Google Cloud

White paper
November 2021

How Customers of RISE with SAP S/4HANA® Cloud, Private Edition and SAP® Enterprise Cloud Services Can Set Up VPC Network Peering with Google Cloud

Table of Contents

Google Cloud

Executive summary

SAP customers of the RISE with SAP offering are embracing business transformation in conjunction with Google Cloud offerings in ever greater numbers. However, to realize the promise of a successful cloud migration, they require secure, low-latency, high-bandwidth connectivity from their SAP® software to systems in Google Cloud. A critical component of this connectivity includes software-as-a-service (SaaS), platform-as-a-service (PaaS), and Google Cloud services, for example, BigQuery, used in customer projects hosted by Google Cloud.

To achieve secure connectivity between customer projects in Google Cloud, a peer virtual private cloud (VPC) network must be set up. This allows network traffic to traverse the Google network without connecting through a WAN provider or the Internet. This document is written for IT network administrators, enterprise architects, and operations engineers who want to set up this connectivity. It focuses on setting up a VPC network from RISE with SAP S/4HANA® Cloud, private edition and SAP Enterprise Cloud Services projects hosted in Google Cloud to one or more customer projects in Google Cloud.

What is VPC Network Peering, and when is it useful?

Google Cloud VPC Network Peering supports the secure connectivity of internal IP addresses across two VPC networks, whether they belong to the same project or organization or not. This allows workloads between two VPC networks to communicate internally, avoiding the customer WAN and Internet. When VPC Network Peering is used in Google Cloud to connect SAP-managed resources to a VPC hub, there is no ingress or egress. VPC Network Peering connects a customer VPC that is managed by SAP for RISE with SAP S/4HANA Cloud, private edition or SAP Enterprise Cloud Services with the customer's VPCs within the customer's own organization or project. This ensures that all VPC-peered network traffic stays within Google's secure network.

Google Cloud VPC Network Peering is useful in the following environments:

- SaaS ecosystems in Google Cloud, with services available privately across different VPC networks within and across organizations
- Organizations that have several network administrative domains that need to communicate using internal IP addresses

