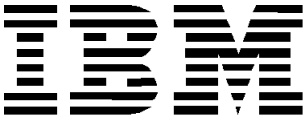
IBM® Storage

# IBM Solutions for Hybrid Cloud Networking Configuration

## Version 1 Release1



# Contents

**About this document** . . . . . 1
Executive summary . . . . . 1
Scope . . . . . 1
Prerequisites . . . . . 1
IBM Cloud: Configuring site-to-site IPSec VPN for hybrid cloud connectivity . . . . . 2
Configuring IPSec site-to-site VPN tunnel . . . . . 2
AWS Cloud: Configuring site-to-site VPN IP sec tunnel for hybrid cloud connectivity . . . . . 5
Summary . . . . . 11
. . . . . 11

**Notices** . . . . . 13
Trademarks . . . . . 14
Terms and conditions for product documentation . . . . . 15
Applicability . . . . . 15
Commercial use . . . . . 15
Rights . . . . . 15
Privacy policy considerations . . . . . 15

# About this document

This document describes the high-level networking architectures and required configuration for establishing the site-to-site Virtual Private Network (VPN) connectivity in the multicloud hybrid environment.

## Executive summary

In today's environment, many organizations are using some form of cloud services, whether private, public, or hybrid cloud and storage infrastructure is an integral part of these deployments. A hybrid cloud is a combination of a private cloud that is combined with the use of public cloud services where one or several touch points exist between the environments.

Networking is the critical component of the hybrid cloud and site-to-site Virtual Private Network (VPN) IPSec tunnel is the widely used option for extending the on-premises environment across multiple public clouds. In this paper, we describe the high-level logical configurations between on-premises and various public cloud service providers, such as Amazon Web Services (AWS) and IBM® Cloud.

## Scope

This technical report does not:

- Provide performance analysis from a user perspective
- Replace any official manuals and documents that are issued by IBM
- Replace any official manuals and documents that are issued by Amazon Web Services (AWS)
- Explain ordering and configuration resources in IBM and AWS cloud

## Prerequisites

This technical paper assumes that the following prerequisites are met:

- Knowledge of IP networking and routing tables
- Basic knowledge and administration of AWS resources and skills of IBM cloud

# IBM Cloud: Configuring site-to-site IPSec VPN for hybrid cloud connectivity

This section describes how to configure hybrid cloud connectivity between the IBM Cloud site and the on-premises site. This section also describes lab setup and the steps to configure the site-to-site IPSec tunnel for communication between IBM Cloud™ and the on-premises site.

**Note:** Although this section describes the logical steps for the use case that is shown, the on-premises network configuration, infrastructure, and security policy can vary on a case-by-case basis. This section is intended to give a high-level logical example.

The high-level logical network architecture for hybrid cloud connectivity is shown in Figure 1.

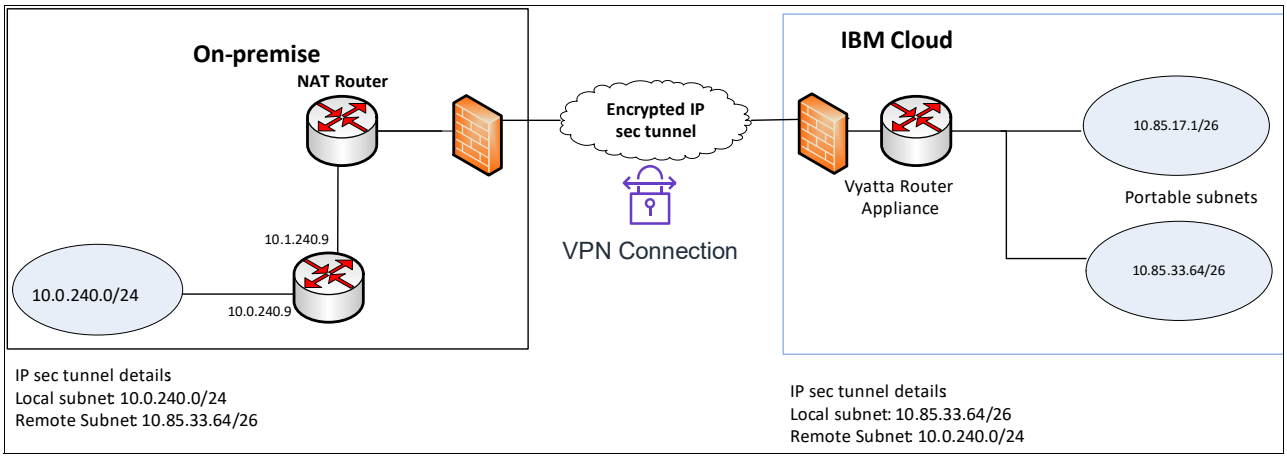



*Figure 1 Hybrid cloud network connectivity topology between IBM cloud and on-premises*

