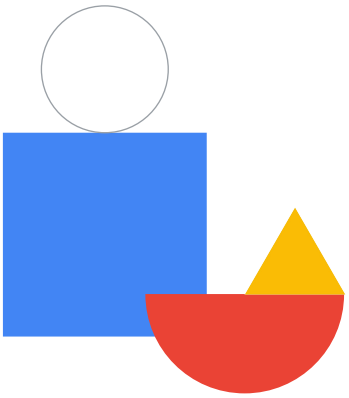
Google Cloud

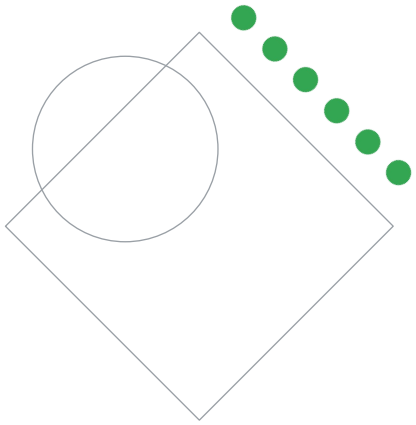


Preparing for Your Professional Cloud Network Engineer Journey

Module 5: Managing, monitoring, and troubleshooting network operations

Welcome to Module 5: Managing, monitoring, and troubleshooting network operations.

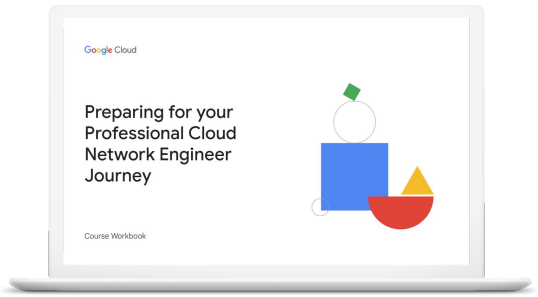
Review and study planning



You'll now review the diagnostic questions and your answers to help you identify what to include in your study plan.

Your study plan:

Managing, monitoring, and troubleshooting network operations



5.1 Logging and monitoring with Google Cloud Observability

5.2 Maintaining and troubleshooting connectivity issues

5.3 Using Network Intelligence Center to monitor and troubleshoot common networking issues

Google Cloud

The diagnostic questions align with these objectives of this exam section. Use the PDF resource that follows to review the questions and how you answered them. Pay specific attention to the rationale for both the correct and incorrect answers. Use the resources detailed under **Where to look** and **Content mapping** to build a study plan that meets your learning needs.

5.1 Logging and monitoring with Google Cloud Observability

Considerations include:

- Enabling and reviewing logs for networking components (e.g., Cloud VPN, Cloud Router, VPC Service Controls, Cloud NGFW, Firewall Insights, VPC Flow Logs, Cloud DNS, Cloud NAT)
- Monitoring metrics of networking components (e.g., Cloud VPN, Cloud Interconnect and VLAN attachments, Cloud Router, load balancers, Google Cloud Armor, Cloud NAT)

Google Cloud

As Professional Cloud Network Engineer, you are expected to help set up and apply processes for logging and monitoring network activity and status.

Question 1 tested your knowledge of using Cloud Logging for networking features, question 2 tested your knowledge of using Cloud Monitoring, and question 3 tested your knowledge of working with logs in Google Cloud.

5.1 Diagnostic Question 01 Discussion

Cymbal Bank needs to log all cache hits and misses for their static assets served from Cloud CDN via an Application Load Balancer backend bucket.

What should you do?

A. Enable logging on the backend bucket and configure logging sample rate to 1.0.

B. Use the default behavior, no configuration required.

C. Enable logging on the backend bucket.

D. Configure the logging sample rate on the backend bucket to 1.0.

Feedback:
A. Incorrect. This would be necessary if the content were served from a backend service, but not for a backend bucket which defaults to your desired behavior.
*B. Correct! Logging all requests served from backend buckets, including whether they were served from cache or not, is default behavior.
C. Incorrect. Backend buckets default to logging enabled (and it cannot be disabled).
D. Incorrect. Backend buckets default to logging 100% of requests (and it cannot be changed).

