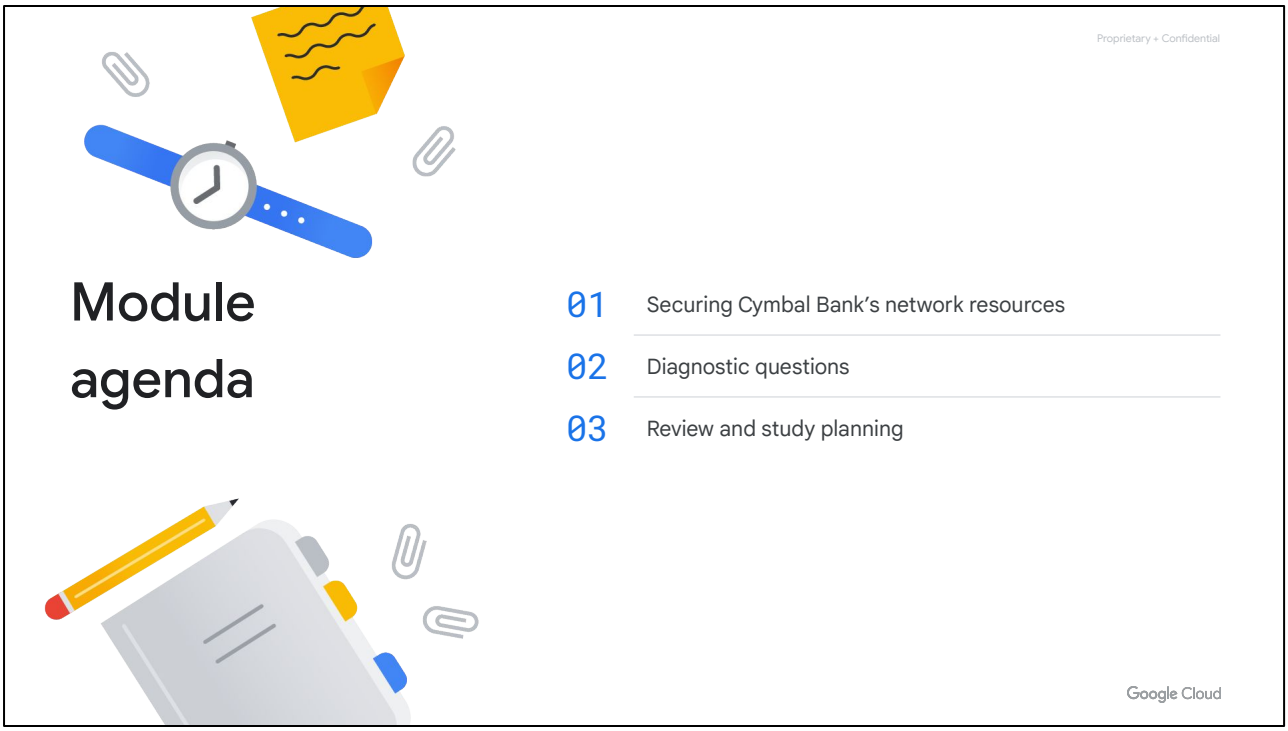
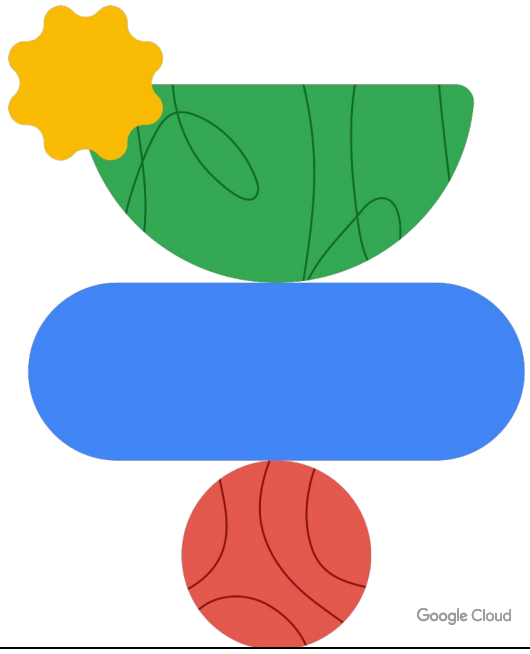
In this module, you'll learn about another area of the Professional Cloud Security Engineer's role at Cymbal Bank. Network security is a critical aspect of overall system security and helping secure networks and network resources will be an important part of the tasks performed by a Professional Cloud Security Engineer. This corresponds to the second section of the Professional Cloud Security Engineer Exam Guide.



As in the previous module, we'll begin by exploring what this aspect of your role looks like at Cymbal Bank. Next, you'll assess your skills in this section through 10 diagnostic questions.

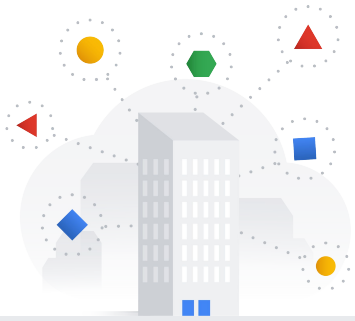
Then, we'll review these questions. Based on the areas you need to learn more about, you'll identify resources to include in your study plan.

Securing Cymbal Bank's network resources



Let's explore how a Professional Cloud Security Engineer at Cymbal Bank helps secure a network and network resources.

Securing Cymbal Bank's network resources



- Designing and configuring perimeter security
- Configuring boundary segmentation
- Establishing private connectivity

Cymbal Bank

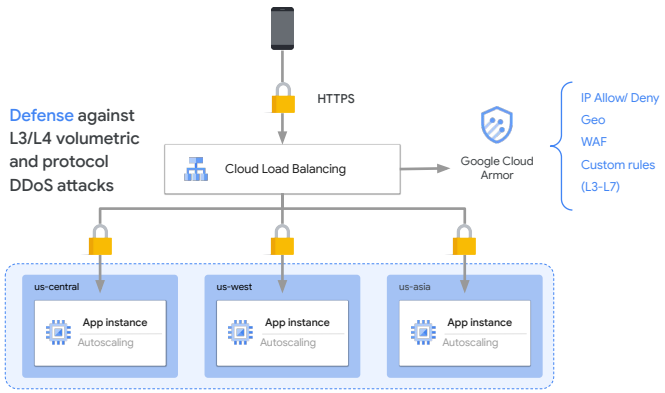
In the previous module, we started with designing identity management and access control for Cymbal Bank. Now your role as a Professional Cloud Security Engineer continues with helping to secure Cymbal Bank's networks and network resources.

Some general patterns can be applied to facilitate securing networks. Keeping most traffic private with limited or no direct exposure of most resources to the internet ensures that attackers have very few attack points from the internet. Resources that are exposed to the internet are the most vulnerable.