As shown in Figure 1, the network gateway appliance at the IBM Cloud site is a Vyatta Gateway Appliance, which acts a default router for the private (`10.85.17.1/26`) and portable private (`10.85.33.64/26`) subnet IP blocks.

All of the compute hosts and IBM Software defined storage systems are configured with IP addresses in the portable IP subnet `10.85.33.64/26`.

At the on-premises site, a network address translation (NAT) router is used (which is the core router) with a public IP address. That public IP address is NAT'ed to a private IP `10.1.210.9`.

The second router that is used for lab purposes is a VyOS software gateway at the on-premises site that acts as a default gateway for a private subnet.

The VPN IPSec site-to-site tunnel creates a secure communication network between your IBM Cloud infrastructure and on-premises infrastructure. Network communication between the private subnets is controlled by the access control list that is populated at the creation of the VPN IPSec site-to-site tunnel.

## Configuring IPSec site-to-site VPN tunnel

Complete the following steps on the IBM Cloud site's Vyatta Gateway Appliance:

1. Set up the virtual interface (VIF) to all subnets in the VLAN. The list of subnets is available in the VLAN from the IBM Cloud website (log in required).

Otherwise, the different subnets cannot access each other. In our example, we use VLAN 846, which has two private IP subnets: 10.85.17.0/26 and 10.85.33.64/26.

To set the VIF, use the following commands:

```
set interfaces bonding dp0bond0 vif 846 address 10.85.33.65/26
set interfaces bonding dp0bond0 vif 846 address 10.85.17.1/26
set interfaces bonding dp0bond0 vif 846 vlan 846
```

Also, set the VIF for the public IP subnet on a different bond. In the lab setup, the VLAN ID for the public IP subnet block is 818:

```
set interfaces bonding dp0bond1 vif 818 address dhcp
set interfaces bonding dp0bond1 vif 818 address x.x.x.x/28
set interfaces bonding dp0bond1 vif 818 vlan 818
```

2. Create the Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) groups for VPN configuration:

```
set security vpn ipsec ike-group IKE-CLOUDDC proposal 1
set security vpn ipsec ike-group IKE-CLOUDDC proposal 1 encryption aes256
set security vpn ipsec ike-group IKE-CLOUDDC proposal 1 hash sha2_256
set security vpn ipsec ike-group IKE-CLOUDDC proposal 1 dh-group 5
set security vpn ipsec ike-group IKE-CLOUDDC lifetime 86400
```

3. Create an ESP group with name CLOUDDC:

```
set security vpn ipsec esp-group ESP-CLOUDDC proposal 1
set security vpn ipsec esp-group ESP-CLOUDDC proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP-CLOUDDC proposal 1 hash 'sha2_256'
set security vpn ipsec esp-group ESP-CLOUDDC lifetime '3600'
set security vpn ipsec esp-group ESP-CLOUDDC compression 'disable'
set security vpn ipsec esp-group ESP-CLOUDDC mode 'tunnel'
set security vpn ipsec esp-group ESP-CLOUDDC pfs 'dh-group5'
```

4. Create site-to-site VPN IPSec configuration and set the pre-shared secret key:

```
set security vpn ipsec site-to-site peer <remote on-premise public IP>
set security vpn ipsec site-to-site peer <remote on-premise public IP>
authentication mode pre-shared-secret
set authentication pre-shared-secret TEST1
set default-esp-group ESP-CLOUDDC
set ike-group IKE-CLOUDDC
set local-address <Local IBM Cloud side public IP >
```

5. Create a tunnel with a local private IP subnet and a remote private IP subnet. After the tunnel is created, all of the machines that are part of these local and remote subnets can communicate with each other:

```
set tunnel 1 local prefix 10.85.33.64/26
set tunnel 1 remote prefix 10.0.210.0/24
```

**Note:** In the solution lab environment, the on-premises private subnet is behind the NAT. Therefore, NAT traversal (NAT-T) must be enabled as a part of VPN tunnel configuration.