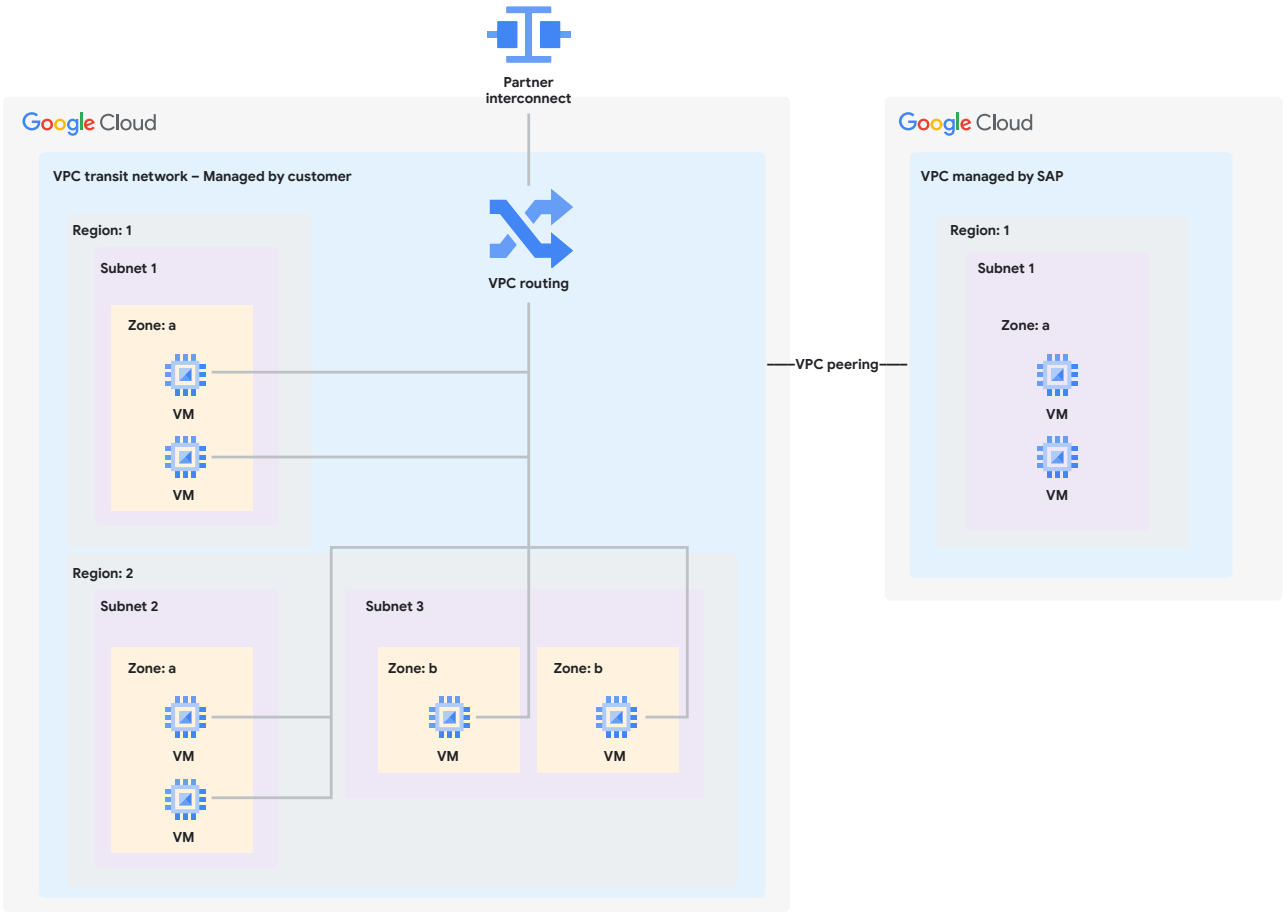
Recommended VPC Setup

We recommend setting up connectivity from on-premises software to RISE with SAP S/4HANA Cloud, private edition or SAP Enterprise Cloud Services through a customer-managed transit VPC. This allows the customer to:

- Leverage existing dedicated interconnects or partner interconnects that link the customer's on-premises network to Google Cloud
- Share existing bandwidth already provisioned to the customer's managed VPCs with one or more SAP-managed VPCs
- Ensure firewall rules are managed according to the customer's organizational policies
- Deploy third-party firewall products, such as those from Palo Alto Networks Inc., in the transit VPC to be used for all cross-VPC network traffic and to on-premises networks
- Control Internet traffic in the transit VPC instead of in the SAP-managed VPC

Figure 1 illustrates a simple networking setup where the customer has provisioned a partner interconnect to a single customer-managed VPC, which is then used as a transit VPC and peered to a single SAP-managed VPC.

Figure 1: Simple Networking Setup



Note About Deploying Multiple VPCs

If the customer has deployed multiple VPCs, the company can adopt a hub-and-spoke model, with the transit VPC as the hub and the SAP-managed VPC as a spoke. Please refer to best practices and reference architectures for VPC design for additional information. If the customer has deployed network address translation (NAT) gateways or third-party firewall products such as those from Palo Alto Networks, see centralized network appliances on Google Cloud for detailed reference architectures.

Prerequisites for VPC setup

Before continuing the setup process, review the VPC Network Peering restrictions to ensure that the peering will be successful. Once you're ready to move forward, you will need the following project and VPC details for both VPC networks to be peered.

Customer-managed VPC (hub)

- The project ID
- The name of the spoke VPC network with which you want to peer
- *Exchange Custom Routes* option for transitive routing, to be requested as needed
- Network IP ranges (subnet IP ranges used in the customer VPC as well as those used on premises) so that you can include them in firewall rules
- Access to create and delete VPC Network Peering
  - > IAM permissions for creating and deleting VPC Network Peering (included in the Compute Network Admin role: roles/compute.networkAdmin

SAP-managed VPC* (spoke)

- The project ID
- The name of the VPC network with which you want to peer
- Subnet IP ranges used in the SAP-managed VPC
  **Can be obtained from SAP by raising a service request*

To start the process with SAP, you will need to raise a service request with SAP to obtain a VPC Network Peering with a hub VPC.