Where to look:
https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/nat/docs/monitoring
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/vpc-service-controls/docs/audit-logging
https://cloud.google.com/armor/docs/audit-logging
https://cloud.google.com/armor/docs/request-logging

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M12: Caching and Optimizing Load Balancing
- On-demand course: **Networking in Google Cloud: Load Balancing**
  - M2: Caching and Optimizing Load Balancing

- Skill badge: Network Performance and Optimization

Summary:
As with most networking services in Google Cloud there are logs collected related to the functionality of the Application Load Balancer. These logs also include logs related to functionality of the Cloud CDN and Google Cloud Armor, which are tightly integrated with the Application Load Balancer. Backend buckets will provide logs automatically, but backend services require configuration to enable logs and set the logs sampling rate.

5.1 Diagnostic Question 02 Discussion

You are designing a monitoring alert to notify you when a Cloud VPN tunnel approaches the limits for bandwidth.

Select the metrics that would be important to include in the alerting policies.

A. **vpn.googleapis.com/network/sent_bytes_count, vpn.googleapis.com/network/received_bytes_count, vpn.googleapis.com/network/sent_packets_count, vpn.googleapis.com/network/received_packets_count**

B. vpn.googleapis.com/network/dropped_received_packets_count, vpn.googleapis.com/network/network/dropped_sent_packets_count

C. vpn.googleapis.com/network/sent_bytes_count, vpn.googleapis.com/network/received_bytes_count

D. vpn.googleapis.com/network/sent_packets_count, vpn.googleapis.com/network/received_packets_count, vpn.googleapis.com/network/dropped_received_packets_count, vpn.googleapis.com/network/network/dropped_sent_packets_count

Feedback:
*A. Correct! An alert can be set to notify if the tunnel is reaching the bandwidth maximum of 375 MBps or 250,000 packets per second.
B. Incorrect. Dropped packets are not an indication of how close a tunnel is to the bandwidth limits.
C. Incorrect. The bytes count can only notify when the 375 MBps limit is being approached and not the 250,000 packets per second limit.
D. Incorrect. Dropped packets are not an indication of how close a tunnel is to the bandwidth limits and the packets count can only notify when the 250,000 packets per second limit is being approached and not the 375 MBps limit.

Where to look:
https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/nat/docs/monitoring
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/interconnect/how-to/monitoring
https://cloud.google.com/armor/docs/monitoring
https://cloud.google.com/monitoring/api/metrics_gcp

Content mapping:
Skill badge: Network Performance and Optimization

Summary:

Most networking features and functions have associated metrics automatically collected by Cloud Monitoring that can be visually tracked over time via charts/dashboards, or alerted on when crossing safe thresholds. For Cloud VPN tunnel capacity, the limitations in bytes and packets per second can be monitored via the associated bytes and packets counts metrics.

5.1 Diagnostic Question 03 Discussion

Cymbal Bank's network team wants to track and analyze detailed logs of all API calls made to their Google Cloud resources, including timestamps, user identities, and specific actions taken.

Which Google Cloud service is the most appropriate choice for Cymbal Bank's network team to achieve this goal?

A. Cloud Audit Logs

B. Cloud Logging

C. VPC Flow Logs

D. Cloud Monitoring

Feedback:
A. Incorrect! Cloud Audit Logs provides logs of administrative activity and access to data in Google Cloud.
*B. Correct. Cloud Logging is designed to store, search, analyze, monitor, and alert on log data and events from Google Cloud resources and applications. It can capture detailed logs of API calls, providing the information Cymbal Bank needs.
C Incorrect. Cloud Monitoring is primarily used for collecting and visualizing metrics related to the performance and health of cloud resources. It's not designed for capturing and analyzing detailed API call logs.
D. Incorrect. VPC Flow Logs capture information about network traffic within a VPC, but they do not typically include the level of detail needed for API call logs, such as user identities and specific actions.