Protect these resources with a web application firewall, such as Google Cloud Armor in Google Cloud. This will allow you to monitor traffic for patterns indicating invalid or attack traffic - and block or filter such traffic.

Private networks can leverage isolation or segmentation to restrict the type of communication that can happen internally in your organization. This means that ports and protocols use for standard workloads are not exposed to the public internet and potential bad actors. You can use service identity to ensure that only valid, authenticated traffic can travel within your private networks.

Configure Application Load Balancers and Google Cloud Armor



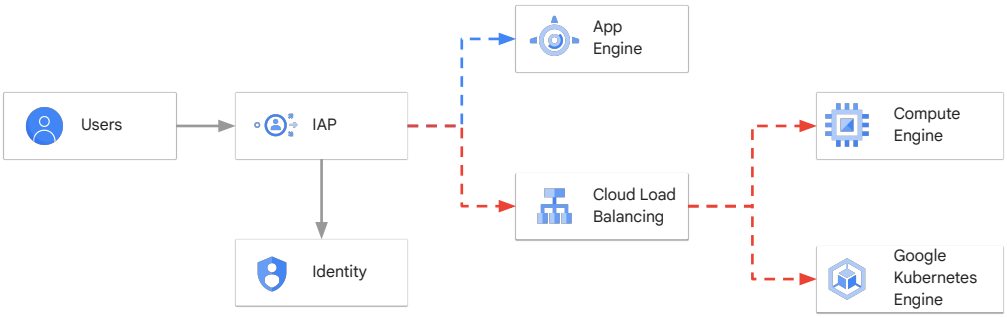
- Provide Layer 7 DDoS defense
- Protect against SQL injection attacks
- Protect against XSS injection attacks
- Configure rules for filtering traffic

Cymbal Bank expects attacks against any endpoints that are accessible from the public internet. Cloud Load Balancing can provide protection against Layer 3 (Network layer) and Layer 4 (Transport layer) attacks. Google Cloud Armor provides a configurable managed service that is integrated with the external Application Load Balancer and the classic Application Load Balancer, and protects against Layer 7 (Application layer) attacks.

Google Cloud Armor protects against SQL injection, XSS injection, and similar attacks. You can also configure Google Cloud Armor to filter traffic based on request properties. Traffic through Google Cloud Armor can also be throttled with configurable rate limits, or challenged with reCAPTCHA for bot management or to further protect against DDoS.

Cymbal Bank will attempt to ensure the majority of traffic arriving at Cymbal Bank services from the public internet goes through the Application Load Balancer and Google Cloud Armor to provide this extra protection.

Connect through Identity-Aware Proxy



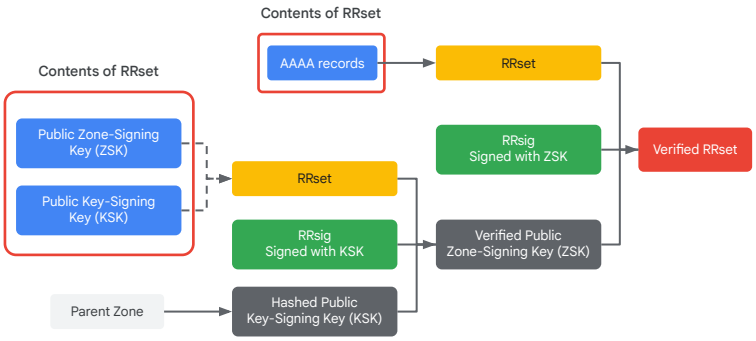
When Cymbal Bank users need to connect via the public internet to resources or services via HTTPS or any TCP protocol (including SSH) that require authenticated and authorized access, they will connect through the Identity-Aware Proxy (IAP).

IAP lets you manage access to any services deployed in Google Cloud with an authentication and authorization layer for your applications. You can use Google-managed identities with Google authentication or SAML2 federated single sign-on. You can also use external identities and other types of SSO when combining the Identity-Aware Proxy with Identity Platform.

Protect public DNS zones

Cloud DNS supports DNSSEC to secure the DNS resources and prevent attackers from manipulating DNS responses.

- Ensures authenticated DNS responses to DNS requests
- Automatically manages DNSSEC related DNS records
- Integrates with DNSSEC at the domain registrar level



Cymbal Bank will ensure security of their public DNS zones to prevent attackers from poisoning or manipulating DNS responses to DNS requests sent to these public DNS zones by activating DNSSEC.

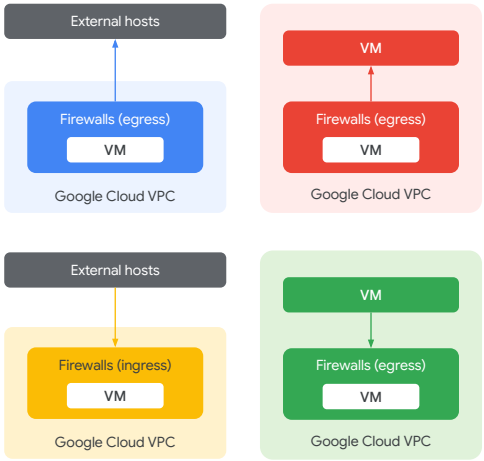
Cloud DNS ensures authenticated DNS responses to DNS requests and automatically manages DNSSEC-related DNS records.

DNSSEC is supported by Cloud DNS and also by Google Domains, Google's domain registration and registry service. Cymbal Bank will activate DNSSEC in both services to ensure security of your public DNS.

Limit VPC traffic with Firewall rules

Cymbal Bank will use firewall rules to only allow valid and expected traffic between workloads, and block all other traffic.

- Stateful rules handle requests in either the ingress or egress direction.
- Firewall rules can defined from source service accounts to target service accounts.
- Firewall rules can be applied in a hierarchical manner to ensure uniform application across projects.



Cymbal Bank will utilize firewall rules to only allow valid and expected network traffic between IP addresses, ports, and protocols used by actual workloads. You will use firewall rules to block all other traffic.

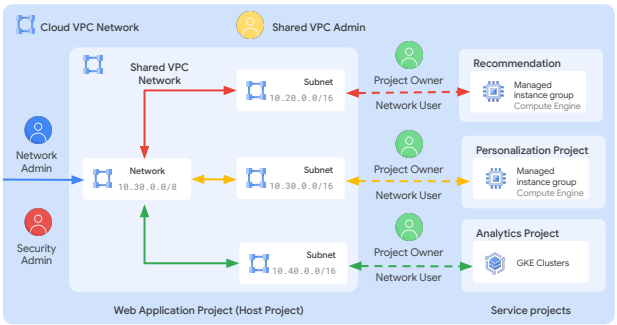
Stateful rules handle requests in either the ingress or egress direction.

