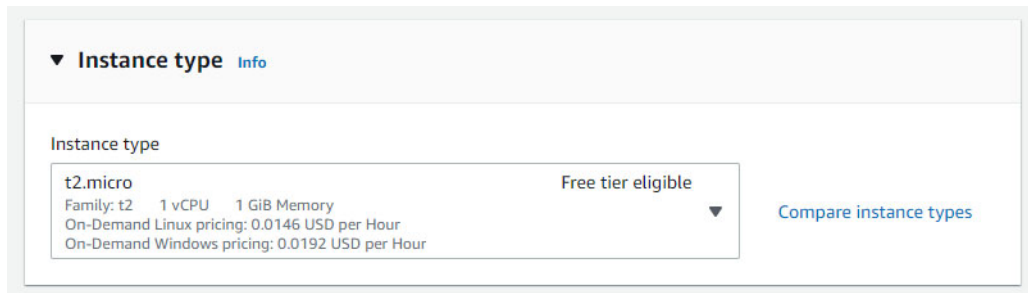
vaa-5.5.2-1.1
ami-05d92637888e52c93
2022-10-05T22:12:47.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Description
-

Architecture	AMI ID
x86_64	ami-05d92637888e52c93

c. Instance type

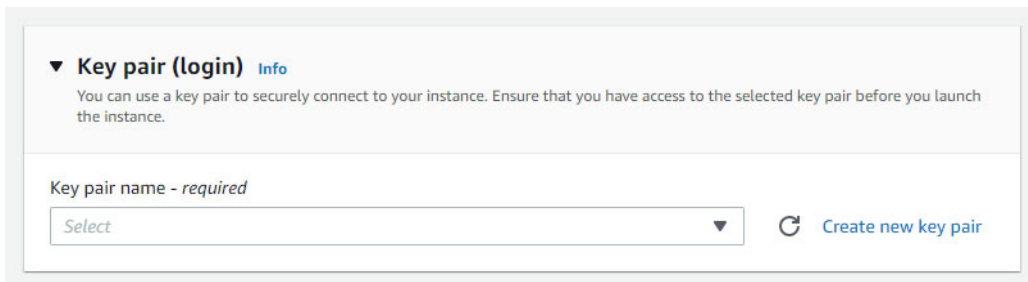
The instance requirements differ depending on the usage environment. Refer to the “[Amazon Web Services \(AWS\)](#)” section and the AWS documentation and select the appropriate instance type.



The screenshot shows the 'Instance type' section of the AWS console. It features a dropdown menu currently set to 't2.micro'. To the right of the dropdown, it indicates 'Free tier eligible' and includes a 'Compare instance types' link. Below the dropdown, the following specifications are listed: 'Family: t2', '1 vCPU', and '1 GiB Memory'. Pricing information is also provided: 'On-Demand Linux pricing: 0.0146 USD per Hour' and 'On-Demand Windows pricing: 0.0192 USD per Hour'.

d. Key Pair (Login)

Caution: The key pair creation here is not used by the AR4000S-Cloud. For details about creating an SSH key pair to secure your connection, refer to the “[SSH connection settings](#)” section.



The screenshot shows the 'Key pair (login)' section of the AWS console. It includes a sub-header 'Key pair (login)' with an 'Info' link and a descriptive paragraph: 'You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.' Below this, there is a label 'Key pair name - required' and a dropdown menu with 'Select' as the current option. To the right of the dropdown is a 'Create new key pair' button with a refresh icon.

e. Network settings

Click **Edit** and configure as follows:

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0d2145b3c4f0742b8 (Main-VPC) [↻](#)
172.30.0.0/16

Subnet [Info](#)

subnet-0cea7c4e8481c3464 **Main-Subnet** [↻](#) [Create new subnet](#)
VPC: vpc-0d2145b3c4f0742b8 Owner: 259623944249
Availability Zone: ap-southeast-2b IP addresses available: 251 CIDR: 172.30.0.0/24

Auto-assign public IP [Info](#)

Enable [↻](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&!;\$*

Description - required [Info](#)

launch-wizard-1 created 2022-10-06T00:48:22.230Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0, Allow SSH) [Remove](#)

Type Info	Protocol Info	Port range Info
ssh ↻	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere ↻	<input type="text" value="0.0.0.0/0"/> ✕	Allow SSH

▼ Security group rule 2 (All, All, 192.168.1.0/24, Allow From User Network) [Remove](#)

Type Info	Protocol Info	Port range Info
All traffic ↻	All	All
Source type Info	Source Info	Description - optional Info
Custom ↻	<input type="text" value="192.168.1.0/24"/> ✕	Allow From User Network

Select the VPC that you created earlier.

Click **Create new subnet**.

Network settings [Info](#)

VPC - required [Info](#)

vpc-0d2145b3c4f0742b8 (Main-VPC)
172.30.0.0/16

Subnet info

Select [Create new subnet](#)

Auto-assign public IP [Info](#)

Select

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .-:/()#,@[]+=&;!\$*

Description - required [Info](#)

launch-wizard-1 created 2022-10-06T00:48:22.230Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere	<input type="text" value="0.0.0.0/0"/> Add CIDR, prefix list or security group	e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Add security group rule](#)

The **Create subnet** screen will be displayed. Set as follows and click **Create subnet**.

VPC

VPC ID
Create subnets in this VPC.

vpc-0d2145b3c4f0742b8 (Main-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
172.30.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Main-Subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 CIDR block [Info](#)

172.30.0.0/24 X

▼ **Tags - optional**

Key	Value - optional	
Name X	Main-Subnet X	Remove

Add new tag

You can add 49 more tags.

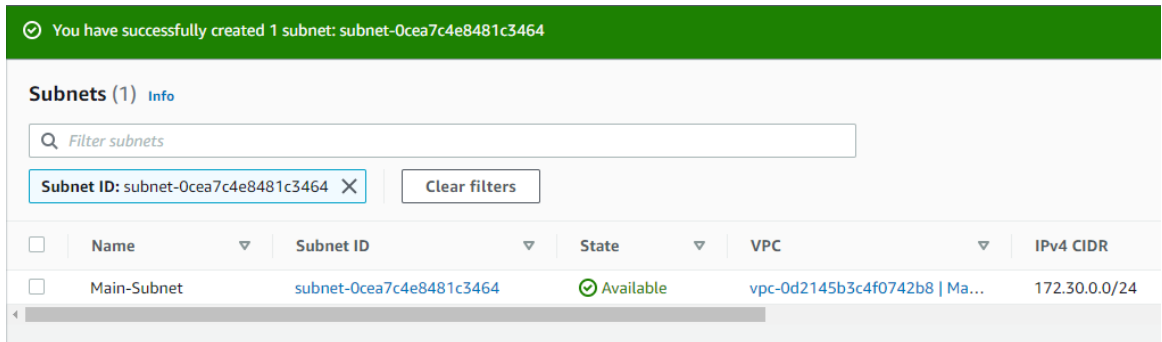
Remove

Add new subnet

Cancel **Create subnet**

A screen similar to the following appears when the subnet is successfully created.

Note: You may need to refresh the subnet list after creation is complete to have your new subnet appear.



✔ You have successfully created 1 subnet: subnet-0cea7c4e8481c3464

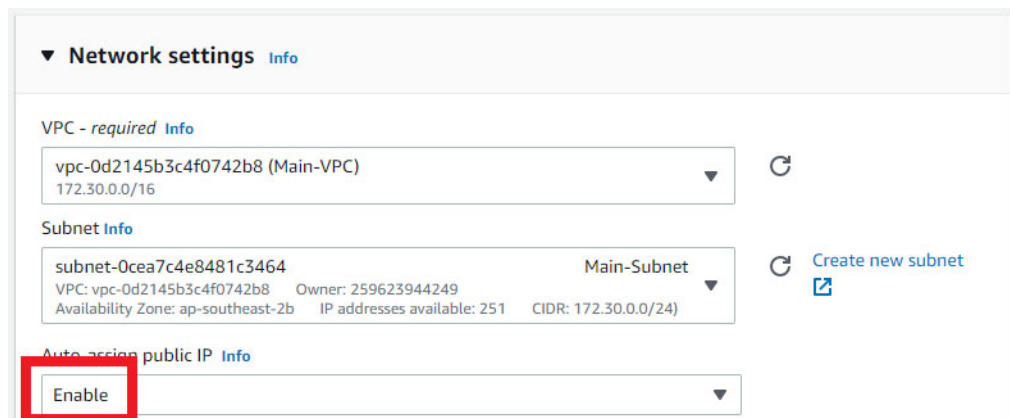
Subnets (1) [Info](#)

Filter subnets

Subnet ID: subnet-0cea7c4e8481c3464 [Clear filters](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Main-Subnet	subnet-0cea7c4e8481c3464	✔ Available	vpc-0d2145b3c4f0742b8 Ma...	172.30.0.0/24

Select **Enable** for automatic public IP assignment



Network settings [Info](#)

VPC - required [Info](#)

vpc-0d2145b3c4f0742b8 (Main-VPC)
172.30.0.0/16

Subnet [Info](#)

subnet-0cea7c4e8481c3464 Main-Subnet
VPC: vpc-0d2145b3c4f0742b8 Owner: 259623944249
Availability Zone: ap-southeast-2b IP addresses available: 251 CIDR: 172.30.0.0/24

Auto-assign public IP [Info](#)

Enable

Select **Create Security Group**.

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your

Create security group Select existing security group

Security group name - *required*
launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;!\$*

Description - *required* Info
launch-wizard-1 created 2022-10-06T00:48:22.230Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

Type Info ssh	Protocol Info TCP	Port range Info 22
Source type Info Anywhere	Source Info Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - <i>optional</i> Info e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

Add security group rule

Click on **Add security group rule**. Configure two security group rules as below.

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0, Allow SSH) Remove

Type Info ssh	Protocol Info TCP	Port range Info 22
Source type Info Anywhere	Source Info Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - <i>optional</i> Info Allow SSH

▼ Security group rule 2 (All, All, 192.168.1.0/24, Allow From User Network) Remove

Type Info All traffic	Protocol Info All	Port range Info All
Source type Info Custom	Source Info Add CIDR, prefix list or security group 192.168.1.0/24 X	Description - <i>optional</i> Info Allow From User Network

f. Configure storage and Advanced details

You can leave the defaults for these sections.

▼ **Configure storage** [Info](#) Advanced

1x GiB ▼ Root volume

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

0 x File systems Edit

▶ **Advanced details** [Info](#)

3. Click **Launch Instance**.

▼ **Summary**

Number of instances [Info](#)

[Software Image \(AMI\)](#)
vaa-5.5.2-1.1
ami-05d92637888e52c93

[Virtual server type \(instance type\)](#)
t2.micro

[Firewall \(security group\)](#)
New security group

[Storage \(volumes\)](#)
1 volume(s) - 10 GiB

4. If the instance is successfully created, you will see a screen like the one below.

EC2 > Instances > Launch an instance

✔ Success
Successfully initiated launch of instance (i-03f75350c8151dddb)

[▶ Launch log](#)

Next Steps

Get notified of estimated charges
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)

How to connect to your instance
Your instance is launching and it might be a few minutes until it is in the running state, when it will be ready for you to use
Click [View Instances](#) to monitor your instance's status. Once your instance is in the 'running' state, you can connect to it from the Instances screen. Find out [how to connect to your instance](#)

[View more resources to get you started](#)

[View all instances](#)

You can also check the public IP address of the instance used for SSH connection, as well as other settings, on the following screen.