Where to look:
https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/nat/docs/monitoring
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/interconnect/how-to/monitoring
https://cloud.google.com/armor/docs/monitoring
https://cloud.google.com/monitoring/api/metrics_gcp

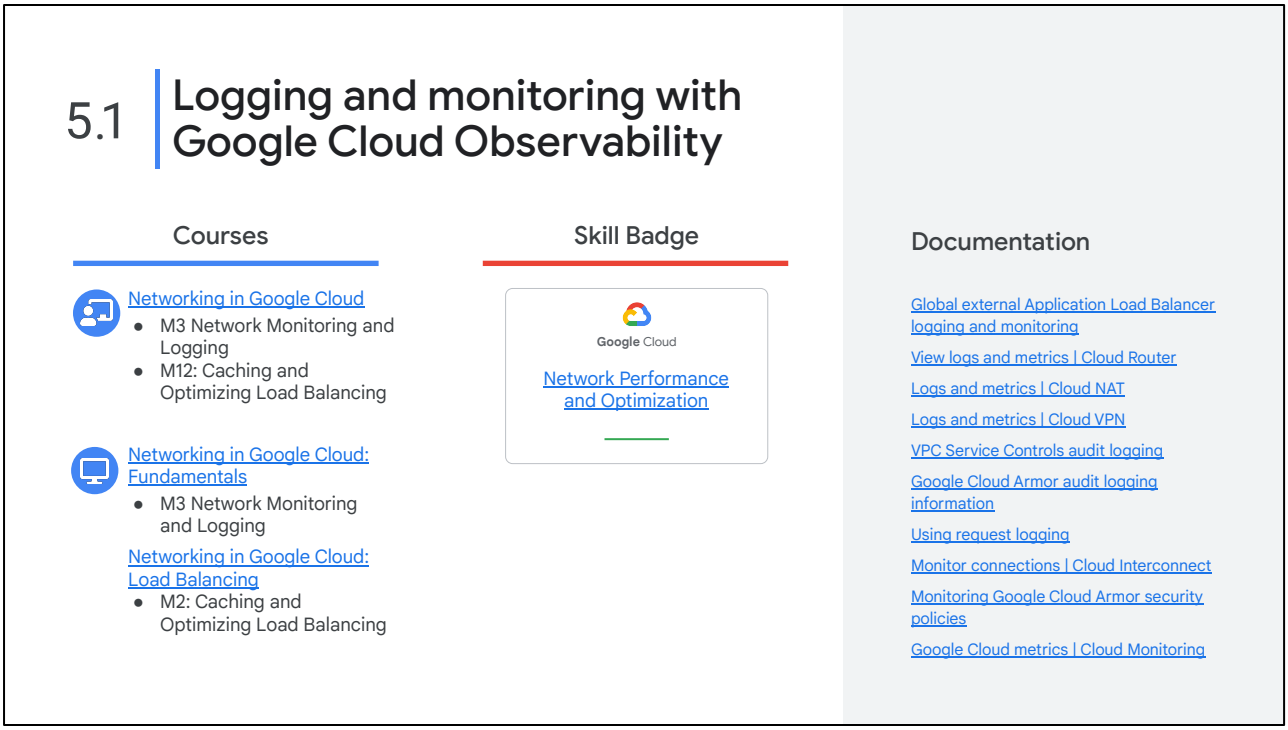
Content mapping:
- ILT course: **Networking in Google Cloud**

    - M3 Network Monitoring and Logging

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

- Skill badge: Network Performance and Optimization

Summary:
Cloud Logging excels at capturing, storing, and analyzing detailed API call logs, providing real-time insights, advanced analysis tools, and robust security and compliance features, making it ideal for monitoring API usage, troubleshooting, and meeting regulatory requirements.