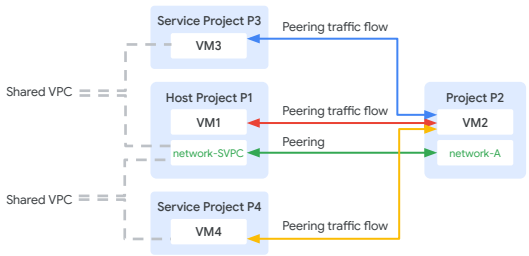
Wherever possible, you will define firewall rules to restrict traffic to specific source and target service accounts.

You will also use hierarchical firewall rules to ensure uniform application of rules across projects.

Isolate networks to secure workloads

Cymbal Bank will connect privately across projects using shared VPC and VPC peering.





Cymbal Bank will use private IP address communication between all resources within Google Cloud. This will happen primarily inside shared VPC networks. Shared VPC provides centralized network administration and allows resources from large numbers of projects to communicate via a single VPC.

Some Cymbal Bank projects may also have standalone VPCs when running isolated ephemeral workloads. These isolated standalone networks can be VPC peered to the shared VPC networks if they need to communicate with standard workloads running in the shared VPC networks.

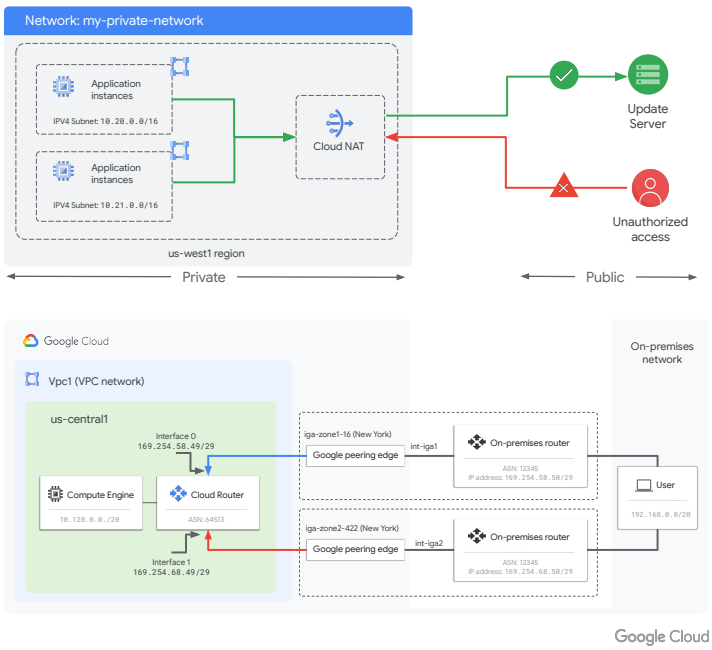
VPC peering provides decentralized network administration and allows VPCs to be connected across projects or even organizations.

Keep traffic private where possible

Cymbal Bank will connect privately from on-premises into Google Cloud to Google APIs or the wider Internet.

You will use:

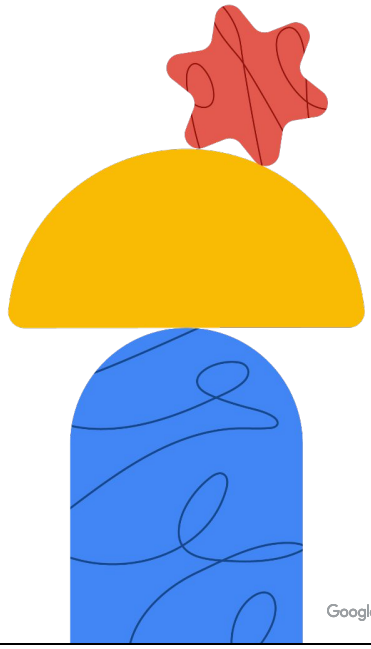
- Cloud VPN and Interconnect
- Google private access
- Cloud NAT



Cymbal Bank will connect privately from on-premises into Google Cloud to Google APIs or the wider Internet.

- Cloud VPN and Interconnect provide private IP communication from on-premises networks to Google Cloud. Cymbal Bank will utilize private IP communication from office and data center networks into Google Cloud via Cloud VPN and Interconnect.
- Google private access enables private IP communication to Google APIs. You will use Google private access to make requests to Google APIs privately from inside Google Cloud or from office and data center private networks.
- Cloud NAT allows resources with only internal IP addresses to make requests to the public Internet. All Cymbal Bank workloads will make internet bound requests through Cloud NAT allowing them to only be given internal IP addresses.

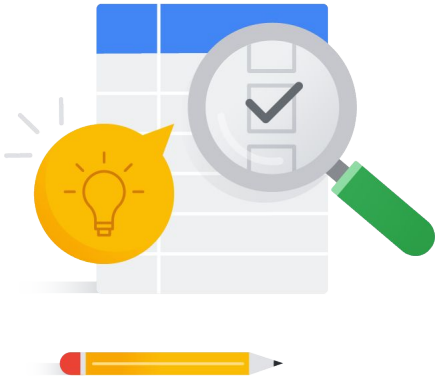
Diagnostic questions



Now it’s your turn to assess your experience and skills related to this section with some diagnostic questions. Remember, the purpose of these questions is to help you better understand what is involved in this section of the exam guide and identify which areas you’ll want to focus on in your study plan.

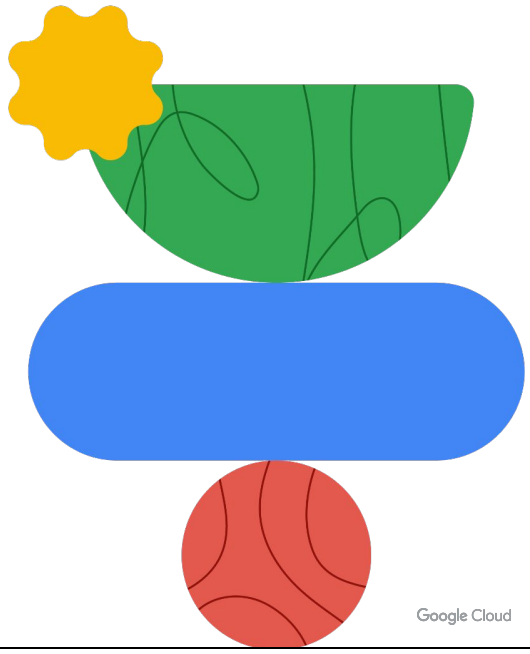
Please complete the diagnostic questions now

- The diagnostic questions are available in the workbook.



Please take 15 minutes to complete the diagnostic questions for this section.

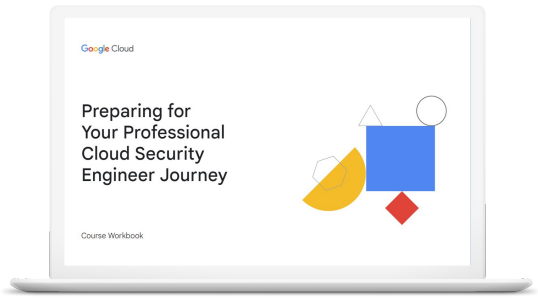
Review and study planning



Now let’s review how to use these diagnostic questions to help you identify what to include in your study plan.