6. Enable NAT-T and allow the required private subnet to communicate across the VPN tunnel:

```
set security vpn ipsec nat-traversal enable
set security vpn ipsec nat-networks allowed-network 10.0.210.0/24
set security vpn ipsec nat-networks allowed-network 10.1.210.0/24
```

Similarly, configure the router for the VPN tunnel at the on-premises site. For this example, we configured the IP addresses for the VyOS router as follows:

`eth0: 10.0.210.9/24`
`eth1: 10.1.210.9/24` (NAT rules are created to translate this private address to the public address.

a. Configure an IKE group, naming it in our example ONPREMDC:

```
set vpn ipsec ike-group IKE-ONPREMDC proposal 1
set vpn ipsec ike-group IKE-ONPREMDC proposal 1 encryption aes256
set vpn ipsec ike-group IKE-ONPREMDC proposal 1 hash sha256
set vpn ipsec ike-group IKE-ONPREMDC proposal 1 dh-group 5
set vpn ipsec ike-group IKE-ONPREMDC lifetime 86400
```

b. Configure an ESP group, naming it in our example ONPREMDC:

```
set vpn ipsec esp-group ESP-ONPREMDC proposal 1
set vpn ipsec esp-group ESP-ONPREMDC proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-ONPREMDC proposal 1 hash 'sha256'
set vpn ipsec esp-group ESP-ONPREMDC lifetime '3600'
set vpn ipsec esp-group ESP-ONPREMDC compression 'disable'
set vpn ipsec esp-group ESP-ONPREMDC mode 'tunnel'
set vpn ipsec esp-group ESP-ONPREMDC pfs 'dh-group5'
```

c. Set the interface that is used for the VPN tunnel; in this example it is eth1:

```
set vpn ipsec ipsec-interfaces interface eth1
```

d. Set the authentication key and create a tunnel between the local (on-premises) private subnet and the remote subnet (cloud site private portable subnet):

```
set vpn ipsec site-to-site peer <Public IP@Cloud Router> authentication mode
pre-shared-secret
set vpn ipsec site-to-site peer <Public IP@Cloud Router> authentication
pre-shared-secret TEST1
set vpn ipsec site-to-site peer <Public IP@Cloud Router> default-esp-group
ESP-ONPREMDC
set vpn ipsec site-to-site peer <Public IP@Cloud Router> ike-group
IKE-ONPREMDC
set vpn ipsec site-to-site peer <Public IP@Cloud Router> local-address
10.1.210.9
set vpn ipsec site-to-site peer <Public IP@Cloud Router> tunnel 1 local
prefix 10.0.210.0/24
set vpn ipsec site-to-site peer <Public IP@Cloud Router> tunnel 1 remote
prefix 10.85.33.64/26
```

e. Enable NAT and NAT-allowed networks for the private subnet blocks at the cloud site:

```
set vpn ipsec site-to-site peer <Public IP@Cloud Router> nat-traversal
enable
set vpn ipsec site-to-site peer <Public IP@Cloud Router> nat-networks
allowed-network 10.85.17.0/26
set vpn ipsec site-to-site peer <Public IP@Cloud Router> nat-networks
allowed-network 10.85.33.64/26
```

This step activates the IPsec VPN tunnel.

To check whether the VPN tunnel is functioning, run the **`show vpn ipsec sa`** command, as shown in Figure 2 on page 5. In the example, the VPN tunnel is up between the on-premises site and the IBM Cloud site.

```
vyatta@vyattagw-1:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
192.                                    158.

    Tunnel  Id          State  Bytes Out/In   Encrypt      Hash      DH A-Time
L-Time
    ------  ----------  -----  -------------  -----------  --------  -- ------
------
    1       986         up     15.6M/17.5M    aes256       sha1      5  3995
0
```

*Figure 2 VPN IPsec tunnel status*

# AWS Cloud: Configuring site-to-site VPN IP sec tunnel for hybrid cloud connectivity

This section describes how to configure hybrid cloud connectivity between the AWS Cloud and the on-premises environment. This section also describes the lab setup and the steps to configure the site-to-site IPsec tunnel for communication between AWS Cloud and the on-premises site.