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. 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.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)
Networking in Google Cloud: Load Balancing (On-demand)

Network Performance and Optimization (Skill badge)

https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/nat/docs/monitoring
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/vpc-service-controls/docs/audit-logging
https://cloud.google.com/armor/docs/audit-logging
https://cloud.google.com/armor/docs/request-logging
https://cloud.google.com/network-connectivity/docs/interconnect/how-to/monitoring
https://cloud.google.com/armor/docs/monitoring

https://cloud.google.com/monitoring/api/metrics_gcp

5.2 Maintaining and troubleshooting connectivity issues

Considerations include:

- Draining and redirecting traffic flows with Application Load Balancers
- Tuning and troubleshooting Cloud NGFW rules or policies
- Managing and troubleshooting VPNs
- Troubleshooting Cloud Router BGP peering issues
- Troubleshooting with VPC Flow Logs, Firewall Logs, and Packet Mirroring

Google Cloud

As a Professional Cloud Network Engineer, you should be able to monitor, maintain, debug, and help resolve network connectivity issues.

Question 4 tested your knowledge of monitoring traffic with VPC Flow Logs. Question 5 asked you to apply approaches for monitoring and troubleshooting VPN configurations.
Question 6 tested your knowledge of approaches for troubleshooting Cloud Router BGP peering issues.

5.2 Diagnostic Question 04 Discussion

You are using VPC Flow Logs to analyze traffic arriving at a subnet. You need to capture approximately 10% of the traffic and determine how much traffic originates from outside the subnet. VPC Flow Logs has already been enabled for the subnet. You want to use the least expensive process.

How should you configure VPC Flow Logs?

A. Configure them with a sampling rate of 0.1 and a filter expression for the connection source and destination IP within the IP range of the subnet.

B. Configure them with a sampling rate of 1.0 and a filter expression for the connection source and destination IP within the IP range of the subnet.

C. Configure them with a sampling rate of 0.1 and a filter expression for the connection destination IP within the IP range of the subnet.

D. Configure them with a sampling rate of 1.0 and a filter expression for the connection destination IP within the IP range of the subnet.

Feedback:
A. Incorrect. The sampling rate will set the percentage of the sampled packets that will be logged. A maximum of 10% of packets are sampled, and setting the sampling rate to 0.1 would only log 10% of those for a maximum of 1% of the total traffic. Also, the filter would exclude traffic originating from outside the subnet.
B. Incorrect. The filter would exclude traffic originating from outside the subnet.
C. Incorrect. The sampling rate sets the percentage of the sampled packets that will be logged. A maximum of 10% of packets are sampled, and setting the sampling rate to 0.1 would only log 10% of those for a maximum of 1% of the total traffic.
*D. Correct! This configuration will log 10% of traffic arriving at the subnet. The connection source IP address in these logs can be compared to the subnet IP range to determine what percentage of the traffic came from inside or outside the subnet.

Where to look:
https://cloud.google.com/vpc/docs/flow-logs
https://cloud.google.com/vpc/docs/using-flow-logs

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging

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

- Skill badge: Network Performance and Optimization

Summary:
VPC flow logs can be enabled and configured on a subnet level and capture a maximum of 10% of traffic. That amount can be further reduced by sampling and/or filtering and is aggregated over a configurable period which defaults to 5 seconds. Log entries are created for the aggregate traffic from the period and information about the source and destination IP addresses and ports, the protocol, and other useful information is provided in the log entry.

5.2 Diagnostic Question 05 Discussion

Cymbal Bank has configured a Classic VPN with a policy-based tunnel to connect to a branch office with an older VPN device that does not support BGP. You have completed the configuration of the office VPN and the logs and monitoring suggest that the tunnel is up and functioning correctly. You find when testing with ping and traceroute that you can reach some VMs but not others in the VPC across the tunnel from the office. You can reach some servers but not others in the office from VMs in the VPC. You have verified the firewall configurations in both environments and determined that is not the cause of the problem.