EC2 > Instances > i-03f75350c8151dddb

Instance summary for i-03f75350c8151dddb (AR4000S-Cloud) Refresh Connect Instance state Actions

Updated less than a minute ago

Instance ID i-03f75350c8151dddb (AR4000S-Cloud)	Public IPv4 address 54.250.131.1* open address	Private IPv4 addresses 172.30.0.145
IPv6 address -	Instance state ✔ Running	Public IPv4 DNS -
Hostname type IP name: ip-172-30-0-145.ap-southeast-2.compute.internal	Private IP DNS name (IPv4 only) ip-172-30-0-145.ap-southeast-2.compute.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 54.250.131.1 [Public IP]	VPC ID vpc-0d2145b3c4f0742b8 (Main-VPC)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0cea7c4e8481c3464 (Main-Subnet)	

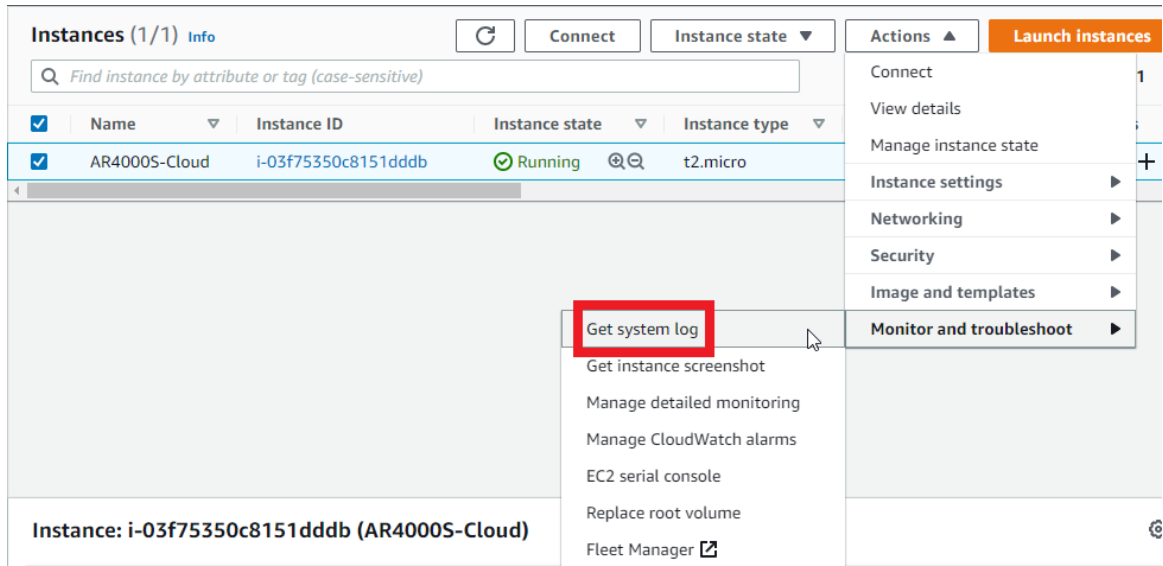
Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ Instance details Info

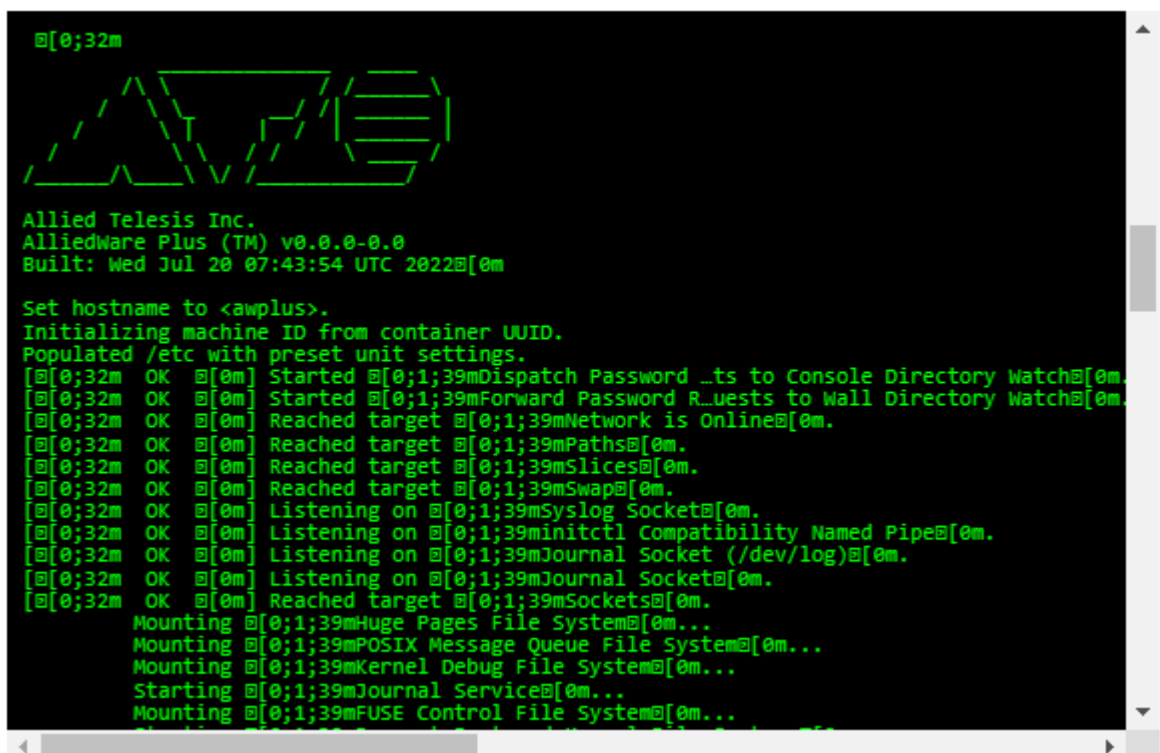
Platform Linux/UNIX (Inferred)	AMI ID ami-05d92637888e52c93	Monitoring disabled
Platform details Linux/UNIX	AMI name vaa-5.5.2-1.1	Termination protection Disabled
Stop protection Disabled	Launch time Thu Oct 06 2022 14:41:39 GMT+1300 (New Zealand Daylight Time) (1 minute)	AMI location 259623944249/vaa-5.5.2-1.1
Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled
AMI Launch index	Key pair name	State transition reason

Note: AWS does not provide a virtual console to access your instances. Control of the instance is only possible via SSH. However, it is possible to view messages output to the internal console of AR4000S-Cloud as read-only logs.

To do this, open the **EC2** dashboard screen by clicking **Services > All services > EC2**. Click **Instances** under **Instances** from the left menu. Select the instance you created earlier, then select **Actions > Monitor and troubleshoot > Get system log** at the top of the screen.



A read-only log is displayed, so confirm that the message at startup is displayed as follows.

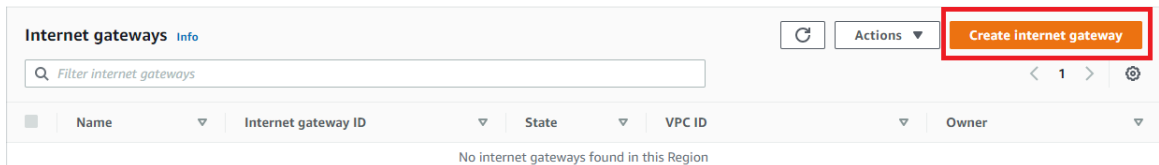


If you don't see anything in the read-only log, wait a few minutes and try refreshing the display. Log files are not updated in real time; they are updated according to a refresh timer determined by AWS.

Create and configure an internet gateway

VPCs are not connected to the Internet by default. To enable communication between your VPC and the Internet, you need to create an Internet gateway, attach it to your VPC, and set a default route in your VPC's route table by following the steps below.

1. From the AWS Management Console's **Services** menu, select **All Services** > **VPC** to open the VPC dashboard screen. On the left menu, under **Virtual private cloud**, click **Internet gateway**. Click **Create internet gateway**.



2. The **Create internet gateway** screen will be displayed. Enter the following information and click **Create internet gateway**.

The screenshot shows the 'Create internet gateway' configuration screen. The breadcrumb navigation is 'VPC > Internet gateways > Create internet gateway'. The main heading is 'Create internet gateway' with an 'Info' link. Below the heading is a description: 'An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.' The form is divided into two sections: 'Internet gateway settings' and 'Tags - optional'. In the 'Internet gateway settings' section, there is a 'Name tag' field with the value 'AR4000S-Cloud-Gateway'. In the 'Tags - optional' section, there is a table with one tag: Key 'Name' and Value 'AR4000S-Cloud-Gateway'. At the bottom right, the 'Create internet gateway' button is highlighted with a red box.

- When the Internet gateway is successfully created, the following screen will be displayed. Click **Attach to a VPC** in the upper right.

The screenshot shows the AWS console interface for an Internet Gateway. At the top, a green notification bar states: "The following internet gateway was created: igw-02c84d9093fdcbbd1 - AR4000S-Cloud-Gateway. You can now attach to a VPC to enable the VPC to communicate with the internet." In the top right corner of this bar, the button "Attach to a VPC" is highlighted with a red rectangle. Below the notification, the breadcrumb navigation shows "VPC > Internet gateways > igw-02c84d9093fdcbbd1". The main heading is "igw-02c84d9093fdcbbd1 / AR4000S-Cloud-Gateway" with an "Actions" dropdown menu. The "Details" section includes a table with the following information:

Internet gateway ID	State	VPC ID	Owner
igw-02c84d9093fdcbbd1	Detached	-	259623944249

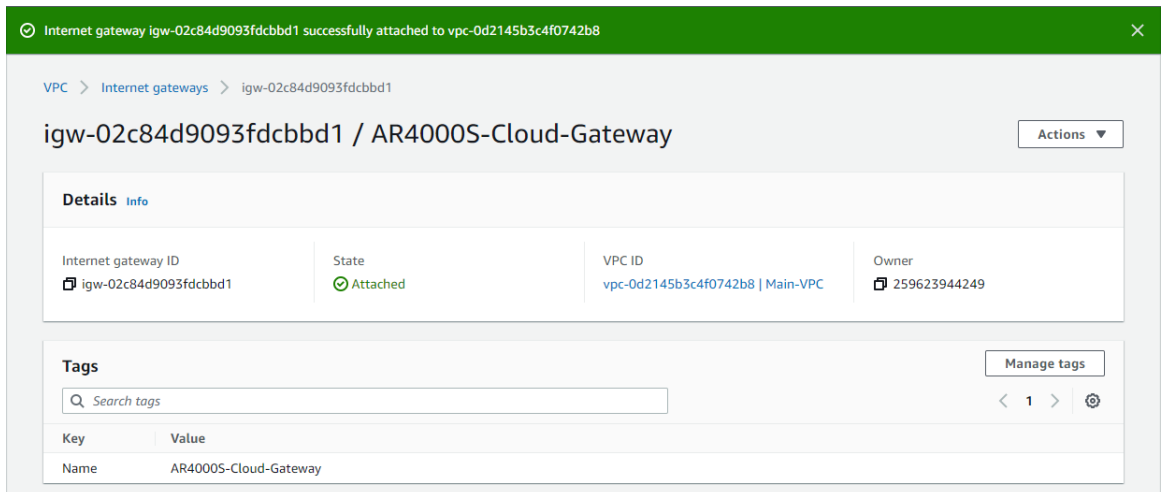
The "Tags" section shows a search bar and a table with one tag:

Key	Value
Name	AR4000S-Cloud-Gateway

- The **Attach to VPC** screen will be displayed. Select the VPC you created earlier and click **Attach internet gateway**.

The screenshot shows the "Attach to VPC" screen in the AWS console. The breadcrumb navigation is "VPC > Internet gateways > Attach to VPC (igw-02c84d9093fdcbbd1)". The main heading is "Attach to VPC (igw-02c84d9093fdcbbd1) Info". The "VPC" section contains the instruction: "Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below." The "Available VPCs" section includes a search bar with the text "vpc-0d2145b3c4f0742b8" and a close button. Below this, there is a section for the "AWS Command Line Interface command". At the bottom right, the "Attach internet gateway" button is highlighted with a red rectangle, next to a "Cancel" button.

- The following is displayed when the Internet gateway attachment is successfully completed.



Internet gateway igw-02c84d9093fdcbbd1 successfully attached to vpc-0d2145b3c4f0742b8

VPC > Internet gateways > igw-02c84d9093fdcbbd1

igw-02c84d9093fdcbbd1 / AR4000S-Cloud-Gateway

Details info

Internet gateway ID igw-02c84d9093fdcbbd1	State Attached	VPC ID vpc-0d2145b3c4f0742b8 Main-VPC	Owner 259623944249
--	-------------------	--	-----------------------

Tags Manage tags

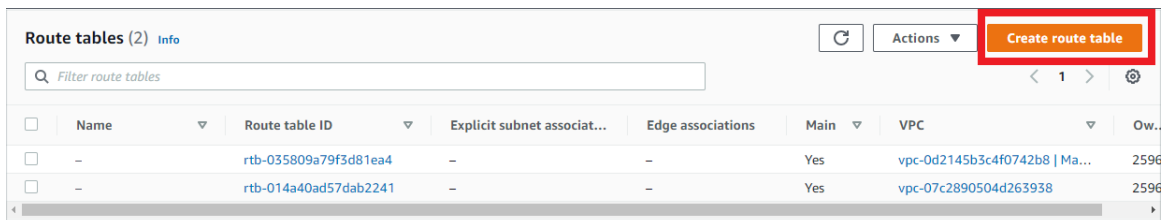
Search tags

Key	Value
Name	AR4000S-Cloud-Gateway

Create a route table

Next, create a route table, register a default route, and configure settings to allow communication from the VPC to the Internet via the Internet gateway.

- On the left menu of the VPC dashboard, under **Virtual private cloud** click **Route tables**. Click **Create route table**.



Route tables (2) info

Filter route tables

Create route table

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow...
<input type="checkbox"/>	-	rtb-035809a79f3d81ea4	-	-	Yes	vpc-0d2145b3c4f0742b8 Ma...	2596
<input type="checkbox"/>	-	rtb-014a40ad57dab2241	-	-	Yes	vpc-07c2890504d263938	2596

2. The **Create route table** screen will be displayed. Enter the following information and click **Create route table**.