Your study plan:

Securing Communications and Establishing Boundary Protection



2.1 Designing and configuring perimeter security

2.2 Configuring boundary segmentation

2.3 Establishing private connectivity

We'll approach this review by looking at the key areas of this exam section and the questions you just answered about each one. We'll talk about where you can find out more about each area in the learning path for this certification and/or where to find the information in Google Cloud documentation.

As we go through each one, take notes on the specific courses (and modules!), skill badges, and documentation pages you'll want to emphasize in your study plan.

2.1 Designing and configuring perimeter security

Considerations include:

- Configuring network perimeter controls (e.g., Cloud Next Generation Firewall [Cloud NGFW] rules and policies Identity-Aware Proxy [IAP], load balancers, and Certificate Authority Service)
- Setting up application layer inspection on Cloud NGFW (e.g., layer 7)
- Differentiating between private and public IP addressing
- Configuring web application firewalls (e.g., Google Cloud Armor)
- Deploying Secure Web Proxy
- Configuring Cloud DNS security settings
- Continually monitoring and restricting configured APIs

As Professional Cloud Security Engineer, you are expected to help design and configure network security.

You tested your knowledge of securing load balancers and backends using firewall rules in question 1, and using SSL policies and certificates in question 2. Question 3 explored how to use IAP to authenticate and control access to services deployed to Google Cloud.

2.1 Diagnostic Question 01 Discussion

Cymbal Bank has published an API that internal teams will use through the Application Load Balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

Feedback:
A. Correct! Action should be set to throttle, rate-limit-threshold-count must be 200, and rate-limit-threshold-interval-sec for 1 hour must be 60 seconds X 60 = 3600 seconds. A 429 error code will convey to the user that they have placed too many requests.

B. Incorrect. This command will set the throttle limit to 200 API calls per minute instead of per hour. Error code 404 will indicate that the resource was not found, which is not the error code you want to convey. Action should be allowed, not denied.

C. Incorrect. Rate-based-ban would be helpful if you wanted to disable the incoming services for a time period. You need a throttle limit. Error 403 is incorrect; it indicates invalid authorization, which is not your use case. Action should be allowed, not denied.

D. Incorrect. Rate-based-ban would be helpful if you wanted to disable the incoming services for a time period. You need a throttle limit. Error 500 indicates internal server error, which would mean your API had an exception or failure, which is not the expected outcome.

Where to look:
- https://cloud.google.com/sdk/gcloud/reference/compute/security-policies/rules/update
- https://cloud.google.com/sdk/gcloud/reference/compute/security-policies

Content mapping:
Partial coverage in:

- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security
  - M8 Securing Google Kubernetes Engine: Techniques and Best Practices
  - M9 Protecting Against DDOS Attacks

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Security Best Practices in Google Cloud**
  - M4 Securing Google Kubernetes Engine: Techniques and Best Practices

- On-demand course: **Mitigating Security Vulnerabilities on Google Cloud**
  - M1 Protecting Against DDOS Attacks

- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging
  - M9 Controlling Access to VPC Networks
  - M11 Hybrid Load Balancing and Traffic Management

- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M3 Network Monitoring and Logging

- On-demand course: **Networking in Google Cloud: Network Security**
  - M2 Controlling Access to VPC Networks

- On-demand course: **Networking in Google Cloud: Load Balancing**
  - M1 Hybrid Load Balancing and Traffic Management

- Skill badge: Build and Secure Networks in Google Cloud

Summary:
Google Cloud Armor provides capabilities to help protect your Google Cloud applications against a variety of Layer 3 and Layer 7 attacks. Google Cloud Armor security policies filter incoming traffic that is destined to an external Application Load Balancer or a classic Application Load Balancer. Rate-based rules help you protect your applications from a large volume of requests that flood your instances and block access for legitimate users.

2.1 Diagnostic Question 02 Discussion

Cymbal Bank is releasing a new loan management application using a Compute Engine managed instance group. External users will connect to the application using a domain name or IP address protected with TLS 1.2. A load balancer already hosts this application and preserves the source IP address. You are tasked with setting up the SSL certificate for this load balancer.

What should you do?

A. Create a Google-managed SSL certificate. Attach a global dynamic external IP address to the internal Application Load Balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

B. Create a Google-managed SSL certificate. Attach a global static external IP address to the global external Application Load Balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

C. Import a self-managed SSL certificate. Attach a global static external IP address to the external proxy Network Load Balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create a TCP proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

D. Import a self-managed SSL certificate. Attach a global static external IP address to the external proxy Network Load Balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an SSL proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

Feedback:

A. Incorrect. Internal Application Load Balancers cannot be directly accessed from the public internet. They are designed to distribute traffic within a Virtual Private Cloud (VPC) network, and they do not have a public IP address.

B. Correct! A Google-managed SSL certificate provides secure communication with external users, and attaching a global static external IP address allows external users to access the application using a fixed IP address. Validating that the existing URL map routes incoming traffic to the managed instance group backend ensures that the application is correctly configured to receive requests. Creating an HTTPS proxy routing to the URL map allows the global external Application Load Balancer to terminate SSL connections from external users and forward the traffic to the backend application, while the global forwarding rule directs incoming requests to the load balancer, making the application accessible from the public internet.

C. Incorrect. While this solution could work, it isn't the best solution. While TCP proxy routing can be used with an external Proxy Network Load Balancer, it's generally recommended to use HTTPS proxy routing when using SSL certificates. HTTPS proxy routing ensures that the load balancer terminates SSL connections and handles the encryption/decryption process, providing better security and performance. To ensure that the load balancer can handle SSL traffic correctly, the URL map should also be configured to use the HTTPS protocol, not TCP.

D. Incorrect. While SSL proxy routing can be used with an external Proxy Network

Load Balancer, it's generally recommended to use HTTPS proxy routing when using SSL certificates, especially in scenarios where performance and security are critical. HTTPS proxy routing ensures that the load balancer terminates SSL connections and handles the encryption/decryption process, providing better security and performance. To ensure that the load balancer can handle SSL traffic correctly, the URL map should also be configured to use the HTTPS protocol, not TCP. Additionally, HTTPS proxy routing can offer benefits such as centralized certificate management, load balancing capabilities, and simplified configuration.

Where to look:

- https://cloud.google.com/load-balancing/docs/https/ext-https-lb-simple
- https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs#load-balancer

Content mapping:
Partial coverage in:

- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

Summary:
When dealing with external HTTPS traffic, you need an external HTTPS load balancer for end-to-end TLS and SSL support. An HTTPS load balancer lets you create HTTPS proxy routing that forwards requests to the appropriate backend. External users can reach this proxy with the help of global forwarding rules.

2.1 Diagnostic Question 03 Discussion

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

Feedback:
A. Incorrect. You need ingress and not egress firewall rules.