What is the next troubleshooting step you should attempt?

A. Investigate the Cloud Router configuration for advertised subnets.

B. Investigate the Cloud Router BGP session status.

C. Investigate the configuration of the local and remote traffic selectors in the Classic VPN tunnel and office VPN configuration.

D. Search the Classic VPN tunnel logs for IKE events indicating a problem.

Feedback:
A. Incorrect. The Cloud Router would not be used for Classic VPN policy-based tunnel.
B. Incorrect. The Cloud Router would not be used for Classic VPN policy-based tunnel.
*C. Correct! If the firewall configurations are verified as correct, then the configuration of the traffic selectors is the most likely cause of connectivity problems between specific VMs and servers in the VPC and office environments.
D. Incorrect. Logs and monitoring suggest that the tunnel is up and functioning correctly. IKE issues would cause the tunnel not to function at all.

Where to look:
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting

Content mapping:
No coverage in training material.

Summary:
Cloud VPN troubleshooting will depend on the type of Cloud VPN tunnel. Classic VPN is primarily used in static routing configurations to create route-based or policy-based tunnels. When using policy-based tunnels, the local and remote traffic selector configuration may result in only partial connectivity between resources on opposite sides of the tunnel.

5.2 Diagnostic Question 06 Discussion

You are debugging a Layer 2 Partner Interconnect connection that is indicating a failure to create a BGP session in the Cloud Router for the associated VLAN attachments.

Select the most likely cause to investigate when troubleshooting this issue.

A. Check the ASN configuration of the on-premises router and the Cloud Router.

B. Check the BGP keepalive timer configuration of the Cloud Router.

C. Check the route advertisement configuration of the Cloud Router.

D. Check the route configuration of the VPC the Cloud Router is in.

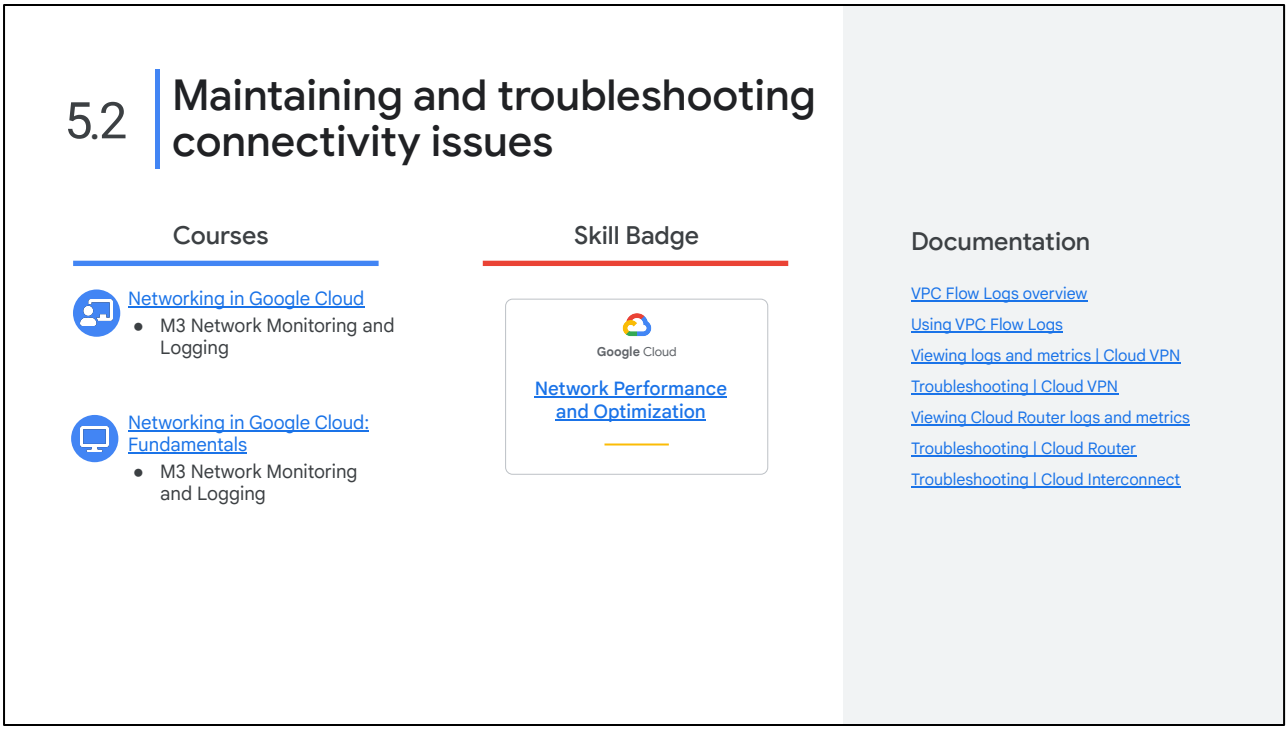
Feedback:
*A. Correct! This is the only available option that could have an impact on BGP session status. The ASN needs to be configured to 16550 in the Cloud Router for Layer 2 Partner Interconnect, and the on-premises router peer ASN should also be configured to that value.
B. Incorrect. This could not be a cause of the BGP session not starting at all.
C. Incorrect. This could not have any impact on BGP session status in the Cloud Router.
D. Incorrect. This could not have any impact on BGP session status in the Cloud Router.