CGN Range Restrictions

Customers of RISE with SAP S/4HANA Cloud, private edition and SAP Enterprise Cloud Services are permitted to "bring your own IP" (BYOIP) in RFC 1918 ranges for an SAP-managed VPC. This allows them to use carrier-grade NAT (CGN) IP ranges (RFC 6598) to manage resources in the VPC. As a result:

- CGN range use in customer on-premises networks or customer-managed VPCs may have restrictions.
- CGN range use in SAP-managed VPCs may have restrictions.

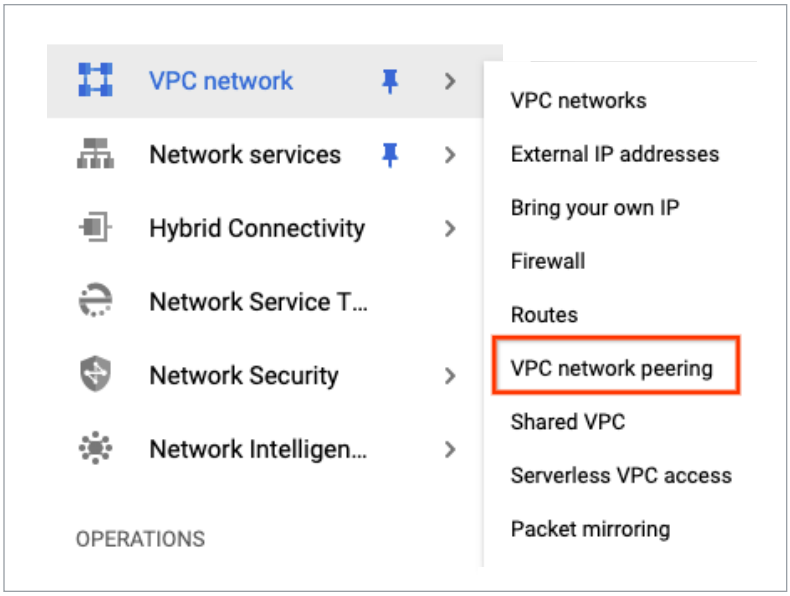
If there is a CGN requirement, we recommend aligning with customer-facing personnel from SAP to address it.

Setting up the customer-managed VPC

To begin the peering process, take the following steps:

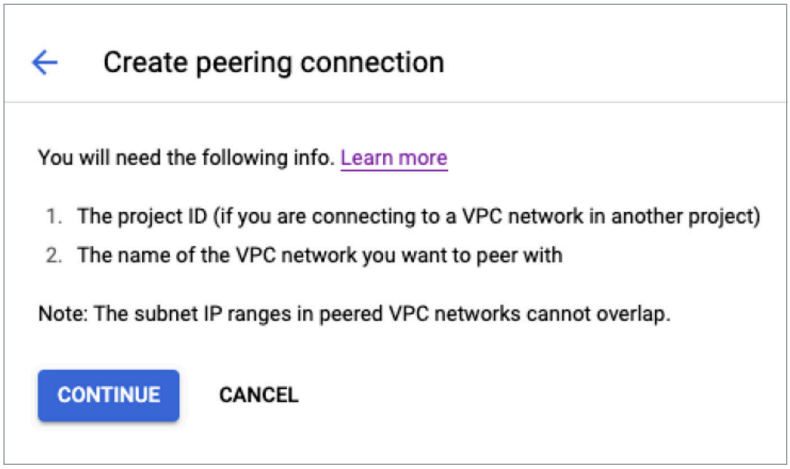
1. Go to the *Google Cloud Console* ➔ *VPC Network* ➔ *VPC Network Peering*. See Figure 2.