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="Main-VPC-Route-Table"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

3. When the route table is created successfully, the following screen will be displayed.

The screenshot shows the AWS Management Console interface for a route table. At the top, a green notification bar states: "Route table rtb-067fef6aea4cf3b6c | Main-VPC-Route-Table was created successfully." Below this, the breadcrumb navigation is "VPC > Route tables > rtb-067fef6aea4cf3b6c". The main heading is "rtb-067fef6aea4cf3b6c / Main-VPC-Route-Table" with an "Actions" dropdown menu. A blue notification box says: "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. The "Details" section shows the following information:

Route table ID rtb-067fef6aea4cf3b6c	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0d2145b3c4f0742b8 Main-VPC	Owner ID 259623944249		

Below the details are tabs for "Routes", "Subnet associations", "Edge associations", "Route propagation", and "Tags". The "Routes" tab is active, showing a table with one route:

Destination	Target	Status	Propagated
172.30.0.0/16	local	Active	No

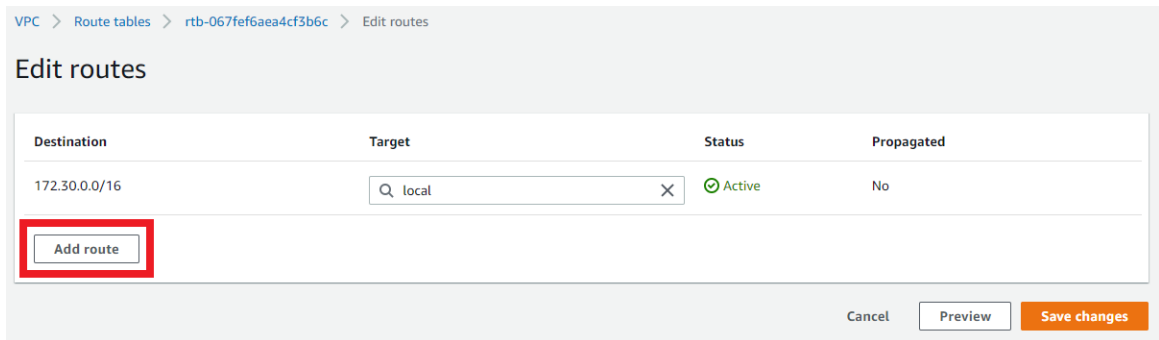
4. On the left menu, under **Virtual private cloud** click **Route tables**. Select the route table you created earlier, click the **Route** tab, and click **Edit Route**.

The screenshot shows the "Route tables (1/3)" page in the AWS Management Console. A search bar is at the top. Below it is a table listing route tables:

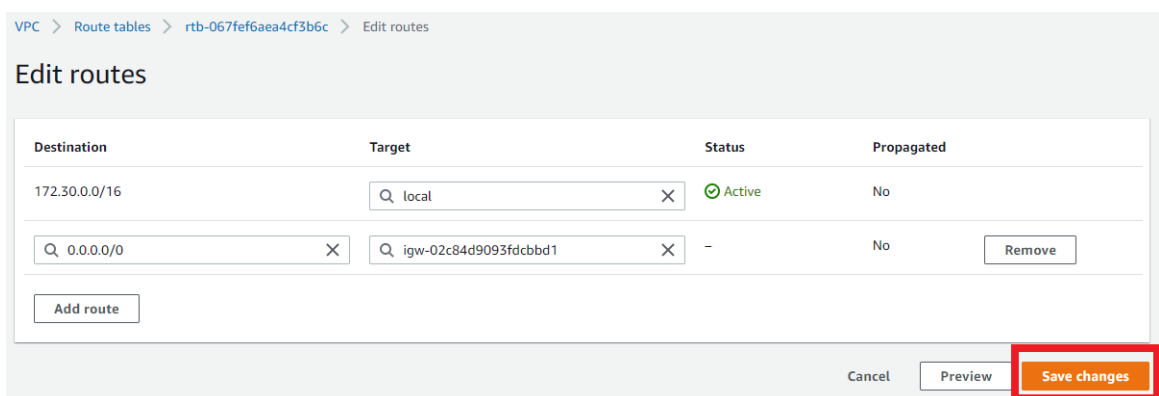
Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
-	rtb-035809a79f3d81ea4	-	-	Yes	vpc-0d2145b3c4f0742b8 Ma...	259623944249
-	rtb-014a40ad57dab2241	-	-	Yes	vpc-07c2890504d263938	259623944249
Main-VPC-Route-Ta...	rtb-067fef6aea4cf3b6c	-	-	No	vpc-0d2145b3c4f0742b8 Ma...	259623944249

The "Main-VPC-Route-Ta..." row is selected. Below the table, the "Routes" tab is highlighted in red. The "Routes" section shows the same table as in the previous screenshot. The "Edit routes" button is highlighted in red.

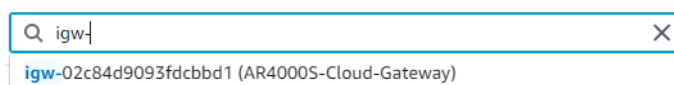
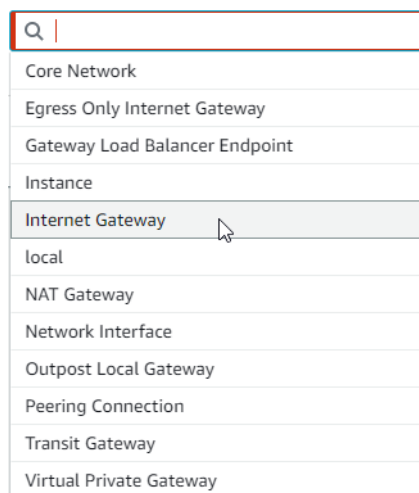
5. The **Edit routes** screen will be displayed. Click **Add route**.



6. Configure additional routes as below and click **Save changes**.



In the **Target** drop-down, if you select **Internet Gateway**, the Internet gateway created earlier will be displayed. Select it.



7. When the route editing is successfully completed, the following screen will be displayed.

8. On the left menu, under **Virtual private cloud** click **Route tables**. Select the route table you just created, and then click **Action > Set main route table**.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
-	rtb-035809a79f3d81ea4	-	-	Yes	vpc-0d2145b3c4f0742b8 Ma...	259623944249
-	rtb-014a40ad57dab2241	-	-	Yes	vpc-07c2890504d263938	259623944249
✓ Main-VPC-Route-Ta...	rtb-067fef6aea4cf3b6c	-	-	No	vpc-0d2145b3c4f0742b8 Ma...	259623944249

9. When the **Set main route table** screen appears, enter “set” and click **OK**.

Set main route table ✕

Main route table controls the routing for all subnets that are not explicitly associated with any other route table. Are you sure you want to set this route table as the main route table?

- rtb-067fef6aea4cf3b6c / Main-VPC-Route-Table

To confirm setting, type set in the field.

Cancel
OK

10. When the main route table configuration is completed successfully, the following screen will be displayed.

You successfully set the route table `rtb-067fef6aea4cf3b6c` / Main-VPC-Route-Table as main.

Route tables (3) [Info](#)

Actions Create route table

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	rtb-035809a79f3d81ea4	-	-	No	vpc-0d2145b3c4f0742b8 Ma...	259623944249
<input type="checkbox"/>	-	rtb-014a40ad57dab2241	-	-	Yes	vpc-07c2890504d263938	259623944249
<input type="checkbox"/>	Main-VPC-Route-Ta...	rtb-067fef6aea4cf3b6c	-	-	Yes	vpc-0d2145b3c4f0742b8 Ma...	259623944249

SSH connection settings

Since AWS does not provide console access to instances (virtual machines), configuration and management of this product on AWS must be done via SSH (Secure Shell).

Note: Any SSH private keys generated by AWS are not used by AR4000S-Cloud. A freshly created AR4000S-Cloud will ignore any AWS generated SSH key pairs, and instead use password authentication with default credentials. Further, any authentication methods configured via AWS will be ignored by AR4000S-Cloud. For example, the "[Key Pair \(Login\)](#)" on page 16 created by AWS will not be used by AR4000S-Cloud.

This section describes how to access the CLI of this product with public key authentication using an SSH key pair, using "PuTTY" for Windows and the ssh command for Ubuntu (Linux) as an SSH client.

SSH key pair

A cryptographic method that uses different keys for data encryption and decryption is called **asymmetric cryptography**, and the two keys used in that method are collectively called a **key pair** or **public key pair**. In asymmetric cryptography, data encrypted with one key of a key pair can only be decrypted with the other key of the pair.

SSH supports **public key authentication** using this property, and the key pair used in this authentication method is called an **SSH key pair**.

An SSH key pair consists of two keys:

- Public Key

A **public key** is a key that does not need to be kept secret. With SSH public key authentication, the user's public key is installed in advance on the access destination host (server, etc.). Public keys can be made public, so it's okay to install the same public key on multiple hosts.

In this product, the public key of the key pair set at the time of instance creation is automatically installed as the public key for the manager user at the time of initial startup. You can log in to this product as a manager user.

- Private Key

A **private key** is a key that is kept securely by its owner and should never be disclosed to anyone else. Since the private key is the only key that can decrypt data encrypted with the public key, the server takes advantage of this property in SSH public key authentication. This allows the server to compare the accessing user's key with the public key installed on the server, determine whether they possess the correct private key, and grant or deny access based on that result.

To access an instance of this product via SSH, you need to configure your SSH client software to authenticate using the private key that corresponds to the public key you entered when creating the instance.

Accessing this product via SSH using "PuTTY"

The following explains how to create an SSH private key in "PuTTY", a typical SSH client for Windows, and connect to this product via SSH.

For more details, please refer to the user guides for AWS and PuTTY.

Prerequisite

Download and install PuTTY from putty.org. The MSI installer or ZIP archive contain PuTTY and all of its companion utilities. You can also download each program individually. You will need to download at least the following programs:

- `putty.exe` (used for SSH connection)
- `puttygen.exe` (used to create a PPK format private key file)

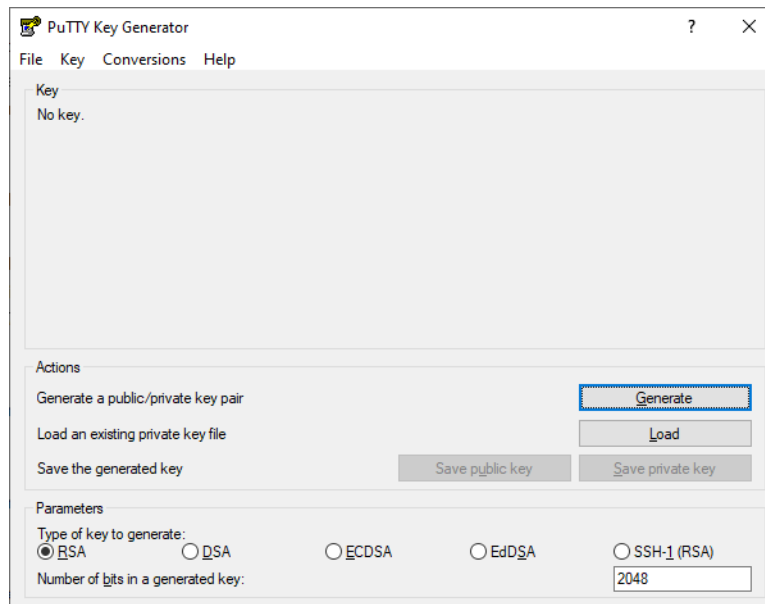
Create an SSH PPK key pair with PuTTYgen

You need a PPK private key pair, created using a utility called PuTTYgen.

1. Start PuTTYgen by one of the following methods:

- In the Start menu, click **All Programs > PuTTY > PuTTYgen**
- At the Run prompt, enter "`c:\Program Files\PuTTY\puttygen.exe`"

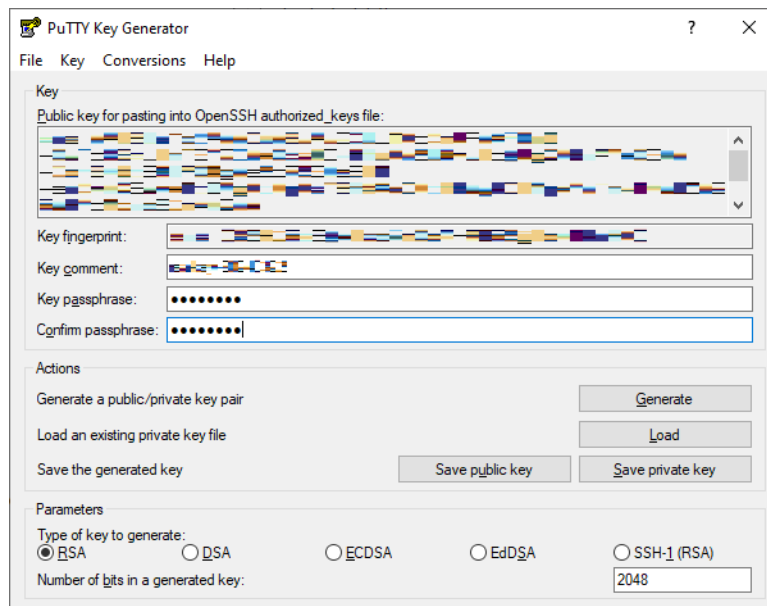
The PuTTY Key Generator window will appear.