Where to look:
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting
https://cloud.google.com/network-connectivity/docs/interconnect/support/troubleshooting

Content mapping:
No coverage in training material.

Summary:
For Partner Interconnect, all the Cloud Routers must have a local ASN of 16550. Dedicated Interconnect and Cloud VPN do not have this requirement. ASN misconfiguration in the Cloud Router or on-premises router is a common cause of

failure to establish a BGP session in the Cloud Router.



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.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)

Network Performance and Optimization (Skill badge)

https://cloud.google.com/vpc/docs/flow-logs
https://cloud.google.com/vpc/docs/using-flow-logs
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting
https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting
https://cloud.google.com/network-connectivity/docs/interconnect/support/troubleshooting

5.3 Using Network Intelligence Center to monitor and troubleshoot common networking issues

Considerations include:

- Using Network Topology to visualize throughput and traffic flows
- Using Connectivity Tests to diagnose route and firewall misconfigurations.
- Using Performance Dashboard to identify packet loss and latency (e.g., Google-wide, project scoped).
- Using Firewall Insights to monitor rule hit count and identify shadowed rules.
- Using Network Analyzer to identify network failures, suboptimal configurations, and utilization warnings

Google Cloud

A Professional Cloud Network Engineer should be familiar with tools and processes for measuring network performance and troubleshooting network traffic flow issues.

Question 7 assessed your ability to apply troubleshooting approaches for routing issues. Question 8 tested your knowledge of using Network Intelligence Center features for monitoring and troubleshooting.

5.3 Diagnostic Question 07 Discussion

You are trying to debug a connectivity issue between VMs in the same VPC using internal IP addresses. The issue began immediately after configuring routes and firewall rules.

What should you do to troubleshoot the problem?

A. Disable firewall rules one by one in all combinations to determine the problem.

B. Remove static routes one by one in all combinations to determine the problem.

C. Review the packet loss statistics in the Network Intelligence Center performance dashboard.

D. Use Connectivity Tests to determine the connectivity problem.

Feedback:
A. Incorrect. This will be a very high-effort and time-consuming approach, and would not find the problem if it was related to a route issue.
B. Incorrect. This will be a very high-effort and time-consuming approach, and would not find the problem if it was related to a firewall rule issue.
C. Incorrect. This would only be useful to indicate if a problem is caused by a transient Google cloud network issue.
*D. Correct! This is the best approach to quickly determine if a route or firewall rule configuration is causing connectivity problems.