B. Incorrect. SOCKS proxy must be created on the server side for applications to be discovered. Applying this solution will set up the opposite of what you need.

C. Incorrect. This approach will expose your Compute Engine instance to the public internet. Anyone will be able to access your Compute Engine instance, not just your on-premises developer.

D. Correct! IAP TCP forwarding establishes an encrypted tunnel that supports both SSH and RDP requests.

Where to look:

- https://cloud.google.com/iap/docs/using-tcp-forwarding#preparing_your_project_for_tcp_forwarding
- https://cloud.google.com/solutions/connecting-securely#preventing_vms_from_being_reached_from_the_public_internet

Content mapping:

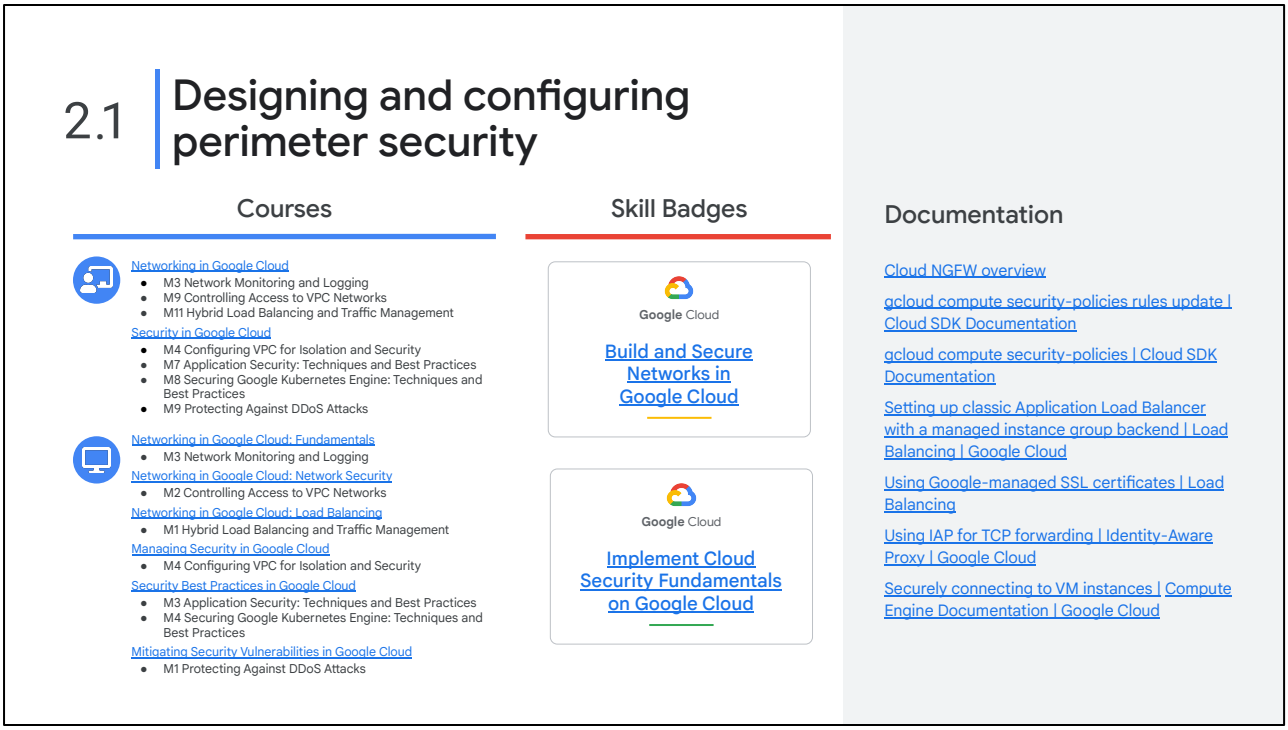
- ILT course: **Security in Google Cloud**
  - M7 Application Security: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**

    - M3 Application Security: Techniques and Best Practices

- Skill badges:
    - Build and Secure Networks in Google Cloud
    - Implement Cloud Security Fundamentals on Google Cloud

Summary:
Cloud Identity-Aware Proxy (IAP) can help manage users and VM instances that users can connect to. Users and groups can connect to Cloud IAP first and can access the underlying permitted resources after authorization. Users and Group access can be controlled at the Project level using IAM.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/firewall/docs/about-firewalls
- https://cloud.google.com/sdk/gcloud/reference/compute/security-policies/rules/update
- https://cloud.google.com/sdk/gcloud/reference/compute/security-policies
- https://cloud.google.com/load-balancing/docs/https/ext-https-lb-simple
- https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs#load-balancer
- https://cloud.google.com/iap/docs/using-tcp-forwarding#preparing_your_project_for_tcp_forwarding
- https://cloud.google.com/solutions/connecting-securely#preventing_vms_from_being_reached_from_the_public_internet

2.2 Configuring boundary segmentation

Considerations include:

- Configuring security properties of a VPC Network, VPC Peering, Shared VPC, and Firewall Rules
- Configuring network isolation and data encapsulation for N-tier applications
- Identifying use cases and configuring VPC Service Controls

A Professional Cloud Security Engineer needs to understand the considerations involved in configuring network segmentation.

Question 4 tested your knowledge of securing Cloud DNS zones using DNSSEC. Question 5 asked you to apply firewall rules with service accounts to secure applications. Question 6 examined the use of VPC subnets for secure resource communication and isolation.

2.2 Diagnostic Question 04 Discussion

You have recently joined Cymbal Bank as a cloud engineer. You created a custom VPC network, selecting to use the automatic subnet creation mode and nothing else. The default network still exists in your project. You create a new Linux VM instance and select the custom VPC as the network interface. You try to SSH into your instance, but you are getting a "connection failed" error.

What answer best explains why you cannot SSH into the instance?

A. You should have deleted the default network. When you have multiple VPCs in your project, Compute Engine can't allow you to connect because overlapping IP ranges prevent the API from establishing a root connection.

B. You should have used the default network when setting up your instance. While custom networks support instance creation, they should only be used for internal communication.

C. You should have used custom subnet creation mode. Since the default VPC still exists, automatic mode created subnets in the same regions, which led to overlapping IP addresses.

D. You did not set up any firewall rules on your custom VPC network. While the default VPC comes with a predefined firewall rule that allows SSH traffic, these need to be added to any custom VPCs.

Feedback:
A. Incorrect. You are allowed to have multiple VPCs in your project. When creating custom subnetwork with auto creation mode, Google Cloud ensures that there are no overlapping CIDR ranges.

B. Incorrect. You do not need to create VM instances using the default network. Custom networks allow for internal and external network traffic.

C. Incorrect. Creating your subnets in the custom network with auto mode ensures that there will be no overlapping IP ranges across your subnets.