2. Make sure that the **RSA** radio button is selected under **Parameters**. Click the **Generate** button.
3. Move your mouse in the blank area below the progress bar until the progress bar is filled. This may take some time.
4. Change the **Key comment** to identify the new key.
5. Set a passphrase.

Enter a passphrase to protect your private key in the **Key passphrase** field.

If you set a passphrase here, even if someone else obtains the private key, they will not be able to use it unless they enter the passphrase.



6. Export PPK format public and private key files

Click the **Save public key** button above. A new window will open. Specify the save destination and file name of the PPK format public key.

Click the **Save private key** button. Repeat the process, and save the destination and file name of the PPK format private key.

You now have a public and private SSH key pair that can be used with PuTTY.

Configure SSH in Vista Manager

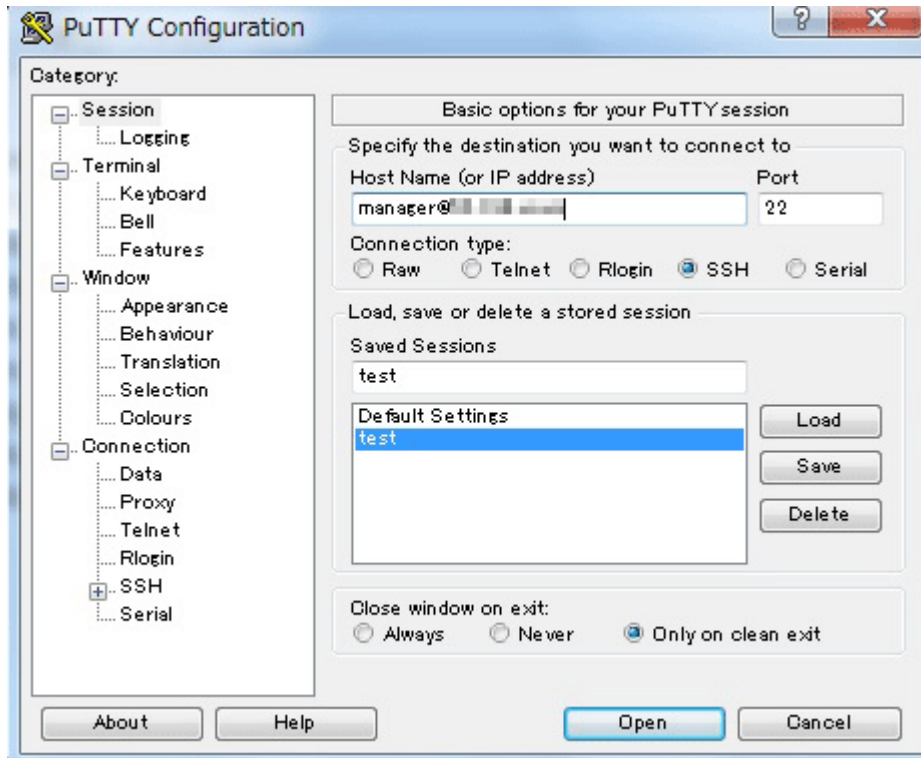
You then need to configure SSH in Vista Manager to allow SSH connections. Configuring SSH and installing the PPK keys is beyond the scope of this document; you can find information on how to configure SSH in the [Secure Shell \(SSH\) Feature Overview and Configuration Guide](#).

Make an SSH connection to Vista Manager using PuTTY and PPK private key

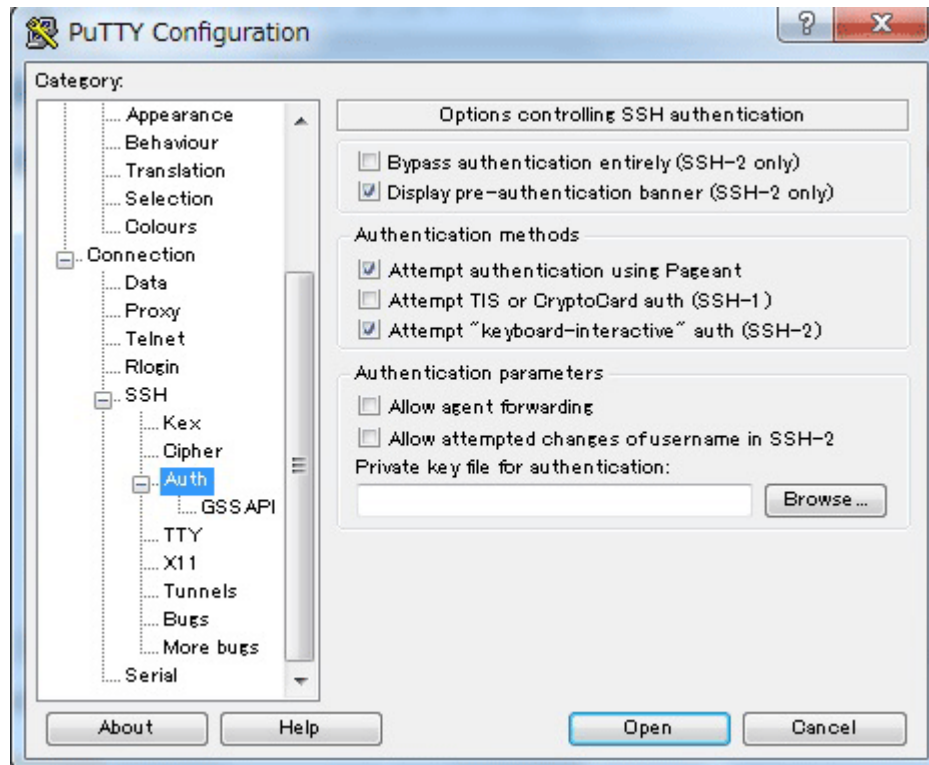
Once you have configured SSH, you can connect to your instance using PuTTY.

1. When PuTTY is opened, a window like the one shown below will be displayed. Enter “manager@ (the public IP address of this instance)” in the **Host Name** field.

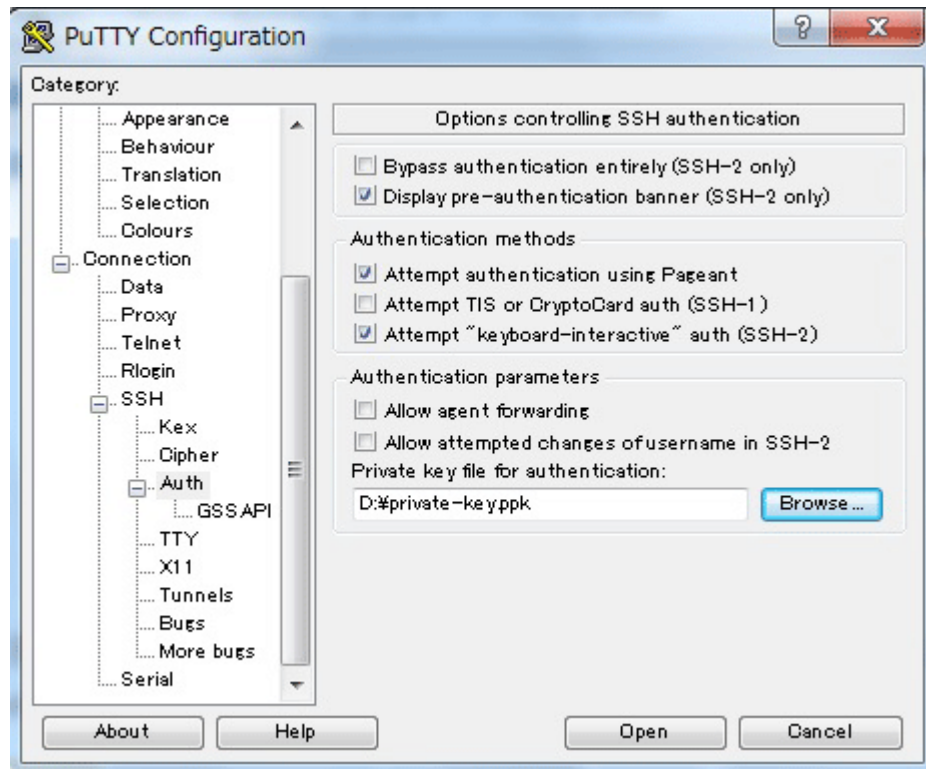
Note: You can check the public IP address from the instance screen of the EC2 dashboard.



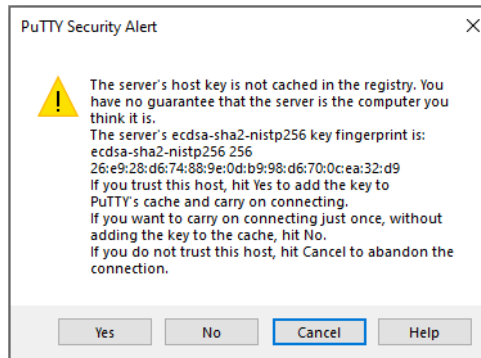
- Next, click **Connection > SSH > Auth** in the left panel.



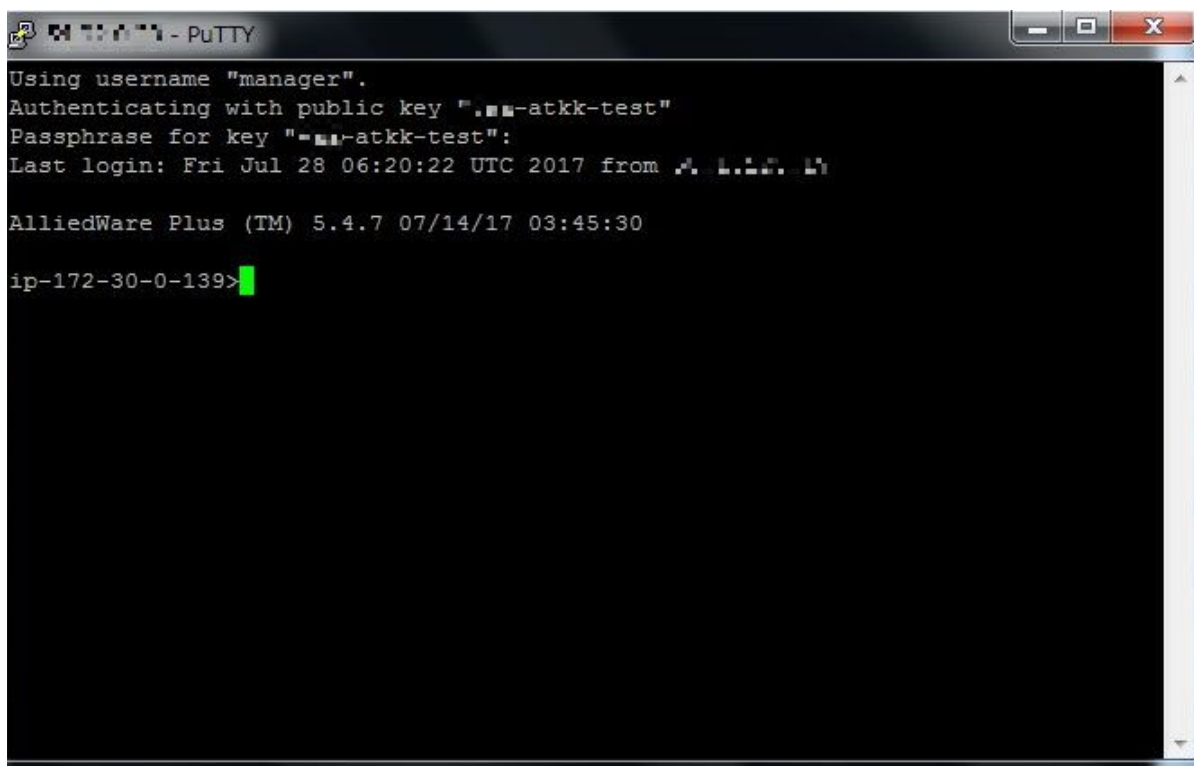
- Click the **Browse** button. Specify the PPK file of the private key saved earlier. Click **Open** to start an SSH session.



4. If this is your first time connecting to an instance of the product, a security alert dialog box will appear asking if you trust the host you are connecting to. Click **Yes** to save the key to your cache.



5. This completes the SSH connection to this product and displays the AlliedWare Plus CLI screen.



SSH connection to this product using SSH client of Ubuntu (Linux)

The following describes how to SSH into this product using the standard OpenSSH SSH client in many Linux and UNIX-like environments.

See the man page for the ssh command for more information.