Where to look:
https://cloud.google.com/vpc/docs/routes
https://cloud.google.com/vpc/docs/ts-vm-vm-internal
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting
https://cloud.google.com/network-intelligence-center/docs/connectivity-tests/concepts/overview

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging

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

- Skill badges:
    - Build a Secure Google Cloud Network
    - Implement Cloud Security Fundamentals on Google Cloud
    - Network Performance and Optimization

Summary:
Routing problems can be caused by misconfiguring VPC routes, firewall rules, firewall software, VPNs, interconnect links, or Cloud Routers. Routing problems can also be caused by malfunctioning or misconfigured software, or transient Google Cloud networking issues. The Network Intelligence Center includes these tools: Network Topology, Connectivity Tests, Performance Dashboard, Firewall Insights, and Network Analyzer. Use these tools to help identify transient Google Cloud networking issues, as well as VPC or hybrid link configuration problems.

5.3 Diagnostic Question 08 Discussion

You are a network administrator responsible for monitoring and troubleshooting networking issues in Cymbal Bank's Google Cloud environment. You want to use Network Intelligence Center to identify and resolve common networking problems.

Which of the following capabilities does Network Intelligence Center provide to help you monitor and troubleshoot common networking issues? (Select TWO correct options.)

A. **Real-time network topology visualization**
B. Automated network configuration management
C. **Flow logs analysis for traffic visibility**
D. Predictive network failure alerts
E. Firewall rule recommendations

Feedback:
*A. Correct! Network Intelligence Center allows you to visualize your network topology in real-time, making it easier to identify potential bottlenecks or misconfigurations.
B. Incorrect. While Google Cloud offers tools for automated network configuration management, this is not a core capability of Network Intelligence Center.
*C. Correct. By analyzing flow logs, Network Intelligence Center provides insights into network traffic patterns, which can help you identify and troubleshoot issues such as excessive latency or packet loss.
D. Incorrect. Network Intelligence Center focuses on providing real-time and historical data for troubleshooting. It does not currently offer predictive network failure alerts.
E. Incorrect. While Google Cloud offers tools for firewall rule management and recommendations, this is not a primary function of Network Intelligence Center.

Where to look:
https://cloud.google.com/network-intelligence-center/docs/performance-dashboard/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-topology/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-topology/reference/metrics-reference
https://cloud.google.com/network-intelligence-center/docs/connectivity-tests/concepts/overview

https://cloud.google.com/network-intelligence-center/docs/network-analyzer/overview