D. Correct! You did not create any firewalls to allow SSH traffic.

Where to look:
- https://cloud.google.com/vpc/docs/firewalls

Content mapping:
- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security
  - M5 Securing Compute Engine: Techniques and Best Practices

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine

- ILT course: **Networking in Google Cloud**
  - M1 VPC Networking Fundamentals
  - M4 Network Routing and Addressing

- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M1 VPC Networking Fundamentals

- On-demand course: **Networking in Google Cloud: Routing and Addressing**
  - M1 Network Routing and Addressing

Summary:
The default network is pre-populated with firewall rules that allow incoming connections to instances. These allow you to connect to instances with tools such as SSH, RDP, ping, and also allow for communication between VM instances within the same VPC network.

You need to create similar firewall rules for networks other than the default network.

2.2 Diagnostic Question 05 Discussion

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

B. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

C. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

D. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

Feedback:
A. Correct! Use service accounts to automate the identification, authentication, and authorization process between the n-tier services. Allow TCP protocol on the port for reading.

B. Incorrect. In order to work with a database, you need TCP connection. ICMP can only send error codes and operational messages.

C. Incorrect. You need a service account, not a user account, to automate the templates for the database.

D. Incorrect. You need service accounts, not user accounts, to automate the templates for both the database and the application. This request will deny the database access instead of allowing it. UDP is an incorrect protocol to connect to a database for transactions.

Where to look:
- https://cloud.google.com/vpc/docs/using-firewalls#serviceaccounts

Content mapping:
- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security
  - M8 Securing Google Kubernetes Engine

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Security Best Practices in Google Cloud**
  - M4 Securing Google Kubernetes Engine

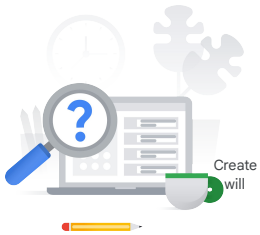
- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging
  - M9 Controlling Access to VPC Networks

- On-demand course: Networking in Google Cloud: **Fundamentals**
  - M3 Network Monitoring and Logging

- On-demand course: Networking in Google Cloud: **Network Security**
  - M2 Controlling Access to VPC Networks

Summary:
Only one firewall rule set is applied on all the subnets in the same network. When resources are in various subnets of the same network, you can create service accounts for each of those resources and apply firewall rules at the service account level.

2.2 Diagnostic Question 06 Discussion



Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

C. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

Feedback:
A. Incorrect. Create one service account for each resource with fine-grained limited permissions. Each application has a specific task, and it's rare for multiple applications to require the same access and permissions. Following the principle of least privileges, provide only limited access to each service account separately.

B. Incorrect. For the firewall rule to allow clients to access the Fraud Detection App, other Compute Engine instances should be the source, and the Compute Engine instance hosting the app should be the target.

C. Correct! Using subnet isolation, you have to authorize every request entering your subnet. The recommended solution is to create a firewall rule that allows only a limited set of service accounts to access the shared target.

D. Incorrect. Target filtering can help with selecting the right resources to apply firewall rules. However, creating an ingress tag to all resources does not achieve the desired communication flow between the API and the database.

Where to look:

- https://cloud.google.com/architecture/best-practices-vpc-design#isolate-data
- https://cloud.google.com/architecture/best-practices-vpc-design#isolate-vms-service-accounts
- https://cloud.google.com/iam/docs/best-practices-for-securing-service-accounts

Content mapping:

- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- ILT course: **Networking in Google Cloud**
  - M1 VPC Networking Fundamentals
  - M2 Sharing VPC Networks
  - M9 Controlling Access to VPC Networks

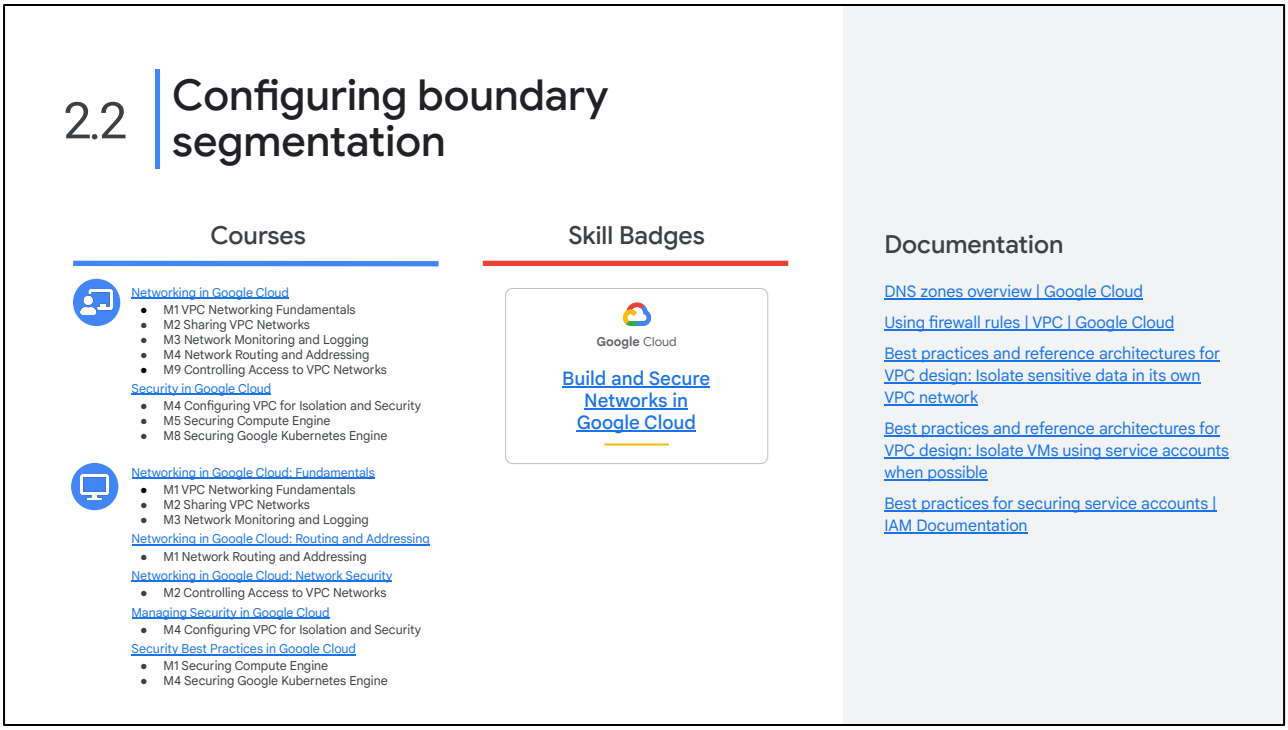
- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M1 VPC Networking Fundamentals
  - M2 Sharing VPC Networks

- On-demand course: **Networking in Google Cloud: Network Security**
  - M2 Controlling Access to VPC Networks

- Skill badge: Build and Secure Networks in Google Cloud

Summary:

VPCs allow secure communication between resources. The specific rules for resource communication should be added to the firewall. Firewalls can use target filtering with the help of tags or subnet isolation. Subnet isolation with the help of service accounts is the recommended method for this situation.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/dns/docs/zones/zones-overview#peering_zones
- https://cloud.google.com/vpc/docs/using-firewalls#serviceaccounts
- https://cloud.google.com/architecture/best-practices-vpc-design#isolate-data
- https://cloud.google.com/architecture/best-practices-vpc-design#isolate-vms-service-accounts
- https://cloud.google.com/iam/docs/best-practices-for-securing-service-accounts

2.3 Establishing private connectivity

Considerations include:

- Designing and configuring private connectivity between VPC networks and Google Cloud Projects (Shared VPC, VPC Peering, and Private Google Access for on-premises hosts)
- Designing and configuring private connectivity and encryption between data centers and VPC network (e.g.,HA-VPN, and Cloud Interconnect)
- Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premises hosts, restricted Google access, Private Service Connect)
- Using Cloud NAT to enable outbound traffic

As a Professional Cloud Security Engineer, you will need to design and configure private connectivity and encryption between networks using Shared VPC, VPC Peering, HA-VPN, and Cloud Interconnect. You also need to establish private connectivity between a VPC and Google CPAs.

Question 7 tested your knowledge of using NAT IP address ranges to ensure secure connectivity between a Shared VPC and connectors. Question 8 asked you to differentiate between options to connect between on-premises applications and Google Cloud. Question 9 tested your ability to set up an environment for on-premises users to access Google Cloud privately. Question 10 tested your knowledge of Cloud NAT.

2.3 Diagnostic Question 07 Discussion

The data from Cymbal Bank's loan applicants resides in a shared VPC. A credit analysis team uses a CRM tool hosted in the App Engine standard environment. You need to provide credit analysts with access to this data. You want the charges to be incurred by the credit analysis team.

What should you do?

A. Add egress firewall rules to allow TCP and UDP ports for the App Engine standard environment in the Shared VPC network. Create either a client-side connector in the Service Project or a server-side connector in the Host Project using the IP Range or Project ID of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

B. Add egress firewall rules to allow SSH and/or RDP ports for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the IP range of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

C. Add ingress firewall rules to allow NAT and Health Check ranges for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

D. Add ingress firewall rules to allow NAT and Health Check ranges for App Engine standard environment in the Shared VPC network. Create a server-side connector in the Host Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

Feedback:
A. Incorrect. You need to use the NAT and Health Check IP address ranges for the App Engine standard environment. In order to communicate to a shared VPC, you need to create ingress firewall rules.

B. Incorrect. This command would work if the VPC was not a Shared VPC. Also, in order to communicate to a shared VPC, you need to create ingress rules in Firewall.

C. Correct! App Engine uses a fixed set of NAT and health check IP address ranges that must be permitted into the VPC. Because the charges must be incurred by the credit analysis team, you need to create the connector on the client side.

D. Incorrect. Creating a connector in the server side will incur charges to the Host Project instead of to the credit analysis team's project.

Where to look:
- https://cloud.google.com/appengine/docs/standard/python3/connecting-shared-vpc
- https://cloud.google.com/vpc/docs/configure-serverless-vpc-access#create-connector

Content mapping:
- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- ILT course: **Networking in Google Cloud**
  - M2 Sharing VPC Networks

- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M2 Sharing VPC Networks

- Skill badges:
  - Build and Secure Networks in Google Cloud
  - Implement Cloud Security Fundamentals on Google Cloud

Summary:
App Engine standard environment uses NAT IP address ranges and Health Checks that ensure secure connectivity between a Shared VPC and connectors. These ranges, 107.178.230.64/26 and 35.199.244.0/19, along with Health Check ranges, are the origin of requests from Cloud Run, Cloud Run functions, and the App Engine standard environment.

Use these ranges to create ingress Firewall rules in a Shared VPC to allow connectors from the App Engine standard environment.

2.3 Diagnostic Question 08 Discussion

Cymbal Bank's Customer Details API runs on a Compute Engine instance with only an internal IP address. Cymbal Bank's new branch is co-located outside the Google Cloud points-of-presence (PoPs) and requires a low-latency way for its on-premises apps to consume the API without exposing the requests to the public internet.

Which solution would you recommend?

A. Use a Content Delivery Network (CDN). Establish direct peering with one of Google's nearby edge-enabled PoPs.

B. Use Carrier Peering. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

C. Use Partner Interconnect. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

D. Use Dedicated Interconnect. Establish direct peering with one of Google's nearby edge-enabled PoPs.

Feedback:
A. Incorrect. CDNs can help direct traffic and static content from VPCs and are cached on the edge. CDNs still need an internet connection.

B. Incorrect. Carrier Peering would require a public IP address attached to the Compute Engine instance.

C. Correct! When you are co-located in one of the Google Cloud PoPs, use Dedicated Interconnect. Otherwise, use Partner Interconnect to connect to Google Cloud with a private IP address.

D. Incorrect. You can only use Dedicated Interconnect if you are co-located in Google Cloud PoPs.

Where to look:
- https://cloud.google.com/vpc-service-controls/docs/overview#hybrid_access
- https://cloud.google.com/network-connectivity/docs/how-to/choose-product

Content mapping:
- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security
- On-demand course: **Managing Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

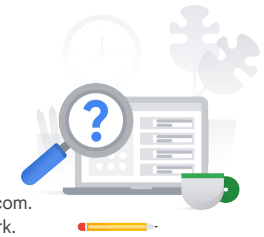
- ILT course: **Networking in Google Cloud**
  - M13 Connectivity Options

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
  - M1 Connectivity Options

Summary:
You can connect to Google Cloud resources using private IP addresses with Interconnect. If you are co-located in Google Cloud Points-of-presence (PoPs), you can use Dedicated Interconnect and configure VLAN attachments on-premises.

If you are located outside of the PoP edge locations, you need to use Partner Interconnect. Partner Interconnect provides an intermediate access point, which then provides connectivity to Google Cloud.

2.3 Diagnostic Question 09 Discussion



An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Dedicated Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

Feedback:
A. Incorrect. Use DNS forwarding to connect to external DNS. VPCs will not accept broadcast or multicast IP addresses. A software-defined firewall has application-level controls only. This solution doesn't meet the requirement to connect to Google Cloud.

B. Incorrect. Using Interconnect for a one-time audit is an expensive choice. Additionally, you will need to add records for both private.googleapis.com and restricted.googleapis.com. Instead, create records for *.googleapis.com.

C. Correct! Cloud VPN provides a cost-effective and easily set-up environment for on-premises users to access Google Cloud privately. Using *.googleapis.com enables requests for both private.googleapis.com and restricted.googleapis.com. Use Cloud Router to set up and announce Google Cloud routes on-premises.

D. Incorrect. Using Interconnect for a one-time audit is an expensive choice. Additional static routes are required if the default routing has changed.