1. In the command shell, move the current directory to the location of the private key file downloaded from AWS when creating the instance.

```
ubuntu@ubuntu-pc:~/tmp$ cd ~/.ssh
```

Note: For security reasons, it is recommended that you set the permissions on the private key file to be read-only for the file owner and inaccessible for everyone else. You can do so with the following commands:

```
ubuntu@ubuntu-pc:~/.ssh$ chmod 400 ar4000s-cloud-atkk-test.pem
ubuntu@ubuntu-pc:~/.ssh$ ls -la ar4000s-cloud-atkk-test.pem
-r----- 1 vaa vaa 1696 Jul 15 15:06 ar4000s-cloud-atkk-test.pem
```

2. Make an SSH connection to the product with the **ssh** command. Use the **-i** option to specify the PEM file downloaded when creating the key pair on AW. **manager** is the default user name, and **XX.XXX.XX.XXX** is the public IP address of the product instance.

Note: You can check the public IP address of the product instance from the instance screen of the EC2 dashboard.

```
ubuntu@ubuntu-pc:~/.ssh$ ssh -i ar4000s-cloud-atkk-test.pem manager@XX.XXX.XX.XXX
```

3. When connecting to the server for the first time, you will be asked to confirm the public key of the server. Type “yes” and press the **Enter** key.

```
The authenticity of host 'XX.XXX.XX.XXX (XX.XXX.XX.XXX)' can't be established.
ECDSA key fingerprint is 7f:4e:5c:04:e2:bc:b1:dc:e5:27:b4:86:17:33:9c:0c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'XX.XXX.XX.XXX' (ECDSA) to the list of known hosts.
```

4. This completes the SSH connection to this product and displays the AlliedWare Plus CLI screen.

```
Last login: Mon Jul 31 05:27:39 UTC 2017 from xx.x.xxx.xx

AlliedWare Plus(TM) 5.5.2 XX/XX/XX XX:XX:XX

ip-172-30-0-139>
```

Connecting to your local network

In order to use this product from the local network, it is necessary to connect AWS (VPC) and the local network. There are two ways to do this:

- Build an IPsec tunnel between the AR4000S-Cloud itself and the local network's VPN router.
- Build an IPsec tunnel between the AWS virtual private gateway and the VPN router on the local network.

The following sections will describe each method using our AT-AR4050S (hereafter referred to as “AR router”) as an example of the VPN router on the local network side.

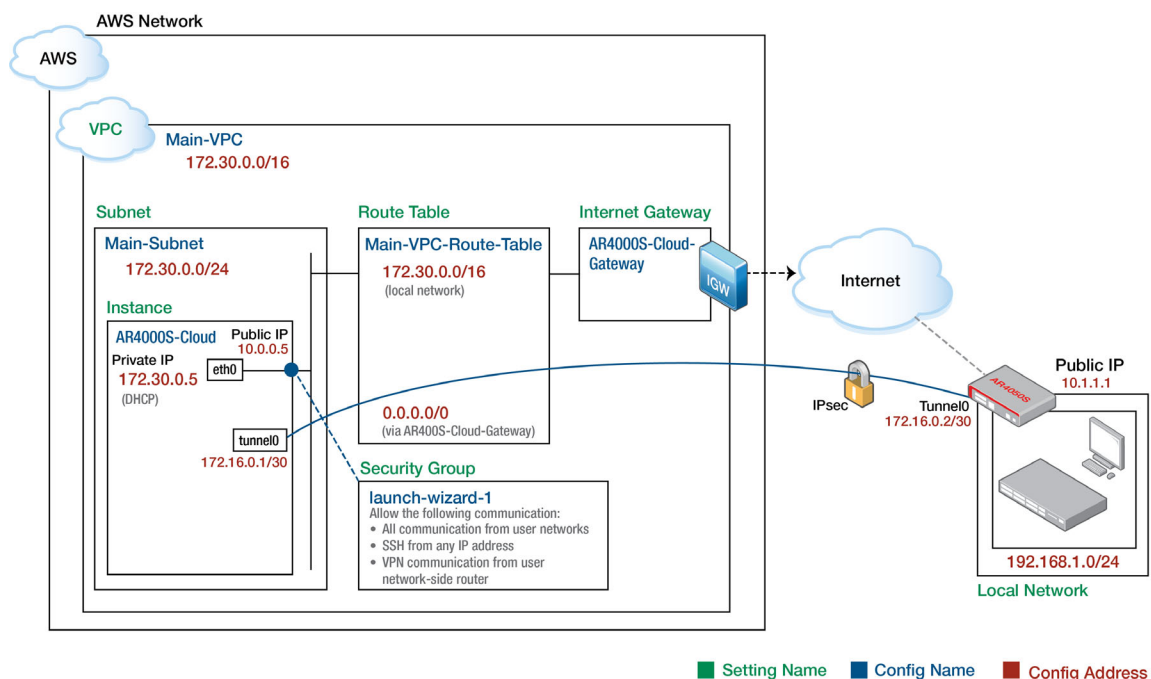
Note: This example assumes that the internet gateway has been set as explained in the “[Create an instance](#)” section.

How to use the VPN function of AR4000S-Cloud

In this configuration, this product itself becomes a VPN router and builds an IPsec tunnel with the VPN router (AR router) on the local network side.

Therefore, VPN connection settings are performed for this product itself. Settings on the AWS (VPC) side, such as a virtual private gateway, are not required, but for the security group, you add a rule to allow VPN communication from the AR router.

Note: The following is an example. Adjust the settings as appropriate to your actual environment.



	This product	AR router
Tunnel interface name	tunnel0	tunnel0
Tunnel operating mode	IPsec (IPv4)	IPsec (IPv4)
Tunnel end address (as viewed from this product)	172.30.0.5 (eth0's private IP)	10.1.1.1 (public IP)
Tunnel end address (as seen from AR router)	10.0.0.5 (instance public IP)	10.1.1.1 (public IP)
Address to set for tunnel I/F	172.16.0.1/30	172.16.0.2/30
ISAKMP Phase 1 ID	vaa0 (host name format string)	10.1.1.1 (IP address)
ISAKMP pre-shared key	abcdefghijklmnopqrstuvwxyz1234	

Note: You can check the public IP address of this product instance from the instance screen of the EC2 dashboard.

Settings on the AWS side

Add an inbound rule that allows VPN communication from the AR router to the security group applied to the instance of this product.

Type	Protocol	Port range	Source	Explanation
Custom UDP rule	UDP	500	10.1.1.1 (public IP address of AR router)	ISAKMP
Custom UDP rule	UDP	4500	10.1.1.1 (public IP address of AR router)	NAT-T (UDP-encap ISAKMP/ESP)

Settings on the AR4000S-Cloud side

This product has a VPN function equivalent to an AR router, so the settings are similar to those of the AR router described later.

However, this product has a private IP address (172.30.0.5) set, and the public IP address (10.0.0.5) of this product has been converted by the NAT function of AWS. In order to correctly identify this product when connecting to ISAKMP, it is necessary to set the tunnel local name to send the name of the local device (host name format string).

1. Set the ISAKMP pre-shared key to be used with the AR router (10.1.1.1). Use the **crypto isakmp** key command for this.

```
crypto isakmp key abcdefghijklmnopqrstuvwxyz1234 address 10.1.1.1
```

2. Create IPsec tunnel interface tunnel0. To do this, create a tunnel interface with the interface command and set the following information:
 - Local side tunnel end address (tunnel source). Specify the eth0 interface of this product
 - Remote side tunnel end address (tunnel destination). Specify the public IP address of the AR router.
 - ISAKMP local name (tunnel local name). Specify a name so that the AR router can identify this product.
 - Tunnelling method (tunnel mode ipsec)
 - Application of IPsec protection to the tunnel interface (tunnel protection ipsec)
 - IP address of the tunnel interface (ip address)
 - MTU of the tunnel interface (mtu)

```
interface tunnel 0
 tunnel source eth0
 tunnel destination 10.1.1.1
 tunnel local name arcloud
 tunnel mode ipsec ipv4
 tunnel protection ipsec
 ip address 172.16.0.1/30
 mtu 1300
```

3. Set a route to the local network (192.168.1.0/24). Use the **ip route** command for this. However, until the VPN connection is enabled, it will be set so that the same route cannot be used.

```
ip route 192.168.1.0/24 tunnel0
ip route 192.168.1.0/24 null 254
```

Settings on the AR router side

Next, configure the VPN settings on the AR router side, which is the VPN router on the local network.

Note: Here we assume that the AR router is connected to the Internet via the ppp0 interface. Also, it is assumed that Internet connection settings and AR4000S-Cloud settings have been completed.

As mentioned above, this product has a private IP address (172.30.0.5), and the public IP address (10.0.0.5) of this product has been converted by the NAT function of AWS. On the router side, it is necessary to specify the same name as that set for this product in the **tunnel remote name** so that this product can be identified correctly during ISAKMP connection.

1. Set the ISAKMP pre-shared key to be used with this product. Use the **crypto isakmp key** command for this.

Since the public IP of this product is actually NAT-converted, this product is identified here by a string ID in the form of a host name.

```
crypto isakmp key abcdefghijklmnopqrstuvwxyz1234 hostname arcloud
```

2. Create IPsec tunnel interface tunnel0. To do this, create a tunnel interface with the interface command and set the following information:
 - Local side tunnel end address (tunnel source). Specify the ppp0 interface of the AR router.
 - Remote side tunnel end address (tunnel destination). Specify the public IP address of this product.
 - ISAKMP remote name (tunnel local name). In order to identify the other party via NAT, specify the same name as set in this product.
 - Tunnelling method (tunnel mode ipsec)
 - Application of IPsec protection to the tunnel interface (tunnel protection ipsec)
 - IP address of the tunnel interface (ip address)
 - MSS rewrite setting on tunnel interface (ip tcp adjust-mss)
 - MTU of tunnel interface (mtu)

```
interface tunnel 0
 tunnel source ppp0
 tunnel destination 10.0.0.5
 tunnel remote name arcloud
 tunnel mode ipsec ipv4
 tunnel protection ipsec
 ip address 172.16.0.2/30
 ip tcp adjust-mss 1260
 mtu 1300
```

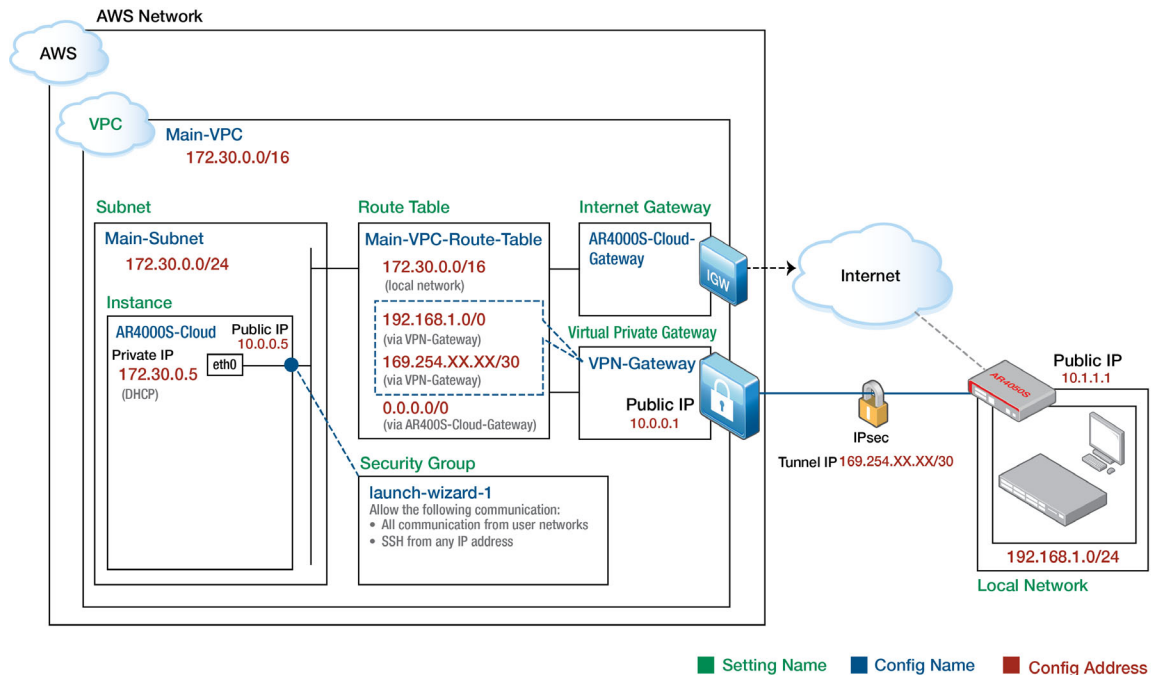
3. Set the route to this product (172.30.0.5/32). Use the **ip route** command for this. However, until the VPN connection is enabled, it will be set so that the same route cannot be used.

```
ip route 172.30.0.5/32 tunnel0
ip route 172.30.0.5/32 null 254
```

At this point, IP communication between this product on AWS and the local network can be established.