Figure 2: The *VPC Network Peering* Option



2. Choose *Create Peering Connection*. The dialog box in Figure 3 appears.

Figure 3: The *Create Peering Connection* Option

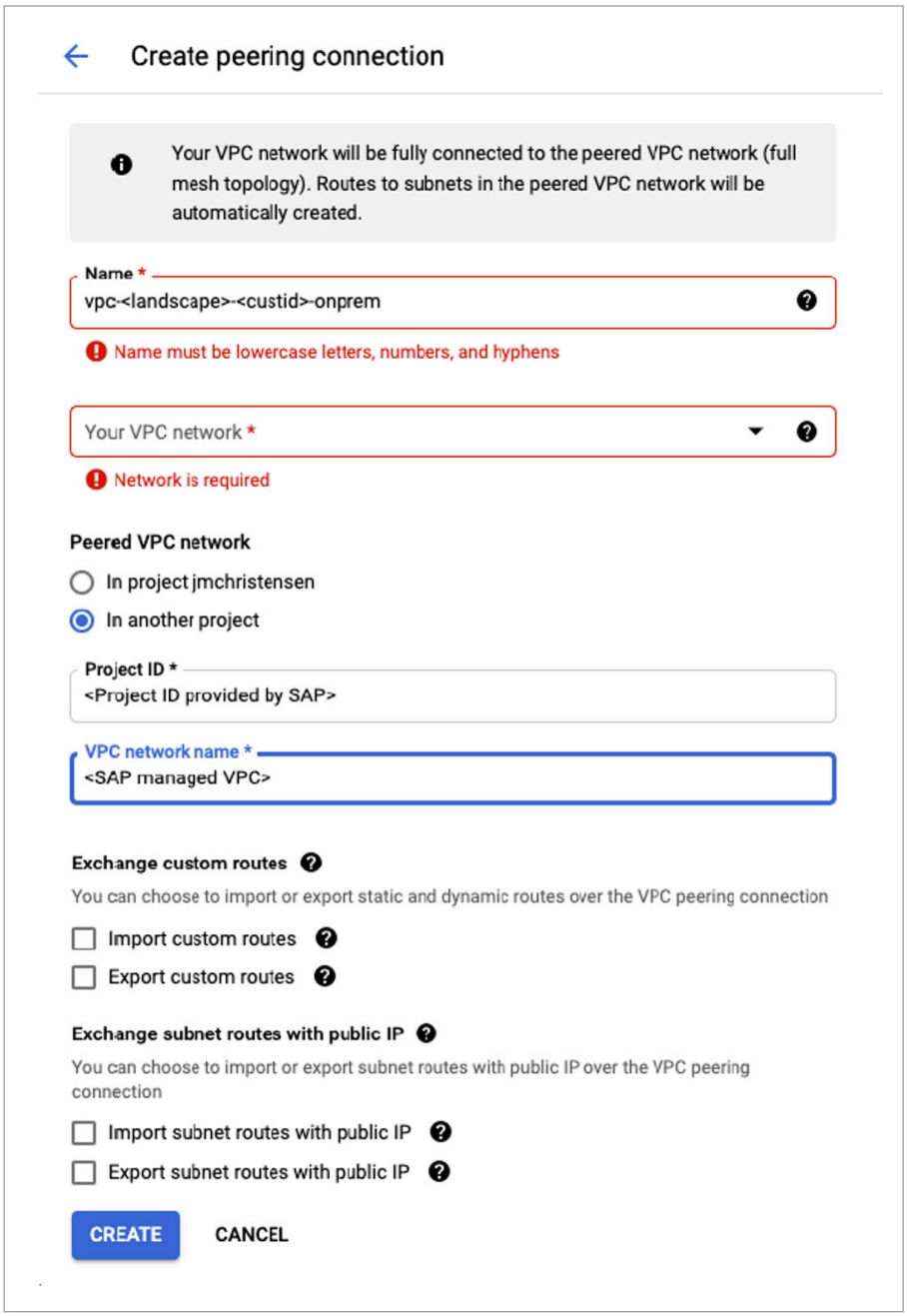


3. Choose *Continue*.

4. Enter details.

5. If you intend to leverage the on-premises connection in the customer-owned project for the SAP-managed VPC, then select the *Export Custom Routes* and *Import Custom Routes* checkboxes. See Figure 4.