**Note:** Although this section describes the logical steps for the use case that is shown, the on-premises network configuration, infrastructure, and security policy can vary on a case-by-case basis. This section is intended to give a high-level logical example.

The high-level architecture for hybrid cloud connectivity between on-premises and AWS cloud is shown in Figure 3.

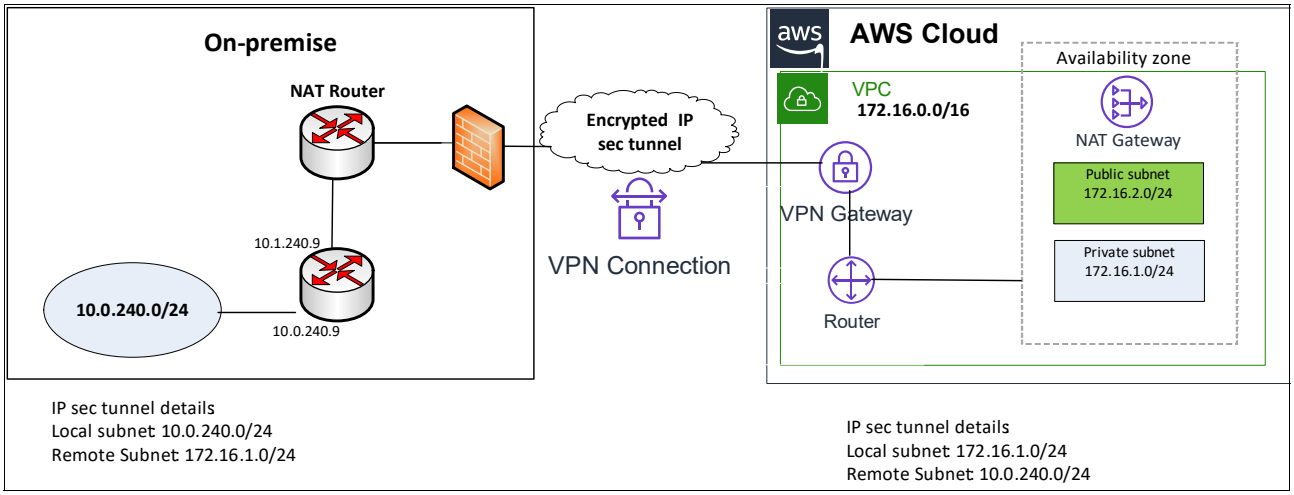



*Figure 3 Hybrid cloud network connectivity topology between AWS cloud and on-premises*

As shown in Figure 3, Virtual Private Cloud (VPC) in AWS is configured with a VPN gateway and router for the CIDR block `172.16.0.0/24`. VPN gateway is required for establishing the tunnel between AWS cloud and on-premises infrastructure. It acts as the default router for communication between AWS and on-premises systems. In AWS, all of the compute hosts and IBM Software defined storage systems are configured with IP addresses in the private IP subnet `172.16.1.0/24`.

At the on-premises site, a network address translation (NAT) router is used (which is the core router) with a public IP address. That public IP address is NAT'ed to a private IP `10.1.210.9`. The second router that is used for lab purposes is a VyOS software gateway at the on-premises site that acts as a default gateway for a private subnet.

The VPN IPsec site-to-site tunnel creates a secure communication network between AWS Cloud infrastructure and on-premises infrastructure. Network communication between the private subnets is controlled by the access control list that is populated at the creation of the VPN IPsec site-to-site tunnel.

## AWS configuration for VPN IP Sec tunnel

This section describes the required steps at the VPC level in AWS cloud for establishing the IP sec tunnel.

1. Create customer gateway. Log in to the AWS console with the resource provisioning privileges and scroll down to the Virtual Private Network (VPN) section in the pane. Click **Customer Gateways** and enter the required information, as shown in the Figure 4.

