Configuring Private Google Access for on-premises hosts

Private Google Access for on-premises enables your on-premises hosts to reach Google APIs and services (https://developers.google.com/apis-explorer/) through a Cloud VPN (https://cloud.google.com/vpn/docs) tunnel or Cloud Interconnect (https://cloud.google.com/interconnect/docs) connection. Hosts don't need an external IP address.

Google Cloud offers two VIP (virtual IP address) ranges for private connectivity: *restricted.googleapis.com* (`199.36.153.4/30`) and *private.googleapis.com* (`199.36.153.8/30`). For more information about each VIP range, refer to Private Google Access-specific domain names and VIPs (https://cloud.google.com/vpc/docs/private-access-options#private-vips).

Before you begin

- You must enable the APIs (https://support.google.com/cloud/answer/6158841?hl=en) that you want to access through the APIs & services page (https://console.cloud.google.com/apis/dashboard) in the Google Cloud Console.
- Project owners, editors, and IAM members with the Network Admin (https://cloud.google.com/compute/docs/access/iam#compute.networkAdmin) role can create or update subnets and assign IP addresses. For more information on roles, read the IAM roles (https://cloud.google.com/compute/docs/access/iam) documentation.
- Private Google Access requires a VPC network (https://cloud.google.com/vpc/docs/vpc). Both auto and custom mode VPC networks are supported. Legacy networks (https://cloud.google.com/vpc/docs/legacy) are not supported.
- For the route, firewall, and DNS configurations, choose whether to use the `restricted.googleapis.com` (`199.36.153.4/30`) or `private.googleapis.com` (`199.36.153.8/30`) domain name and VIP range. For more information, refer to Domain names and VIPs (https://cloud.google.com/vpc/docs/private-access-options#domain-vips).
- Your VPC network is already connected to your on-premises network by using a Cloud VPN (https://cloud.google.com/vpn/docs) tunnel or Cloud Interconnect

(https://cloud.google.com/interconnect/docs) connection.

- Your VPC network must have a route for traffic destined to `199.36.153.4/30` or `199.36.153.8/30` (depending on the VIP you use) whose next hop is the default Internet gateway. You can do this by using the default route (https://cloud.google.com/vpc/docs/routes#routingpacketsinternet) or a custom static route.

Setting up Private Google Access for on-premises hosts

To set up Private Google Access for on-premises hosts, you must complete the following tasks:

- You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection. For more information, see Configuring routes (#configuring-routes). If you have multiple tunnels or interconnects, you can't create cross-region asymmetric routes back to your on-premises network. Google Cloud doesn't support them.
- You must configure firewall rules on your on-premises firewall to allow traffic from your on-premises hosts to reach a particular VIP range. For more information, see Configuring firewall rules (#configuring-firewall).
- You must configure DNS so that traffic to Google APIs resolves to to correct domain name (`restricted.googleapis.com` or `private.googleapis.com`). For more information, see Configuring DNS (#configuring-dns).

Configuring routes

Cloud Router custom advertisements

You can use a Cloud Router custom route advertisement (https://cloud.google.com/router/docs/how-to/advertising-custom-ip) to announce the ***VIP_RANGE*** (`199.36.153.4/30` or `199.36.153.8/30`) to your on-premises network. Even though these are public IP address ranges, Google doesn't advertise routes to them publicly. These IP address ranges are only accessible to on-premises hosts that can reach your VPC network through internal IP addresses, such as through a Cloud VPN tunnel or Cloud Interconnect connection.

You can configure a custom route advertisement for all BGP sessions on the Cloud Router or just select a BGP session (for example, for a single Cloud VPN tunnel or VLAN attachment).