How to use AWS (VPC) VPN function

The basic configuration for connecting a VPC and a local network using the VPN function of AWS (VPC) is as follows.



This configuration utilizes a virtual private gateway provided by AWS (VPC) as a VPN router. Therefore, VPN connection settings are made for AWS (VPC). No settings are required on the product side.

Settings on the AWS side

The AWS-side components required to establish a VPN connection between AWS and your network are:

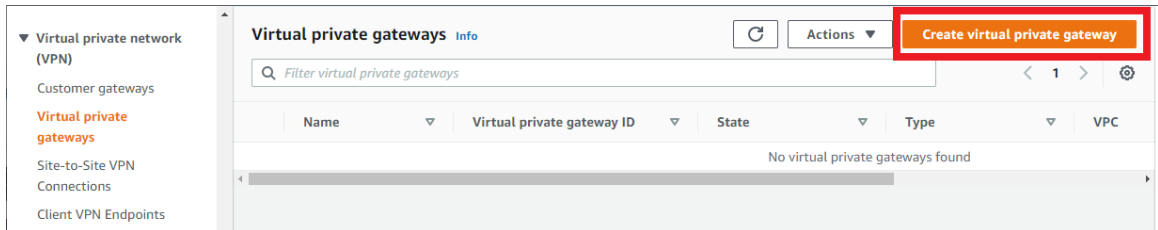
- Virtual Private Gateway - Virtual VPN router on AWS side
- VPN connection - A collection of information necessary for VPN connection between AWS and local network

For more information on VPN terminology in AWS (VPC), please refer to Amazon's user guide.

Create a virtual private gateway

Create a virtual private gateway which is a VPN router on the AWS side.

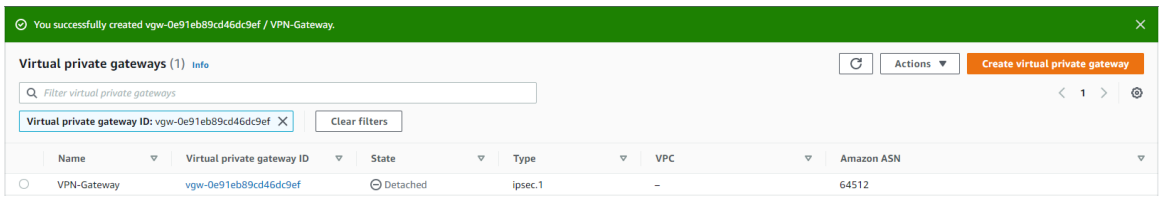
1. From the **Services** menu of the AWS Management Console, select **All Services** > **VPC** to open the VPC dashboard screen. Then, from the left menu, select **Virtual private gateways** under **Virtual private network (VPN)**, then click **Create virtual private gateway**.



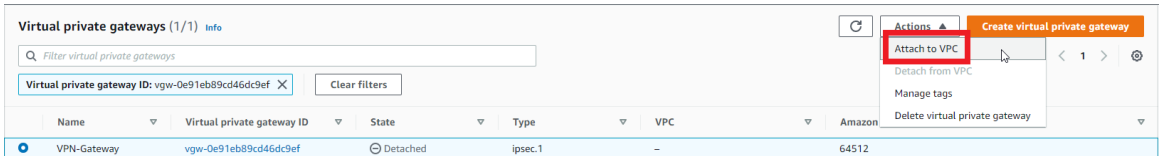
2. The **Create virtual private gateway** screen will be displayed. Set as follows and click **Create virtual private gateway**.

 A screenshot of the 'Create virtual private gateway' configuration page. The breadcrumb trail is 'VPC > Virtual private gateways > Create virtual private gateway'. The page title is 'Create virtual private gateway' with an 'Info' link. Below the title is a descriptive sentence: 'A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.' The form is divided into two sections: 'Details' and 'Tags'. In the 'Details' section, there is a 'Name tag - optional' field with the value 'VPN-Gateway' and a note that the value must be 256 characters or less. Below this is the 'Autonomous System Number (ASN)' section, where 'Amazon default ASN' is selected with a radio button. The 'Tags' section explains that a tag is a label with a key and an optional value. It shows a list of tags with a key of 'Name' and a value of 'VPN-Gateway', and an 'Add new tag' button. At the bottom right, there are 'Cancel' and 'Create virtual private gateway' buttons, with the latter highlighted by a red box.

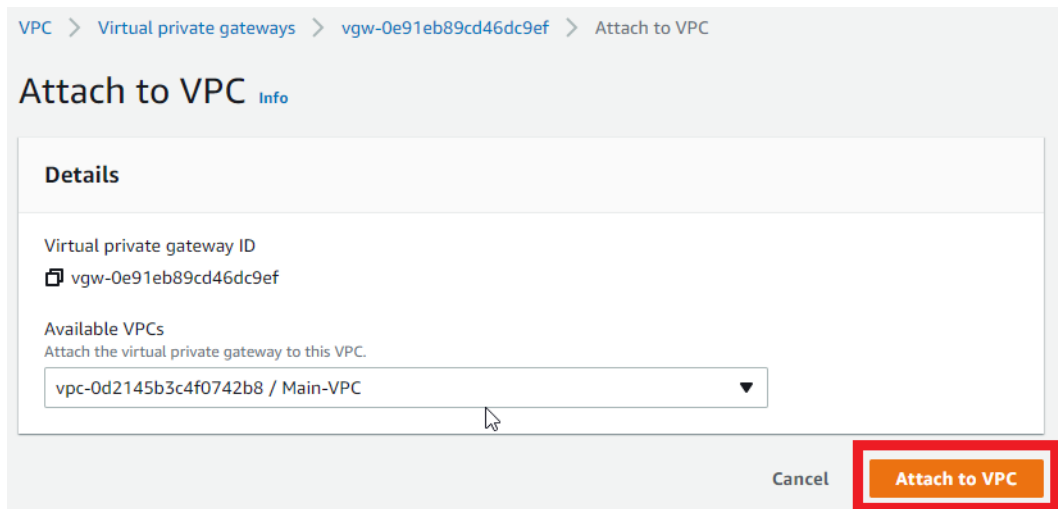
3. If the virtual private gateway is successfully created, you will see a screen like the one below.



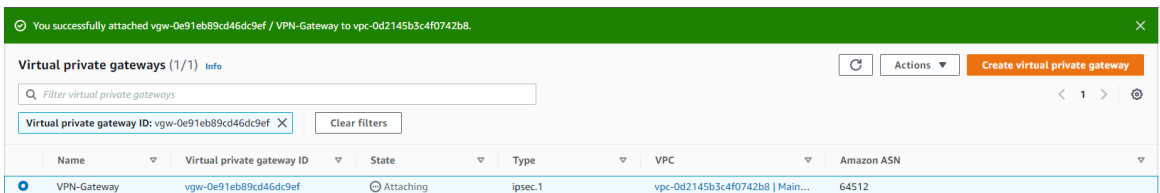
4. Select **Actions** and click **Attach to VPC**.



5. The **Attach to VPC** screen will be displayed. Select the VPC you created earlier and click **Attach to VPC**.

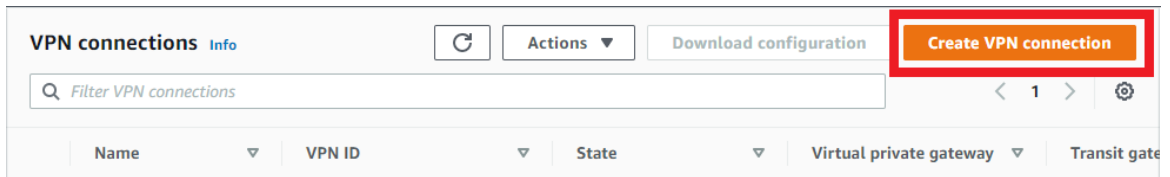


6. When the attachment to the VPC is completed successfully, the following screen will be displayed.

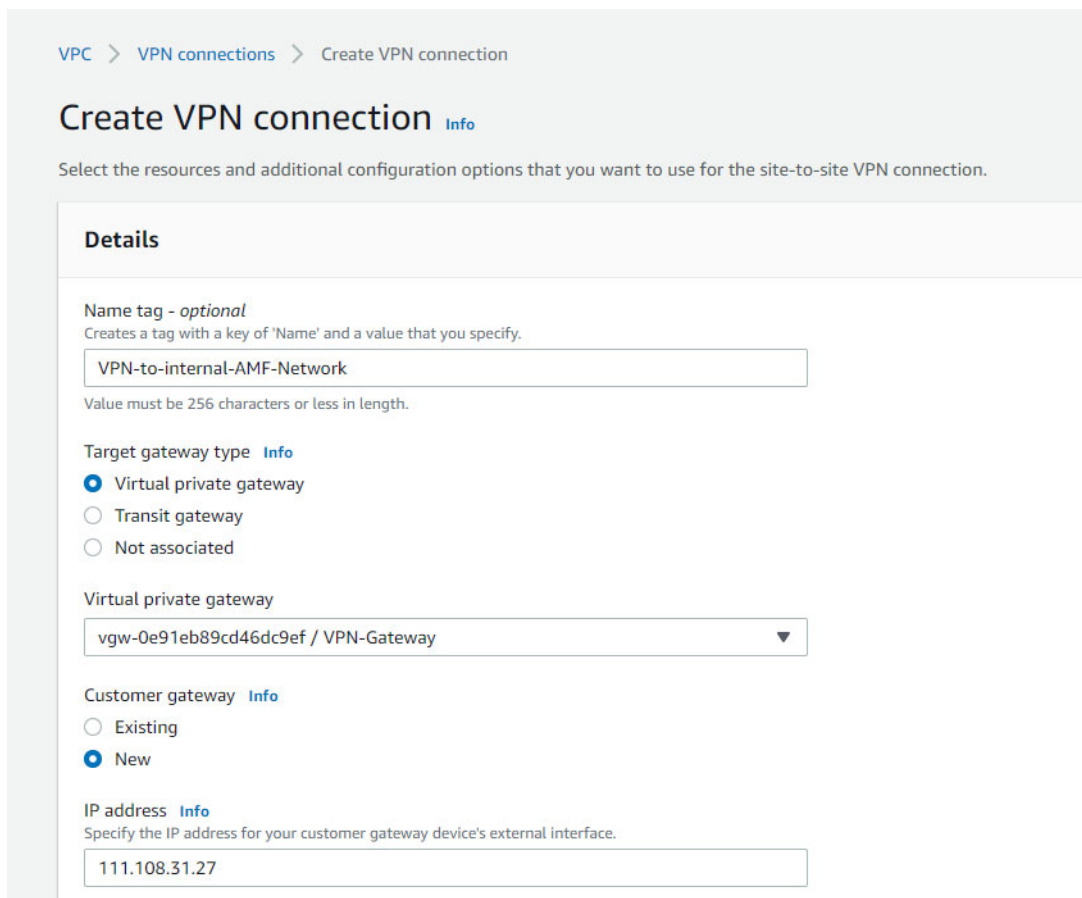


Create a VPN connection

1. From the left menu of the VPC dashboard screen, click **Site-to-Site VPN Connections** under **Virtual private network (VPN)** and click **Create VPN connection**.



2. The **Create VPN connection** screen will be displayed. Set as follows and click **Create VPN connection**.

A screenshot of the 'Create VPN connection' configuration screen in the AWS VPC console. The breadcrumb trail is 'VPC > VPN connections > Create VPN connection'. The main heading is 'Create VPN connection' with an 'Info' link. Below the heading is the instruction: 'Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.' The configuration is organized into a 'Details' section with the following fields:

- Name tag - optional**: A text input field containing 'VPN-to-internal-AMF-Network'. Below it, a note says 'Value must be 256 characters or less in length.'
- Target gateway type**: Three radio button options: 'Virtual private gateway' (selected), 'Transit gateway', and 'Not associated'.
- Virtual private gateway**: A dropdown menu showing 'vgw-0e91eb89cd46dc9ef / VPN-Gateway'.
- Customer gateway**: Two radio button options: 'Existing' and 'New' (selected).
- IP address**: A text input field containing '111.108.31.27'. Below it, a note says 'Specify the IP address for your customer gateway device's external interface.'

Certificate ARN
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).

BGP ASN [Info](#)
The ASN of your customer gateway device.

Value must be in 1 - 2147483647 range.

Routing options [Info](#)

Dynamic (requires BGP)

Static

Static IP prefixes [Info](#)

Local IPv4 network CIDR - optional
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

Remote IPv4 network CIDR - optional
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

▶ **Tunnel 1 options** - optional [Info](#)

▶ **Tunnel 2 options** - optional [Info](#)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key: Value - optional:

You can add 49 more tags.

