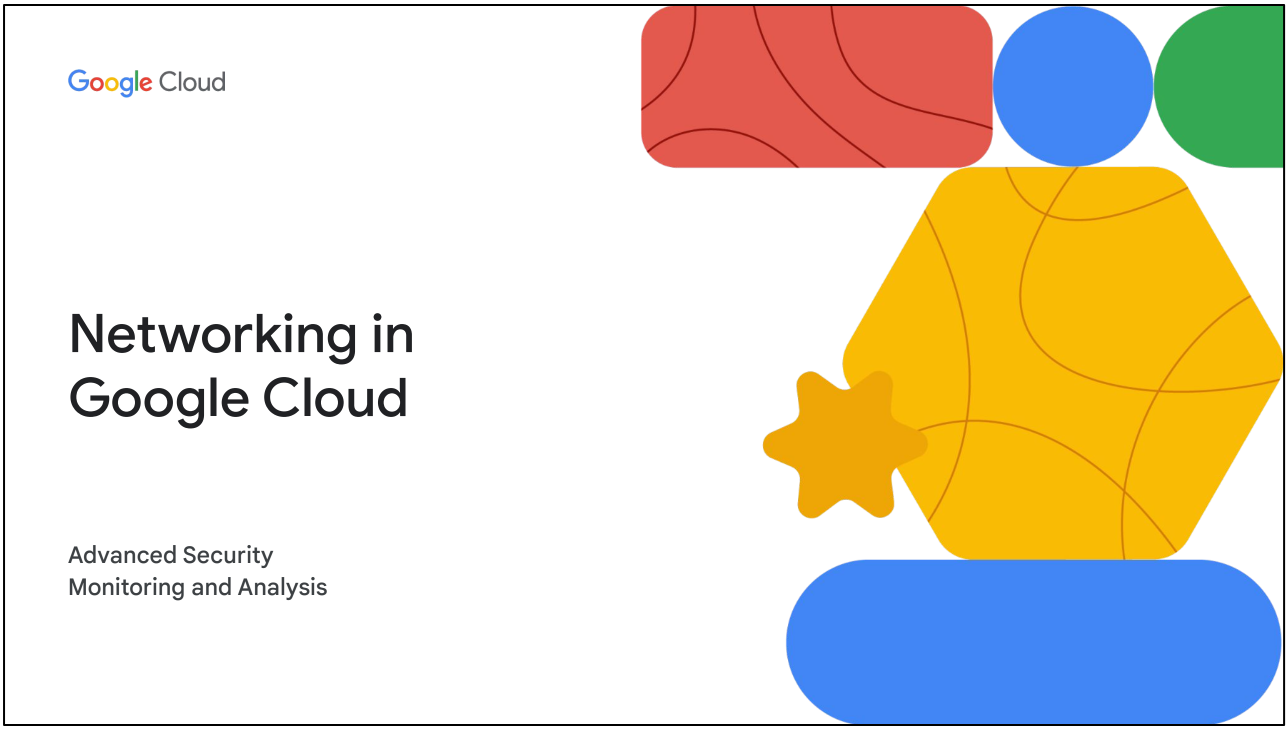
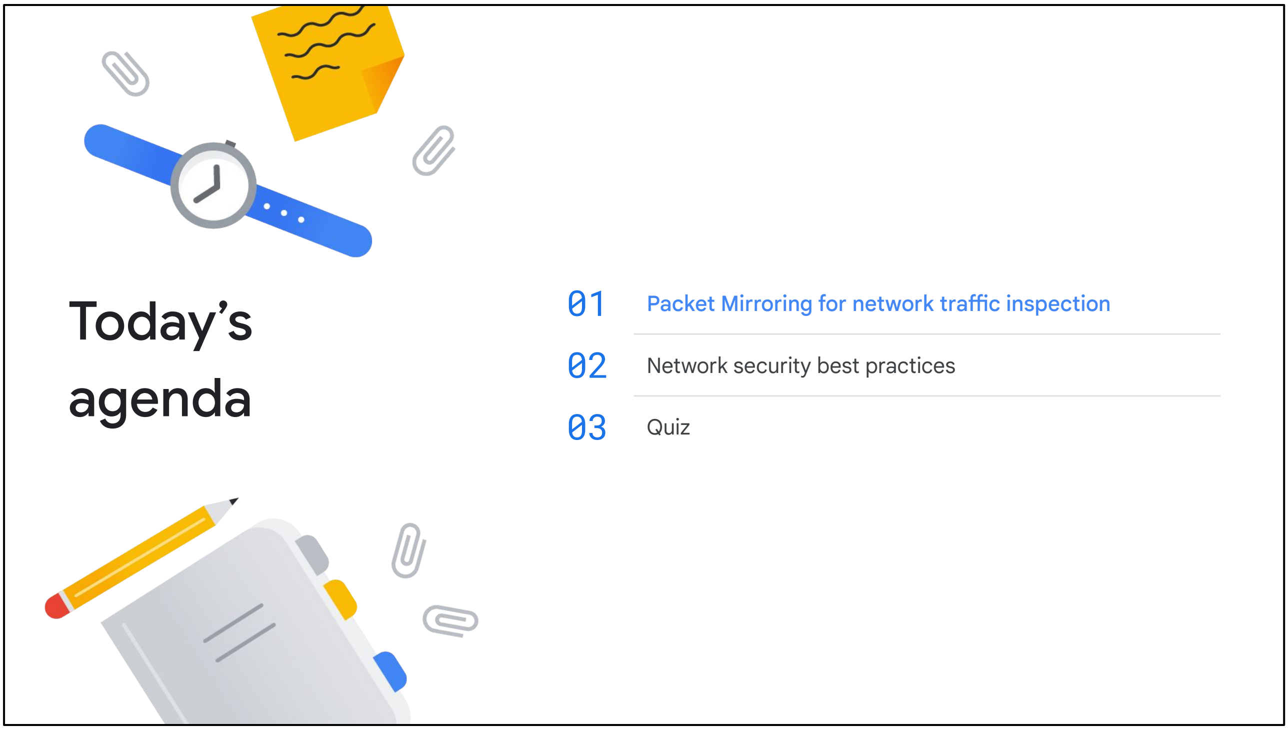