To create a custom route advertisement for a particular VIP range for all BGP sessions on an existing Cloud Router:

CONSOLE GCLOUD

1. Go to the Cloud Router page in the Google Cloud Console.
   CLOUD ROUTER LIST (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/INTERCONNECT/ROUTERS/LIST)
2. Select the Cloud Router to update.
3. In the Cloud Router's detail page, select **Edit**.
4. Expand the **Advertised routes** section.
5. For the **Routes**, select **Create custom routes**.
6. Select **Advertise all subnets visible to the Cloud Router** to continue advertising the subnets available to the Cloud Router. Enabling this option mimics the Cloud Router's default behavior.
7. Select **Add custom route** to add an advertised route.
8. Configure the route advertisement.
   - **Source** — Select **Custom IP range** to specify a custom IP range.
   - **IP address range** — Specify ***VIP_RANGE***.
   - **Description** — Add a description for this advertisement.
9. After you're done adding routes, select **Save**.

To create a custom route advertisement for particular VIP range on a specific BGP session of an existing Cloud Router:

CONSOLE GCLOUD

1. Go to the Cloud Router page in the Google Cloud Console.
   CLOUD ROUTER LIST (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/INTERCONNECT/ROUTERS/LIST)
2. Select the Cloud Router that contains the BGP session to update.
3. In the Cloud Router's detail page, select the BGP session to update.
4. In the BGP session details page, select **Edit**.
5. For the **Routes**, select **Create custom routes**.

6. Select **Advertise all subnets visible to the Cloud Router** to continue advertising the subnets available to the Cloud Router. Enabling this option mimics the Cloud Router's default behavior.
7. Select **Add custom route** to add an advertised route.
8. Configure the route advertisement.
    - **Source** — Select **Custom IP range** to specify a custom IP range.
    - **IP address range** — Specify ***VIP_RANGE***.
    - **Description** — Add a description for this advertisement.
9. After you're done adding routes, select **Save**.

VPC network route requirement

Your VPC network must have a route for traffic destined to a VIP range whose next hop is the default internet gateway. In a newly created VPC network, you can use the default route (https://cloud.google.com/vpc/docs/routes#routingpacketsinternet); however, you can also create a custom static route (https://cloud.google.com/vpc/docs/using-routes#addingroute) whose destination is the chosen VIP range and whose next hop is the default internet gateway. Creating a custom static route is required if you remove the default route.

Configuring firewall rules

You must configure your on-premises firewall rules to allow traffic from your on-premises hosts to reach the *restricted* or *private* VIP range.

Configuring DNS

Configure DNS to resolve `*.googleapis.com` as a CNAME to ***DOMAIN_NAME*** (either `restricted.googleapis.com` or `private.googleapis.com`), and create the appropriate A record for ***DOMAIN_NAME***.

Important: Clients cannot make HTTP requests directly to URLs that include either `restricted.googleapis.com` or `private.googleapis.com`. You must configure DNS as described in this section so that clients continue making requests to the appropriate host name of the Google API or service, such as `www.googleapis.com` or `storage.googleapis.com`. This ensures that the `Host` header in an HTTP request is what the Google API or service expects.

You can use either a Cloud DNS managed private zone with a Cloud DNS inbound forwarding policy, or you can configure a DNS name server in your on-premises network, such as BIND (https://www.wikipedia.org/wiki/BIND).

- Cloud DNS private DNS zones enable you to host a DNS zone accessible from authorized VPC networks and, if you configure forwarding, from certain on-premises name servers. You can create a private zone for `googleapis.com` with an `A` record for ***DOMAIN_NAME*** and a CNAME record that directs `*.googleapis.com` to ***DOMAIN_NAME***. Cloud DNS private zones do not support partial overrides, which means that you can only choose to redirect **all** requests to `*.googleapis.com` to ***DOMAIN_NAME***. As a result, you won't be able to use any Google APIs and services that do not support use of your chosen domain name. For more information, see Managing Zones (https://cloud.google.com/dns/zones/).
- You can't use BIND and the `restricted.googleapis.com` or `private.googleapis.com` domain for Dataflow because DNS resolution of Dataflow can't be customized.