3. Once the VPN connection is successfully created, you will see a screen similar to the one below.

You successfully created vpn-03d87c000a9593585 / VPN-to-internal-AMF-Network

VPN connections (1/1) [Info](#)

VPN ID: vpn-03d87c000a9593585

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway ad...	Inside IP
VPN-to-internal-A...	vpn-03d87c000a9593585	Pending	vgw-0e91eb89cd46dc9ef	-	cgw-0ef213c76ce7006c3	111.108.31.27	IPv4

Add Static IP Prefix

If you want to communicate (ping, etc.) from the AR router to AWS via the tunnel, you need to tell the VPN gateway on the AWS side the range of link-local addresses used on the tunnel. Otherwise, even if the packet arrives from the AR router to AWS, the return packet will be discarded by the VPN gateway.

This can be addressed by adding the link-local prefix as a static route.

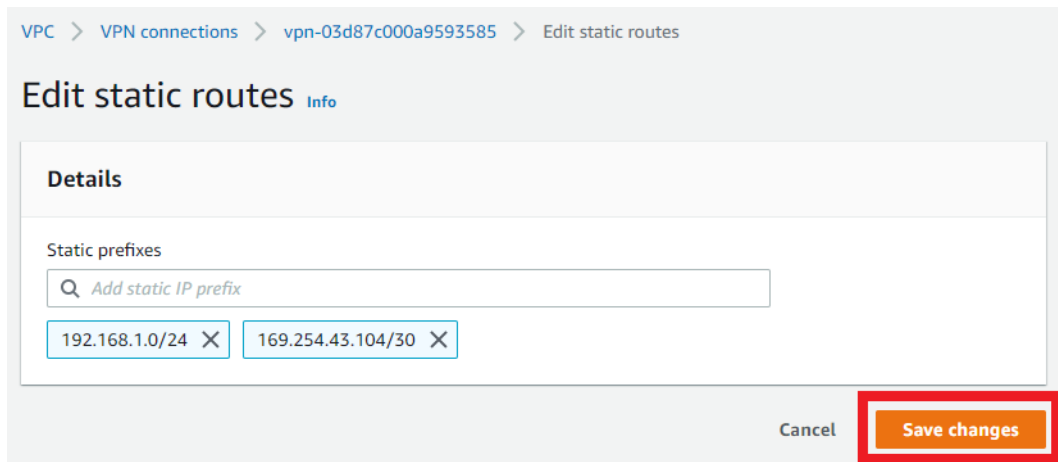
Register a static route as follows:

1. Click **Site-to-Site VPN Connections** under **Virtual private network (VPN)** from the left menu of the VPC dashboard screen. Select your VPN, click on the **Static routes** tab, and click on **Edit routes**.

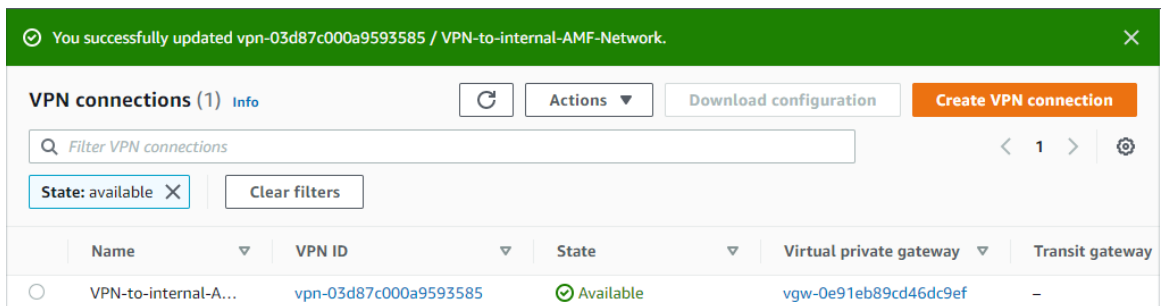
The screenshot displays the AWS VPC console interface for managing VPN connections. At the top, there's a section for 'VPN connections (1/1)' with a search bar, a 'Filter VPN connections' input, and buttons for 'State: available', 'Clear filters', 'Actions', 'Download configuration', and 'Create VPN connection'. Below this is a table listing VPN connections. The first entry is 'VPN-to-internal-A...' with VPN ID 'vpn-03d87c000a9593585', State 'Available', and Virtual private gateway 'vgw-0e91eb89cd46dc9ef'. Below the table, the console shows the details for 'vpn-03d87c000a9593585 / VPN-to-internal-AMF-Network'. The 'Static routes' tab is selected and highlighted with a red box. Underneath, there's a section for 'Routes (1)' with a search bar and an 'Edit routes' button, also highlighted with a red box. Below the search bar is a table of IP prefixes:

IP prefixes	State
192.168.1.0/24	Available

- The **Edit static routes** screen will appear, add a static IP prefix and click **Save changes**. Check the link-local address used on the tunnel in the “**Tunnel settings**” section.



- If the static IP prefix is added successfully, you will see a screen like the one below.



Enable route propagation

In order for VPN static IP prefixes (static routes) to be properly installed in the routing table, route propagation must be enabled. Otherwise, VPN static route traffic may not be routed correctly.

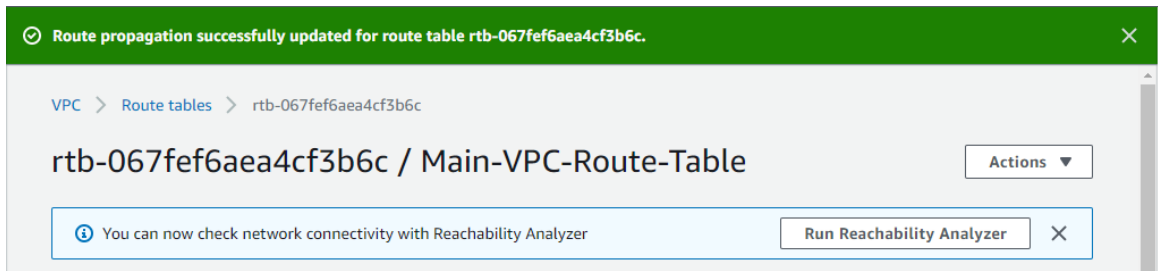
1. From the left menu of the VPC dashboard screen, click **Route Tables** under **Virtual private cloud**. Select the route table you created earlier, click the **Route propagation** tab, and click **Edit route propagation**.

The screenshot shows the AWS VPC console interface. At the top, there's a header for 'Route tables (1/1) Info' with a refresh button, an 'Actions' dropdown, and a 'Create route table' button. Below this is a search bar for 'Filter route tables' and a filter box showing 'Name: Main-VPC-Route-Table'. A table lists route tables, with the selected one being 'Main-VPC-Route-Ta...' with ID 'rtb-067fef6aea4cf3b6c'. Below the table, the 'Route propagation' tab is selected and highlighted with a red box. Under this tab, there's a section for 'Route Propagation (1)' with a search bar and an 'Edit route propagation' button, which is also highlighted with a red box. Below this, a table shows the propagation settings for a 'Virtual Private Gateway' named 'vgn-0e91eb89cd46dc9ef / VPN-Gateway'.

2. The **Edit route propagation** screen will be displayed. Check **Enable** in the **Propagation** column and click **Save**.

The screenshot shows the 'Edit route propagation' dialog box. It has a title 'Edit route propagation' and two main sections. The first section, 'Route table basic details', shows the 'Route table ID' as 'rtb-067fef6aea4cf3b6c'. The second section, 'Edit route propagation', shows the 'Virtual Private Gateway' as 'vgn-0e91eb89cd46dc9ef / VPN-Gateway' and the 'Propagation' status as 'Enable' with a checked checkbox. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red box.

- After successfully editing the route propagation, you will see a screen like the one below.



Settings on the AR router side

Next, we will explain the IPsec-related settings of the AR router, which is the VPN router on the local network side.

For network configuration, see the “[How to use AWS \(VPC\) VPN function](#)” section.

Here we assume that the AR router is connected to the Internet via the ppp0 interface.

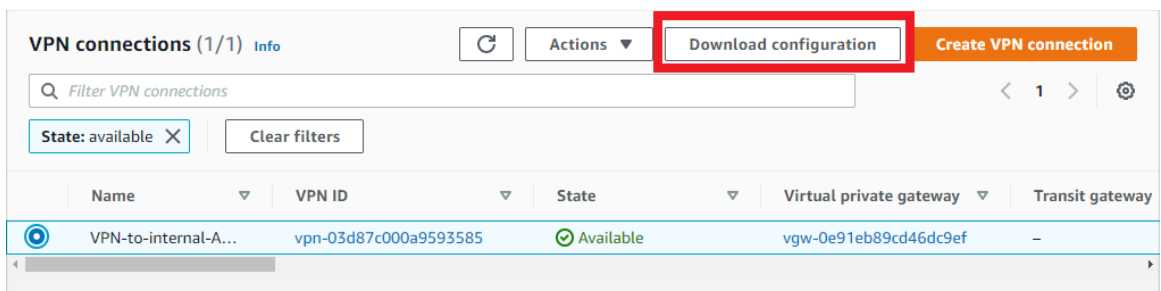
Also, it is assumed that the settings on the AWS side have been completed. See the “[Settings on the AWS side](#)” section.

Once the VPN settings on the AWS side are complete, you will be able to download configuration samples for various VPN routers from the AWS dashboard.

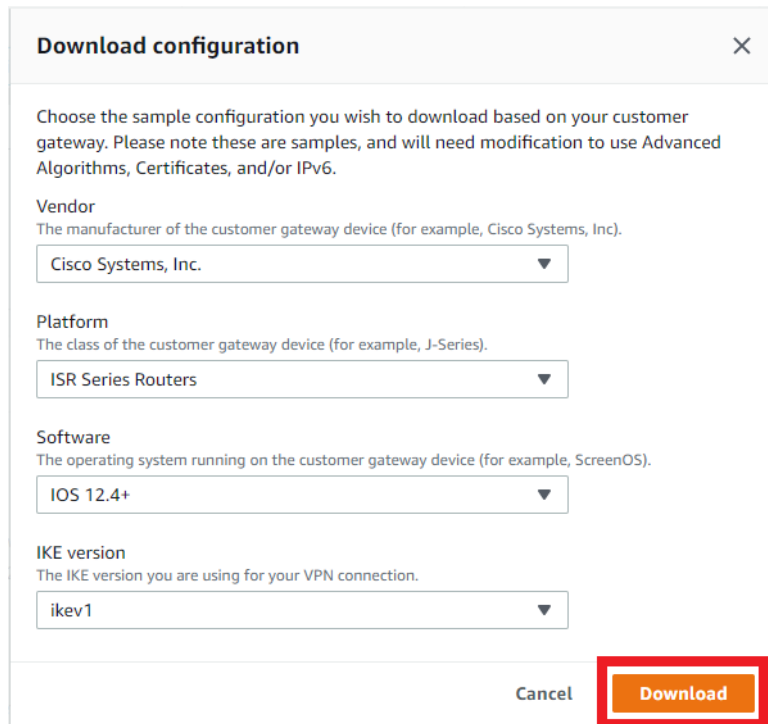
The following explains how to set the AR4050S based on the setting sample of the Cisco Systems ISR series.

The reason for using the setting sample for the ISR series instead of the general-purpose setting sample is that the latter is closer to the setting of the AR4050S.

- From the left menu of the VPC dashboard screen, click **Site-to-Site VPN connections** under **Virtual private network (VPN)**. Select your VPN and click **Download configuration**.



- The **Download configuration** screen will be displayed. Set as follows and click **Download**.



Download configuration ✕

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor
The manufacturer of the customer gateway device (for example, Cisco Systems, Inc).

Cisco Systems, Inc. ▼

Platform
The class of the customer gateway device (for example, J-Series).

ISR Series Routers ▼

Software
The operating system running on the customer gateway device (for example, ScreenOS).

IOS 12.4+ ▼

IKE version
The IKE version you are using for your VPN connection.

ikev1 ▼

Cancel **Download**

The downloaded configuration sample has many sections, but this manual will extract only the important parts and show the configuration for the ISR series and for the AR4050S in comparison.

The important sections in the configuration sample are:

- Custom ISAKMP profile
- Key
- Custom IPSEC profile
- Assign Profile to Tunnel Peer
- tunnel

ISAKMP profile configuration (“Policy” on Cisco)

Corresponding part of the configuration sample for Cisco ISR.

```
crypto isakmp policy 200
 encryption aes 128
 authentication pre-share
 group 2
 lifetime 28800
 hash sha
 exit
```

AR4050S settings.

```
awplus(config)# crypto isakmp profile AWS-ISAKMP-Phase-1
awplus(config-isakmp-profile)# transform 1 integrity sha1 encryption aes128 group
2
awplus(config-isakmp-profile)# lifetime 28800
awplus(config-isakmp-profile)# dpd-interval 10
awplus(config-isakmp-profile)# version 1 mode main
awplus(config-isakmp-profile)# end
awplus#
```

Note: For IKE exchange mode, Cisco automatically tries both modes (aggressive, main), but AR4050S requires manual configuration.