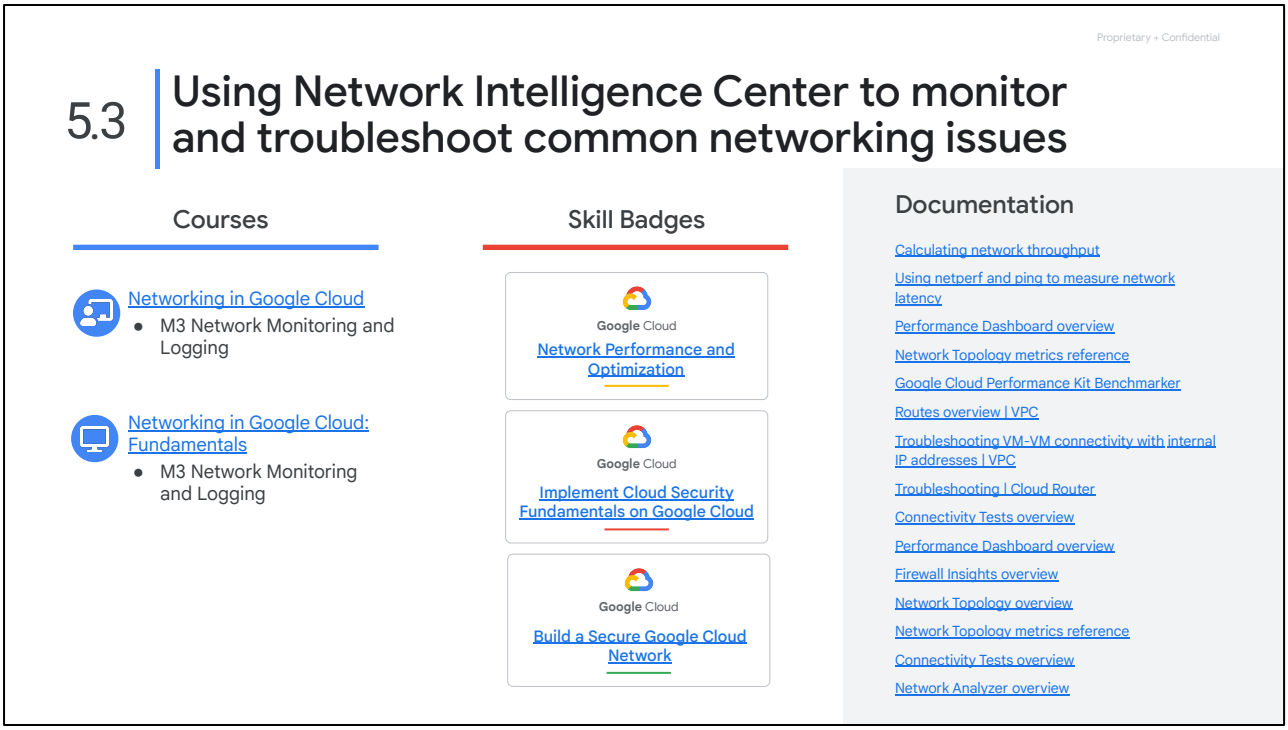
Content mapping:

- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging

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

- Skill badge: Implement Cloud Security Fundamentals on Google Cloud

Summary:
Network Intelligence Center tools provide simple network monitoring and debugging capabilities to help identify problems, as well as monitor performance of your VPC networks and connectivity to on-premises networks. The Network Topology tool provides a topological visualization of your VPC networks and the infrastructure within, as well as links to on-premises networks and the internet. The tool also provides metrics on traffic and latency between resources and across links. The Performance Dashboard tool provides metrics on packet loss and latency between zones within and across regions. The Connectivity Tests tool provides static and dynamic connectivity tests to verify if the network configuration is blocking connectivity. The Firewall Insights tool provides details and metrics about the behavior of the firewall configuration. The Network Analyzer tool automatically monitors your Virtual Private Cloud (VPC) network configurations and detects misconfigurations and suboptimal configurations.



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.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)

Network Performance and Optimization (Skill badge)
Implement Cloud Security Fundamentals on Google Cloud (Skill badge)
Build a Secure Google Cloud Network (Skill badge)

https://cloud.google.com/community/tutorials/network-throughput
https://cloud.google.com/blog/products/networking/using-netperf-and-ping-to-measure-network-latency
https://cloud.google.com/network-intelligence-center/docs/performance-dashboard/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-topology/reference/metrics-reference
https://github.com/GoogleCloudPlatform/PerfKitBenchmarker

https://cloud.google.com/vpc/docs/routes
https://cloud.google.com/vpc/docs/ts-vm-vm-internal
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting
https://cloud.google.com/network-intelligence-center/docs/connectivity-tests/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/performance-dashboard/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-topology/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-topology/reference/metrics-reference
https://cloud.google.com/network-intelligence-center/docs/connectivity-tests/concepts/overview
https://cloud.google.com/network-intelligence-center/docs/network-analyzer/overview