Google Cloud

Networking in Google Cloud

Advanced Security
Monitoring and Analysis

Welcome to the Advanced Security Monitoring and Analysis module.



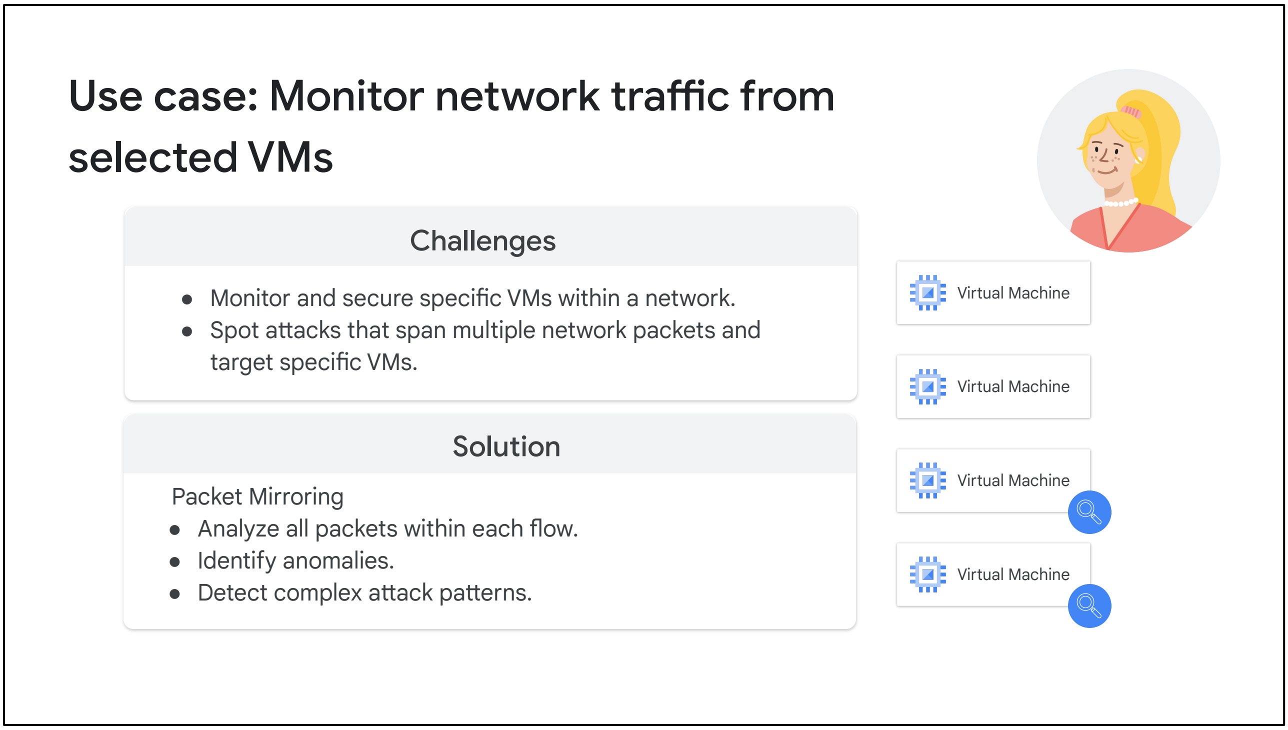
Today's agenda

01 Packet Mirroring for network traffic inspection

02 Network security best practices

03 Quiz

This module provides an overview of packet mirroring for enhanced network security. Learn how to leverage this tool for traffic inspection, threat detection, and troubleshooting. We'll also cover essential network security best practices and test your knowledge with a quiz.