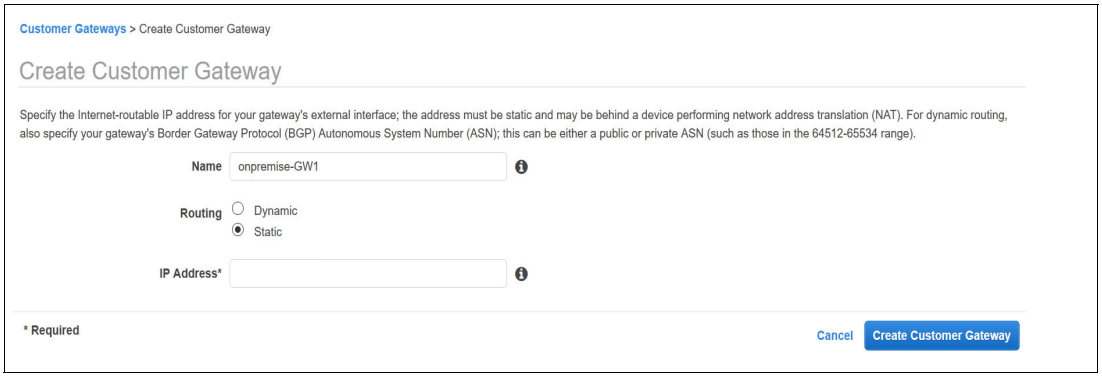



*Figure 4 Customer gateway configuration in AWS*

2. Create Virtual Private Gateways. Click the **Virtual Private Gateways** section in the VPC and configure the required information, as shown in the Figure 5.


*Figure 5 Virtual private gateway configuration in AWS*

3. Attach Virtual private gateway to the VPC, as shown in the Figure 6.


*Figure 6 Attaching Virtual private gateway to VPC in AWS*

4. Create Site-to-Site VPN connection in AWS console, as shown in Figure 7. Select the Virtual Private Gateway and customer gateway parameters (see Figure 6).

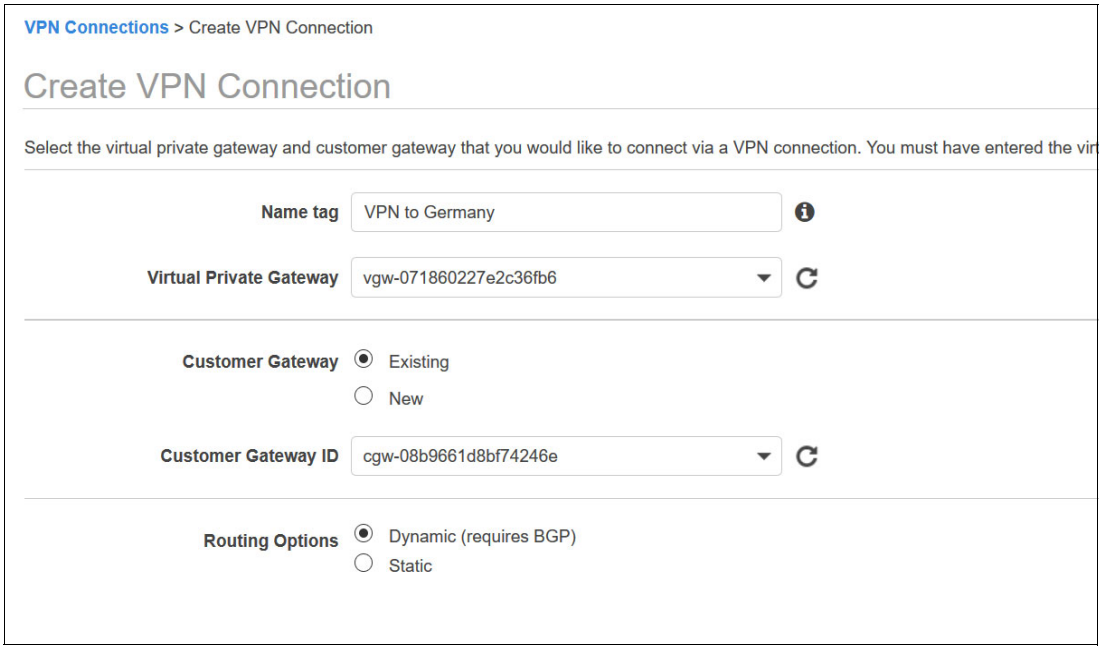



*Figure 7* Creating VPN connection in AWS

This step creates two tunnels in the VPC that are used for the configuration at the other end of the tunnel.