Configuring DNS with Cloud DNS

To enable DNS resolution for Private Google Access by using Cloud DNS, use the following procedure:

GCLOUD

1. Create a managed private zone and authorize it to be used by your VPC network.

```
gcloud dns managed-zones create apis \
    --visibility private \
    --networks https://www.googleapis.com/compute/v1/projects/[PROJECT_ID]/gl
    --dns-name googleapis.com \
    --description "Private Google APIs access"
```

2. Create a policy and enable inbound forwarding for your VPC network.

```
gcloud beta dns policies create apipolicy \
    --networks https://www.googleapis.com/compute/v1/projects/[PROJECT_ID]/gl
    --enable-inbound-forwarding \
    --description "enable inbound forwarding for Private Google APIs"
```

3. Start a transaction.

```
gcloud dns record-sets transaction start -z apis
```

4. Add DNS records.

```
gcloud dns record-sets transaction add --name=*.googleapis.com. \
    --type=CNAME DOMAIN_NAME. --zone apis --ttl 300
```

```
gcloud dns record-sets transaction add --name=DOMAIN_NAME \
    --type=A IP_ADDRESS_1 IP_ADDRESS_2 IP_ADDRESS_3 IP_ADDRESS_4\
    --zone apis --ttl 300
```

The following example creates a DNS record for the `private.googleapis.com` domain:

```
gcloud dns record-sets transaction add --name=private.googleapis.com. \
    --type=A 199.36.153.8 199.36.153.9 199.36.153.10 199.36.153.11 \
    --zone apis --ttl 300
```

5. Execute the transaction.

```
gcloud dns record-sets transaction execute --zone apis
```

6. In your on-premises network, point your on-premises DNS to the Cloud DNS forwarder IP address. To find the forwarder IP address, use the `compute addresses list` command:

```
gcloud compute addresses list --filter='name ~ ^dns-forwarding.*' \
    --format='csv[no-heading](address, subnetwork)'
```

★ **Note:** Your VPC network only has a forwarder IP address if you have configured an inbound DNS forwarding policy for it. For more information about DNS policies, see the Cloud DNS overview (https://cloud.google.com/dns/docs/overview#dns-server-policy) and Creating a DNS policy that enables inbound DNS forwarding (https://cloud.google.com/dns/zones/#creating_a_dns_policy_that_enables_inbound_dns_forwarding)
.

Configuring DNS with BIND

If you use BIND (https://www.wikipedia.org/wiki/BIND) for your on-premises DNS resolution, you can configure it to redirect requests for `*.googleapis.com` to a particular domain name by using

response policy zones (https://wikipedia.org/wiki/Response_policy_zone) (RPZ), as shown in the following BIND configuration:

Note: If you use Dataflow, you can't customize it's DNS resolution.

1. Add the following lines to `/etc/bind/named.conf`:

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
```

2. Add the following lines to `/etc/bind/named.conf.options`:

```
options {
  directory "/var/cache/bind";

  dnssec-validation no;

  auth-nxdomain no;    # conform to RFC 1035
  listen-on-v6 { any; };
  listen-on { any; };
  response-policy { zone "googleapis.zone"; };
  allow-query { any;};
};
```

3. Add the following lines to `/etc/bind/named.conf.local`:

```
include "/etc/bind/named.conf.default-zones";

zone "googleapis.zone" {
  type master;
  file "/etc/bind/db.googleapis.zone";
  allow-query {none;};
};
```

4. Add the following lines to `/etc/bind/db.googleapis.zone`:

```
$TTL 1H
@                       SOA LOCALHOST. noreply.localhost(1 1h 15m 30d 2h)
                        NS  LOCALHOST.
```

```
*.googleapis.com CNAME DOMAIN_NAME.
DOMAIN_NAME CNAME rpz-passthru.
```

What's next

- If you also want VMs that are using internal, private IP addresses in your GCP VPC network to access Google APIs, see Configuring Private Google Access for VPC (https://cloud.google.com/vpc/docs/configure-private-google-access/)

Last updated January 13, 2020.