Where to look:
- https://cloud.google.com/vpc/docs/private-google-access#pga-supported
- https://cloud.google.com/dns/docs/zones#create-private-zone
- https://cloud.google.com/vpc/docs/private-google-access-hybrid

Content mapping:
- ILT course: **Security in Google Cloud**

    - M4 Configuring Virtual Private Cloud for Isolation and Security
    - M5 Securing Compute Engine: Techniques and Best Practices

- On-demand course: **Managing Security in Google Cloud**
    - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Security Best Practices in Google Cloud**
    - M1 Securing Compute Engine: Techniques and Best Practices

- ILT course: **Networking in Google Cloud**
    - M14 Cloud VPN

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
    - M2 Cloud VPN

- Skill badge: Implement Cloud Security Fundamentals on Google Cloud

Summary:
Cloud VPN and Interconnect are ideal options for private connectivity. Use Cloud VPN if initial setup and cost are challenges, but latency is acceptable. Use Interconnect for dedicated long-term usage for large throughput.

You also need to configure DNS records and on-premises routing, for which you can use Cloud DNS and Cloud Router. The private usage requires announcing and adding routes on-premises for private.googleapis.com and restricted.googleapis.com.

After the Firewall rules have been configured on-premises and on the VPC, the VPC containing the private resources will be accessible to on-premises systems. If you are using a default VPC, the VPC will contain a default route. Otherwise, you will also need to add custom static routes for private Google Cloud access.

2.3 Diagnostic Question 10 Discussion

An ecommerce portal uses Google Kubernetes Engine to deploy its recommendation engine in Docker containers. This cluster instance does not have an external IP address. You need to provide internet access to the pods in the Kubernetes cluster. What configuration would you add?

What should you do?

A. Cloud DNS, subnet primary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

B. Cloud VPN, subnet secondary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

C. Nginx load balancer, subnet secondary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

D. Cloud NAT gateway, subnet primary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

Feedback:
A. Incorrect. Cloud DNS is required for domain name resolution; it cannot decide upon internet access.

B. Incorrect. You need to set the primary, not secondary, IP address range for nodes. Cloud VPN would be used if you need to connect on-premises users to the GKE cluster, which is not the requirement.

C. Incorrect. Load balancers help with distributing incoming traffic between machines. You need an outbound connection.

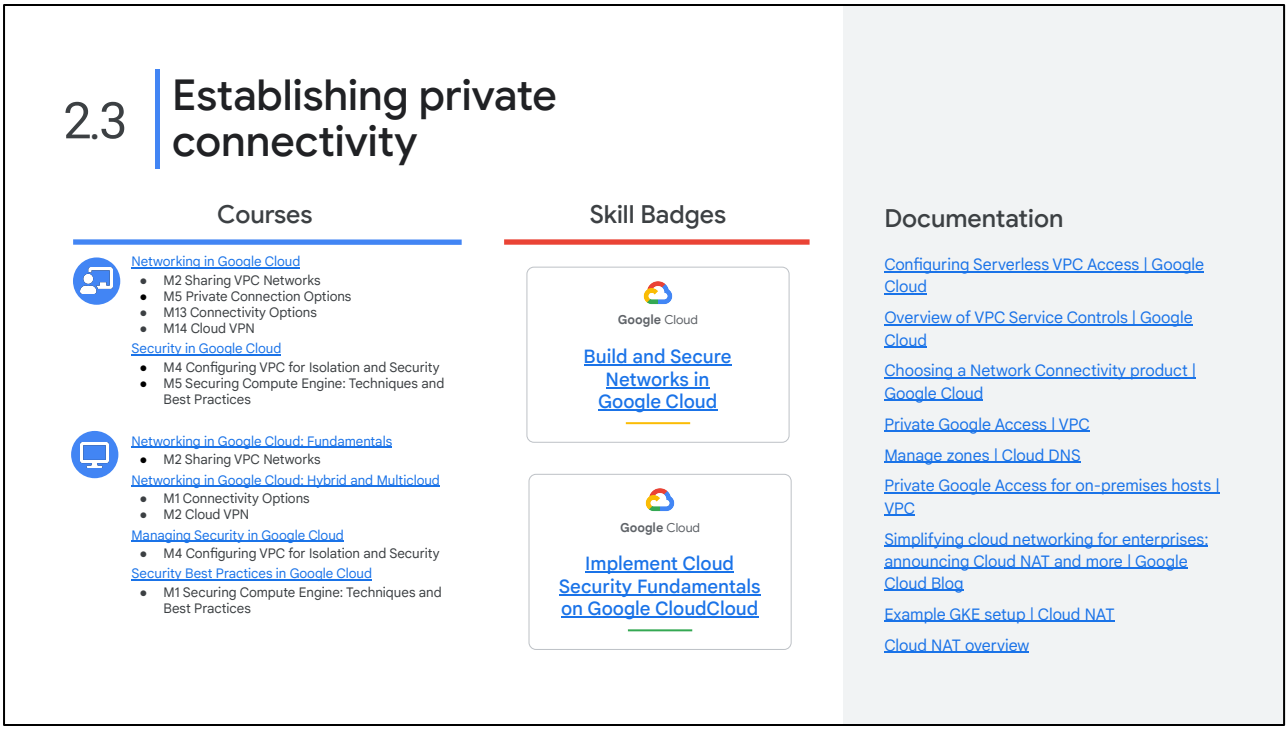
D. Correct! Cloud NAT gateways help provide internet access (outbound) without requiring a public IP address.

Where to look:
- https://cloud.google.com/blog/products/networking/simplifying-cloud-networking-for-enterprises-announcing-cloud-nat-and-more
- https://cloud.google.com/nat/docs/gke-example
- https://cloud.google.com/nat/docs/overview

Content mapping:
- ILT course: **Networking in Google Cloud**
  - M5 Private Connection Options

- On-demand course: **Networking in Google Cloud: Routing and Addressing**
    - M2 Private Connection Options

Summary:
Cloud NAT can provide outbound internet access to certain resources such as Compute Engine, Google Kubernetes Engine, Cloud Run (using Serverless VPC) and Cloud Run functions, and App Engine standard environment.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/appengine/docs/standard/python3/connecting-shared-vpc
- https://cloud.google.com/vpc/docs/configure-serverless-vpc-access#create-connector
- https://cloud.google.com/vpc-service-controls/docs/overview#hybrid_access
- https://cloud.google.com/network-connectivity/docs/how-to/choose-product
- https://cloud.google.com/vpc/docs/private-google-access#pga-supported
- https://cloud.google.com/dns/docs/zones#create-private-zone
- https://cloud.google.com/vpc/docs/private-google-access-hybrid
- https://cloud.google.com/blog/products/networking/simplifying-cloud-networking-for-enterprises-announcing-cloud-nat-and-more
- https://cloud.google.com/nat/docs/gke-example
- https://cloud.google.com/nat/docs/overview