## Configuring the VyOS router at on-premises

Complete the following steps:

1. Enable NAT-T. The address of the external interface for your customer gateway must be a static address. In the LAB configuration, we used the VyOS gateway that is behind a device performing network address translation (NAT). To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall rules to unblock UDP port 4500:

```
set security vpn ipsec nat-traversal enable
```

2. Complete the following steps to configure IPSec tunnel #1:

   a. Use the following Internet Key Exchange (IKE) configuration:

   ```
   set vpn ipsec ike-group AWS lifetime '28800'
   set vpn ipsec ike-group AWS proposal 1 dh-group '2'
   set vpn ipsec ike-group AWS proposal 1 encryption 'aes128'
   set vpn ipsec ike-group AWS proposal 1 hash 'sha1'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS) authentication
   mode 'pre-shared-secret'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS) authentication
   pre-shared-secret 'mD2UOcZmKY23sX3Ou.Iox_OFj_GYcsEd'
   set vpn ipsec site-to-site  <Public IP of tunnel1@AWS)description 'VPC
   tunnel 1'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS)ike-group 'AWS'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS)local-address
   <local public IP >'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS)vti bind 'vti0'
   set vpn ipsec site-to-site peer <Public IP of tunnel1@AWS)vti esp-group
   'AWS'
   ```

   b. Use the following Encapsulating Security Payload (ESP) configuration:

   ```
   set vpn ipsec ipsec-interfaces interface 'eth0'
   set vpn ipsec esp-group AWS compression 'disable'
   set vpn ipsec esp-group AWS lifetime '3600'
   set vpn ipsec esp-group AWS mode 'tunnel'
   set vpn ipsec esp-group AWS pfs 'enable'
   set vpn ipsec esp-group AWS proposal 1 encryption 'aes128'
   set vpn ipsec esp-group AWS proposal 1 hash 'sha1'
   ```

   c. Configure the IPSec dead peer detection parameters:

   ```
   set vpn ipsec ike-group AWS dead-peer-detection action 'restart'
   set vpn ipsec ike-group AWS dead-peer-detection interval '15'
   set vpn ipsec ike-group AWS dead-peer-detection timeout '30'
   ```

   d. Configure the IPsec tunnel parameters:

   ```
   set interfaces vti vti0 address '169.254.40.102/30'
   set interfaces vti vti0 description 'VPC tunnel 1'
   set interfaces vti vti0 mtu '1436'
   ```

   e. Configure the Border Gateway Protocol (BGP). BGP is used within the tunnel to exchange prefixes between the Virtual Private Gateway and your Customer Gateway. The Virtual Private Gateway announces the prefix that corresponds to your VPC:

   ```
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell1@AWS) remote-as
   '64512'
   set protocols bgp 65000 neighbor <Inside IP CIDR of
   tunell1@AWS)soft-reconfiguration 'inbound'
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell1@AWS)timers
   holdtime '30'
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell1@AWS)timers
   keepalive '10'
   ```

   Your Customer Gateway can announce a default route (0.0.0.0/0), which can be done with the 'network' statement:

   ```
   set protocols bgp 65000 network 0.0.0.0/0
   ```

To advertise more prefixes to Amazon VPC, replace the `0.0.0.0/0` with the prefix you want to advertise. Make sure that the prefix is present in the routing table of the device with a valid next-hop.

3. Repeat steps 1 and 2 to configure IPSec tunnel#2:

   a. Use the following IKE parameters:

   ```
   set vpn ipsec ike-group AWS lifetime '28800'
   set vpn ipsec ike-group AWS proposal 1 dh-group '2'
   set vpn ipsec ike-group AWS proposal 1 encryption 'aes128'
   set vpn ipsec ike-group AWS proposal 1 hash 'sha1'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@ AWS)authentication
   mode 'pre-shared-secret'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@ AWS)authentication
   pre-shared-secret '63VRY4qF.6viqkguHB8wOwQKOFJdsvk1'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@AWS) description 'VPC
   tunnel 2'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@AWS) ike-group 'AWS'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@AWS) local-address
   <local Public IP address>
   set vpn ipsec site-to-site peer <Public IP of tunnel2@AWS) vti bind 'vti1'
   set vpn ipsec site-to-site peer <Public IP of tunnel2@AWS)vti esp-group
   'AWS'
   ```

   b. Use the following Tunnel Interface configuration:

   ```
   set interfaces vti vti1 address '169.254.42.106/30'
   set interfaces vti vti1 description 'VPC tunnel 2'
   set interfaces vti vti1 mtu '1436'
   ```

   c. Use the following BGP configuration:

   ```
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell2@AWS)remote-as
   '64512'
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell2@AWS)
   soft-reconfiguration 'inbound'
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell2@AWS)timers
   holdtime '30'
   set protocols bgp 65000 neighbor <Inside IP CIDR of tunell2@AWS)timers
   keepalive '10'
   ```

d. Check the tunnel status. On the VyOS router, the VPN IPsec tunnel status can be verified by running the **`show vpn ipsec sa`** command, as shown in Figure 8.

```
vyos@VyOS-class24:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
[redacted]                              10.1.240.9

    Description: VPC tunnel 3

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ------  -----
    vti     up     9.0K/8.5K      aes128   sha1    yes    1392    3600    all

Peer ID / IP                            Local ID / IP
------------                            -------------
[redacted]                              10.1.240.9

    Description: VPC tunnel 4

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ------  -----
    vti     up     938.3K/1009.7K aes128   sha1    yes    1245    3600    all

Peer ID / IP                            Local ID / IP
------------                            -------------
[redacted]                              10.1.240.9

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ------  -----
    1       up     3.2K/5.7K      aes256   sha256  yes    999     3600    all
    2       up     1.4M/2.5M      aes256   sha256  yes    3030    3600    all
```

*Figure 8 Checking VPN IPSec status at VyOS router*

You can also check the status at VPC AWS console by clicking **Site-to-site connections** → **Tunnel Details**, as shown in Figure 9.

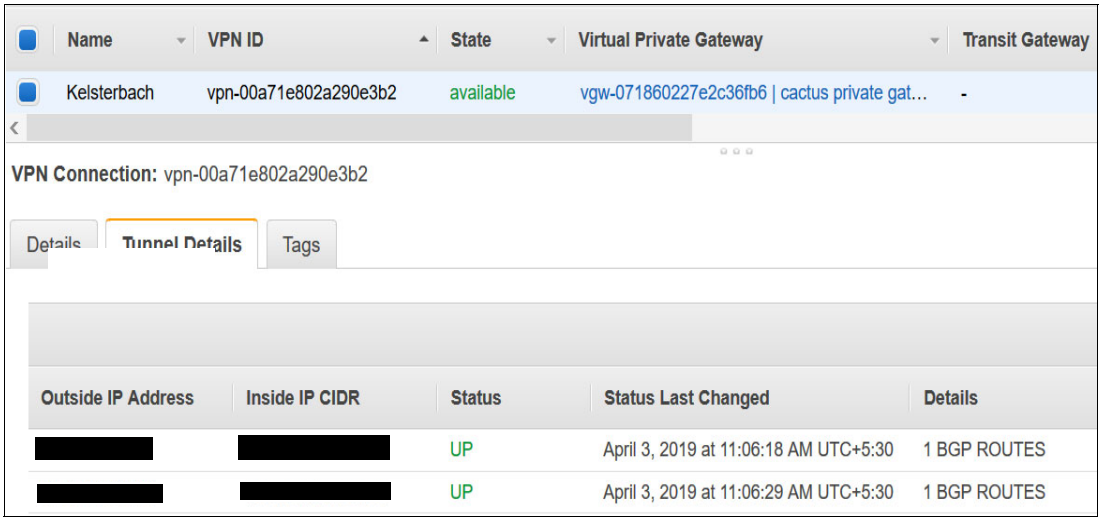



*Figure 9 Checking VPN IPSec status from AWS console*

# Summary

With so many cloud networking options available today, virtually no two hybrid clouds are built the same way. It takes a keen understanding of the business, and of the available networking options to create the hybrid solution that is best suitable for your specific goals. The most widely used choice is a site-to-site virtual private network (VPN) IPSec tunnel across the internet for creating secure hybrid connectivity.

This paper describes the logical hybrid networking configurations with the various public cloud end points. For a larger enterprise customer, the on-premises network configuration, infrastructure, and security configurations can vary according to organization policies. The choice of connectivity depends on the customer environment and their preferences.

# Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
*IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Redbooks (logo)  ®  IBM®  IBM Cloud™

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.

# Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

## Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

## Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

## Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.



May 2019



Please recycle

ISBN 0738457736

REDP-5542-00