Figure 4: The *Export Custom Routes* and *Import Custom Routes* Checkboxes



6. Select *Create*.

Further details on the VPC network peering setup are covered in the Google Cloud documentation.

Using the gcloud Command

VPC Network Peering can also be created through this gcloud command:

gcloud compute networks peerings create NAME --network=NETWORK
--peer-network=PEER_NETWORK [--async] [--auto-create-routes]
[--export-custom-routes] [--export-subnet-routes-with-public-ip]
[--import-custom-routes] [--import-subnet-routes-with-public-ip]
[--peer-project=PEER_PROJECT] [GCLOUD_WIDE_FLAG …]
gcloud compute networks peerings create

Setting up the SAP-managed VPC

SAP will need to perform the changes in the SAP-managed VPC similar to the steps described above based on the support request you submitted to SAP's customer-facing personnel. The VPC Network Peering will not become active until the setup is completed by SAP.

Using Private Google Access

A benefit of connecting your SAP-managed resources to Google Cloud is that you can take advantage of Google Cloud services. When accessing Google Cloud Storage, for example, you can utilize Private Google Access to avoid traffic traversing the Internet. This is enabled by default on the SAP-managed VPC. We recommend enabling it on the customer-managed VPC as well.

Sharing partner interconnect

You can share a partner interconnect to Google Cloud across RISE with SAP S/4HANA Cloud, private edition or SAP Enterprise Cloud Services and customer projects. Follow the recommended setup using a customer-managed transit VPC to enable the connectivity from RISE with SAP S/4HANA Cloud, private edition and SAP Enterprise Cloud Services to on-premises systems.

Testing connectivity

Once the peering has been set up in both the customer project and the SAP-managed project, it's time to test it. A simple test case is to ping the SAP-managed hosts from a VM in the customer VPC and ping a customer VM from an SAP-managed VM. Make sure to maintain firewall rules to allow for the traffic across the peered network and to review general troubleshooting steps for VPC Network Peering.

Additional considerations

Bear in mind the following recommendations and guidelines when implementing VPC Network Peering:

- If disaster recovery (DR) VPCs are used, then VPC Network Peering should also be requested for DR VPCs in both the customer and SAP-managed VPCs.
- Routes through VPC Network Peering will be the preferred routing if the same routes are also available through VPN or cloud interconnect connections to VPCs hosted in RISE with SAP S/4HANA Cloud, private edition or SAP Enterprise Cloud Services.
- Some subnets in the private CIDR range provided to SAP are consumed for Google Cloud Filestore and database and application backup solutions. These subnets are not visible through VPC Network Peering in the routes advertised by VPCs hosted in RISE with SAP S/4HANA Cloud, private edition or SAP Enterprise Cloud Services.
- SAP may implement firewall rules at the subnet level but not at the port level. This is due to the fact that ports consumed by each service may vary (as in TCP/IP Ports of All SAP Products). SAP therefore recommends implementing firewall rules in the customer transit VPC. Connect with SAP's customer-facing personnel for more details.

Get up to speed on Google Cloud networking

The setup to connect your RISE with SAP S/4HANA Cloud, private edition and SAP Enterprise Cloud Services systems to your Google resources can be performed securely and efficiently using VPC Network Peering. In addition to allowing partner or interconnects to be reused, the setup keeps your information encrypted within the Google network and enables additional security features in Google Cloud, such as third-party firewalls and network package inspection. For customers of the RISE with SAP offering, VPC Network Peering is yet another tool that accelerates and simplifies the business transformation journey.

Technical documentation & resources

VPC Network Peering Overview
Using VPC Network Peering
Private Google Access
Best practices and reference architectures for VPC design
Centralized network appliances on Google Cloud