Use the **show isakmp profile** command to check the settings.

```
awplus# show isakmp profile AWS-ISAKMP-Phase-1
ISAKMP Profile: AWS-ISAKMP-Phase-1
  Version: IKEv1
  Mode: Main
  Authentication: PSK
  Expiry: 8h
  DPD Interval: 10s
  DPD Timeout: 150s
  Transforms:
    Integrity Encryption DH Group
    1 SHA1 AES128 2
```

ISAKMP pre-shared key setting

Corresponding part of the configuration sample for Cisco ISR.

```
crypto keyring keyring-vpn-4234d12b-0
 local-address 10.1.1.1
 pre-shared-key address 10.0.0.1 key j3mqY_4dtzOHG7uP9mREjNkQxyeqnmEc
 exit
```

AR4050S settings.

```
awplus(config)# crypto isakmp key j3mqY_4dtzOHG7uP9mREjNkQxyeqnmEc address
10.0.0.1
```

Use the **show isakmp key** command to check the settings.

```
awplus# show isakmp key
Hostname/IP address Key
-----
10.0.0.1 j3mqY_4dtzOHG7uP9mRE
                                     jNkQxyeqnmEc
```

Custom ISAKMP Profile Assignment to AWS Peers

AR4050S settings.

```
awplus(config)# crypto isakmp peer address 10.0.0.1 profile AWS-ISAKMP-Phase-1
```

Use the **show isakmp peer** command to check the settings.

```
awplus# show isakmp peer
Peer Profile (* incomplete) Key
-----
10.0.0.1 AWS-ISAKMP-Phase-1 PSK
```

IPsec settings

Corresponding part of the configuration sample for Cisco ISR.

```
crypto IPsec transform-set IPsec-prop-vpn-4234d12b-0 esp-aes 128 esp-sha-hmac
mode tunnel
exit
```

AR4050S settings.

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

Use the **show ipsec profile** command to check the settings.

```
awplus# show ipsec profile AWS-IPSEC-Phase-2
IPsec Profile: AWS-IPSEC-Phase-2
Replay-window: 32
Expiry: 1h
PFS group: 2
Transforms:
  Protocol Integrity Encryption
  1 ESP SHA1 AES128
```

Tunnel settings

Corresponding part of the configuration sample for Cisco ISR.

```
interface Tunnel1
ip address 169.254.XX.XX 255.255.255.252
ip virtual-reassembly
tunnel source 10.1.1.1
tunnel destination 10.0.0.1
tunnel mode IPsec ipv4
tunnel protection IPsec profile IPsec-vpn-4234d12b-0
! This option causes the router to reduce the Maximum Segment Size of
! TCP packets to prevent packet fragmentation.
ip tcp adjust-mss 1387
no shutdown
exit
```

AR4050S settings.

```
awplus(config)# int tunnel1
awplus(config-if)# mtu 1434
awplus(config-if)# ip address 169.254.XX.XX/30
awplus(config-if)# tunnel source 10.1.1.1
awplus(config-if)# tunnel destination 10.0.0.1
awplus(config-if)# tunnel mode IPsec ipv4
awplus(config-if)# tunnel protection IPsec profile AWS-IPSEC-Phase-2
awplus(config-if)# ip tcp adjust-mss 1387
awplus(config-if)# end
```

Use the **show ip interface** and **show interface** commands to check the settings.

```
awplus# show ip interface brief
Interface          IP-Address          Status              Protocol
eth1                unassigned          admin up            running
eth2                unassigned          admin up            down
lo                  unassigned          admin up            running
vlan1               unassigned          admin up            down
vlan10              192.168.1.0/24     admin up            running
tunnel1             169.254.XX.XX/30   admin up            running
ppp0                 10.1.1.1/32        admin up            running

awplus# show interface tunnel1
Interface tunnel1
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 169.254.XX.XX/30 point-to-point 169.254.XX.XX
  index 14 metric 1 mtu 1434
  IPv4 mss 1387
  <UP, POINT-TO-POINT, RUNNING, MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 10.1.1.1, destination 10.0.0.1
  Tunnel name local 10.1.1.1, remote 10.0.0.1
  Tunnel protocol/transport IPsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, path MTU discovery disabled
  Tunnel protection via IPsec (profile "AWS-IPSEC-Phase-2")
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 00:21:30
```


Note: While the tunnel interface is 'UP', the tunnel does not track the state of the peer. This means that the tunnel is ready to initiate connections or respond to peer initiation. To check if the tunnel is working, try pinging the link-local address of your AWS router (169.254.XXX.XXX) from your AT-AR4050S. If the ping is successful, the tunnel is up and working. Try pinging other desired networks to see if the routing is working as desired, and configure static routing if necessary.

Routing settings

In this example, the AR4050S does not have a default route. Use the following command to register the public IP address of the AWS router and the static route to the subnet to which this product belongs.

```
ip route 0.0.0.0/0 ppp0
ip route 172.30.0.0/24 169.254.XX.XX
```

For communication initiated from the AR4050S, the settings for correctly returning the return packet from this product to the AR4050S are configured in the “[IPsec settings](#)” section.

At this point, IP communication between this product on AWS and the local network can be established.

Licensing

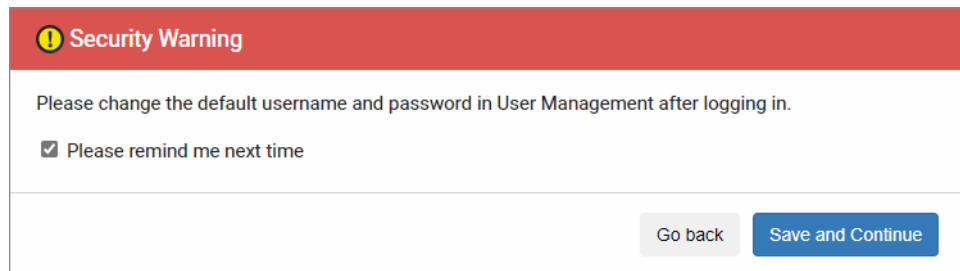
Once you finish your setup, you need to install a subscription base license. This license is required before the device will work.

Accessing the Web GUI and Installing Licenses

1. Open the **EC2** dashboard screen by clicking **Services > All services > EC2**. Click **Instances** under **Instances** from the left menu. Select the instance you created, and note the **Public IP**.
2. Launch your web browser and enter the IP address from Step 1 to access the AR4000S-Cloud web GUI.
For example, **https://192.168.10.103** (replacing the IP with your IP address).
3. When the login screen appears, enter your user-name and password and click the **Sign In** button.

Note: The default user-name is “manager” and password is “friend”. If they have been updated, use the changed password. However, since the settings cannot be saved when the license is not installed, be aware that restarting the virtual machine will return to the initial password.

Note: When you log in with the default user-name and password, you will get a security warning: “Click Save and Next to continue logging in.”



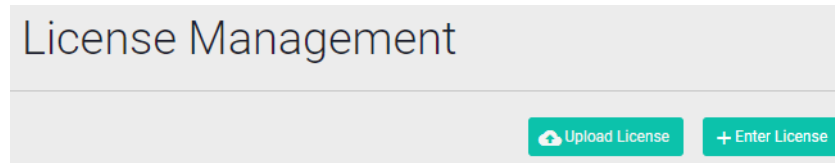
Click **Save and Continue** to log in.

4. The AR4000S-Cloud dashboard screen will be displayed.

Without a VPN license installed, the menu column on the left side of the screen shows only minimal menu items.

5. To install a VPN license, you need to request a license key and obtain a license file. From the menu on the left side of the screen, click on the **System > About** screen. Note the **Serial Number**, which you will use to request the license key.

- Note:** For license key requests, please contact your sales representative, agency, or contact point. The required license for the AR4000S-Cloud is **AT-AR-VPN10**. For further ordering information, please refer to the product datasheet.
- Note:** The AR4000S-Cloud serial number will be changed if you delete the AR4000S-Cloud virtual machine and create it again. If the serial number is changed, the license will need to be reissued, so please be careful not to delete the virtual machine unless necessary.
6. After obtaining the license file, log in to the Web GUI again. Click on **System > License Management** from the menu on the left side of the screen. and click the **Upload License** button.



7. Specify the license file in the file selection dialog.
8. After reloading the browser, all menu items will be displayed in the menu column on the left side of the screen. Installation of the license is now complete.

Firmware update

To update the firmware of this product, use the **software-upgrade** command.

Prerequisite

It is necessary to download the maintenance firmware (ISO image file) of this product from our website and upload it to this product on AWS.

About ISO files and VHD files

The firmware for this product is distributed in the following two formats, each of which has a different purpose as follows:

- An ISO image file is used to update the firmware.
- The VHD image file is for uploading to AWS to create the AMI of this product.

For more information, see [“Create an Amazon Machine Image”](#).

The ISO image file provided on our website is for updating the firmware of this product that is already running on AWS.

Update procedure

To update the firmware of this product, log in to the CLI of this product and perform the following procedure.

1. Make sure the ISO image file exists on the file system.

```
awplus# dir
...
25499648 -rw- Jul 16 2022 20:45:45 AR4000S-Cloud-5.5.2-1.2.iso
```

2. Specify the ISO image file using the **software-upgrade** command. A confirmation message will be displayed; verify the ISO is correct then enter “y”.

```
awplus# software-upgrade AR4000S-Cloud-5.5.2-1.2.iso
Install this release to disk? (y/n): y
Upgrade succeeded, the changes will take effect after rebooting the device.
```

3. Reboot with new firmware.

```
awplus# reboot
```

Tips and troubleshooting

Lost network connection

This product has a mechanism called fail-safe mode as an automatic recovery method. The product enters failsafe mode when it detects that the network connection with AWS has been lost.

If this product cannot connect to some of the default servers that exist on AWS, it assumes that access to the management function is no longer possible and starts a 5-minute monitoring timer. If 5 minutes pass without the connection being restored, the product will restart with default settings.

This feature is primarily intended for automatic recovery from connectivity failures due to the following reasons:

- eth0 port shut-down
- Incorrect static IP address setting for eth0
- routing problems

When the product is launched with default settings, it can be accessed via SSH using the original SSH key pair assigned when the instance was created. In addition, the configuration file before restart will be renamed to “default_backup.cfg” and saved.

When the SSH server function is disabled

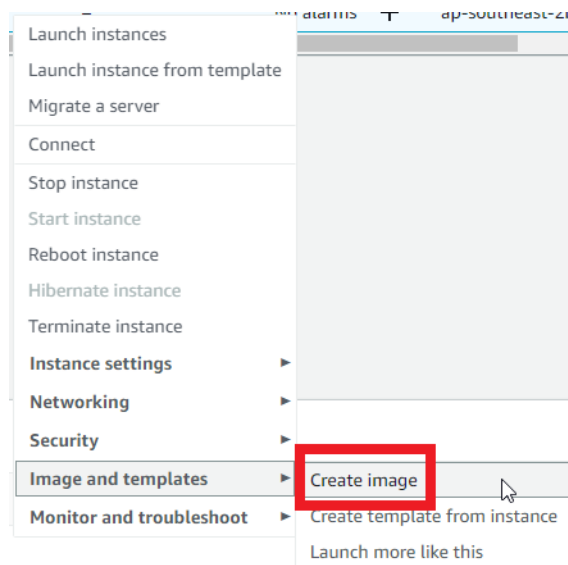
This product also starts a 5-minute monitoring timer when the SSH server function is disabled. This is because the management functions of this product can only be accessed via SSH.

If 5 minutes have passed with the SSH server function disabled, the product will restart with the default settings. The configuration file before restart will be renamed to “default_backup.cfg” and saved.

Creating an instance snapshot

Follow the steps below to take a snapshot of an instance image while it is running normally. This snapshot can be used in case the connection to this product cannot be restored even with the above mechanism.

1. Click **Instances** on the EC2 Dashboard.
2. Select the desired instance, right-click, and select **Image and templates > Create image**.



3. Enter an **Image name**, and click **Create image**.

You can check the created snapshot image in **Image > AMI**.

Amazon Machine Images (AMIs) (1) Info				
Owned by me ▼		Find AMI by attribute or tag		
Backup X		Clear filters		
<input type="checkbox"/>	Name ▼	AMI ID ▼	AMI name ▼	Source
<input type="checkbox"/>	-	ami-0efc6b4c577a78991	AR4000S-Backup	259623944249/AR4000S-Backup

To create a machine from this snapshot, create a new instance by selecting the created snapshot image in the **My AMIs** tab, using the same process described in the [“Create an instance”](#) section.

Note: If you have multiple AMIs of your own, when you click the **My AMIs** tab, a different one than the snapshot image you created may be selected. In that case, select the target snapshot from the drop-down list.

Note: If you recreate an instance from a snapshot, the MAC and IP addresses will be different than before. Therefore, it is necessary to manually reconfigure the network and re-register the annual license.

C613-04141-00 REV D



North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

© 2022 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.