Use case: Monitor network traffic from selected VMs

Challenges

- Monitor and secure specific VMs within a network.
- Spot attacks that span multiple network packets and target specific VMs.

Solution

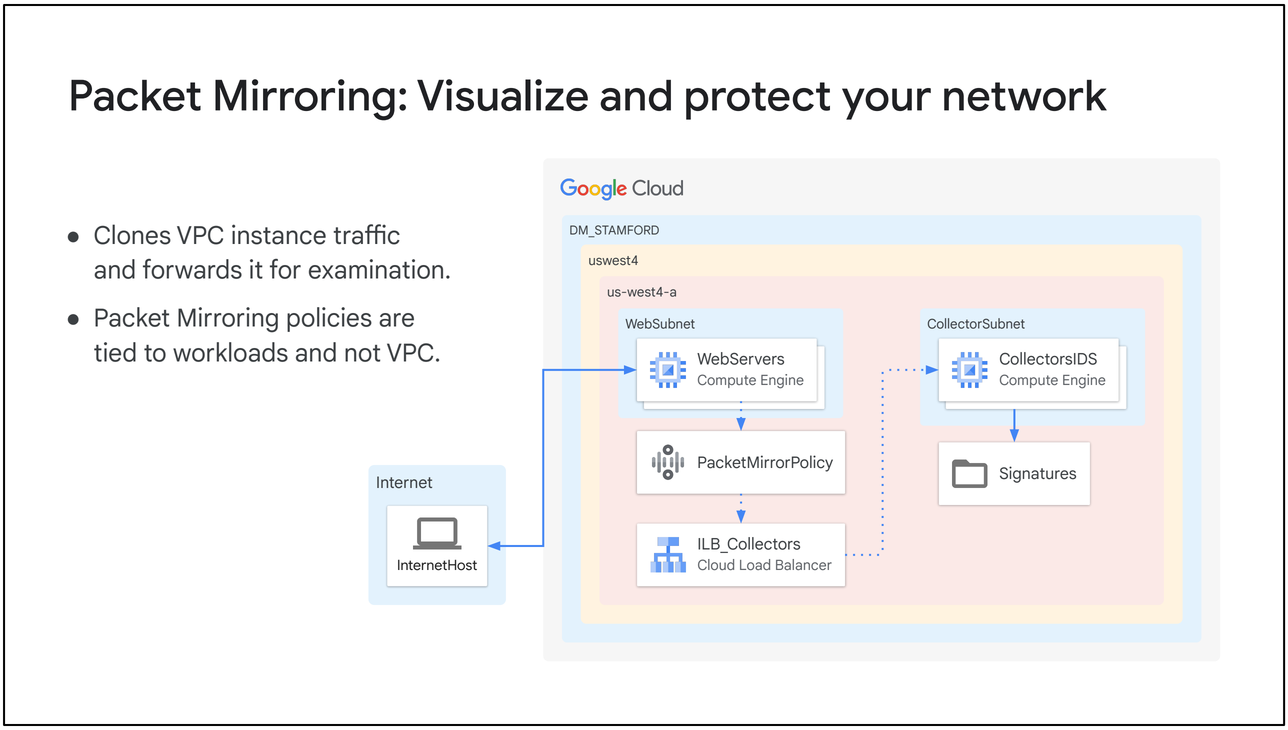
Packet Mirroring

- Analyze all packets within each flow.
- Identify anomalies.
- Detect complex attack patterns.

Virtual Machine
Virtual Machine
Virtual Machine
Virtual Machine

Izumi, a network engineer at Cymbal Corporation, needs to monitor the network traffic from selected virtual machines (VMs) to determine if malicious activity is occuring. Organizations face challenges in monitoring and securing specific virtual machines (VMs) within their network. Traditional security measures might not be sufficient to detect sophisticated attacks that span multiple network packets and target specific VMs. This can lead to vulnerabilities and security breaches, compromising sensitive data and critical systems.

Packet mirroring offers a solution by creating a copy of network traffic specifically from the selected VMs. This mirrored traffic is then directed to a security analysis platform where it undergoes deep packet inspection. By capturing and analyzing all packets within each flow, security teams can identify anomalies, detect complex attack patterns, and promptly respond to threats targeting those specific VMs. This proactive approach enhances security posture, safeguards sensitive data, and ensures the integrity of critical systems.



Packet Mirroring: Visualize and protect your network

- Clones VPC instance traffic and forwards it for examination.
- Packet Mirroring policies are tied to workloads and not VPC.

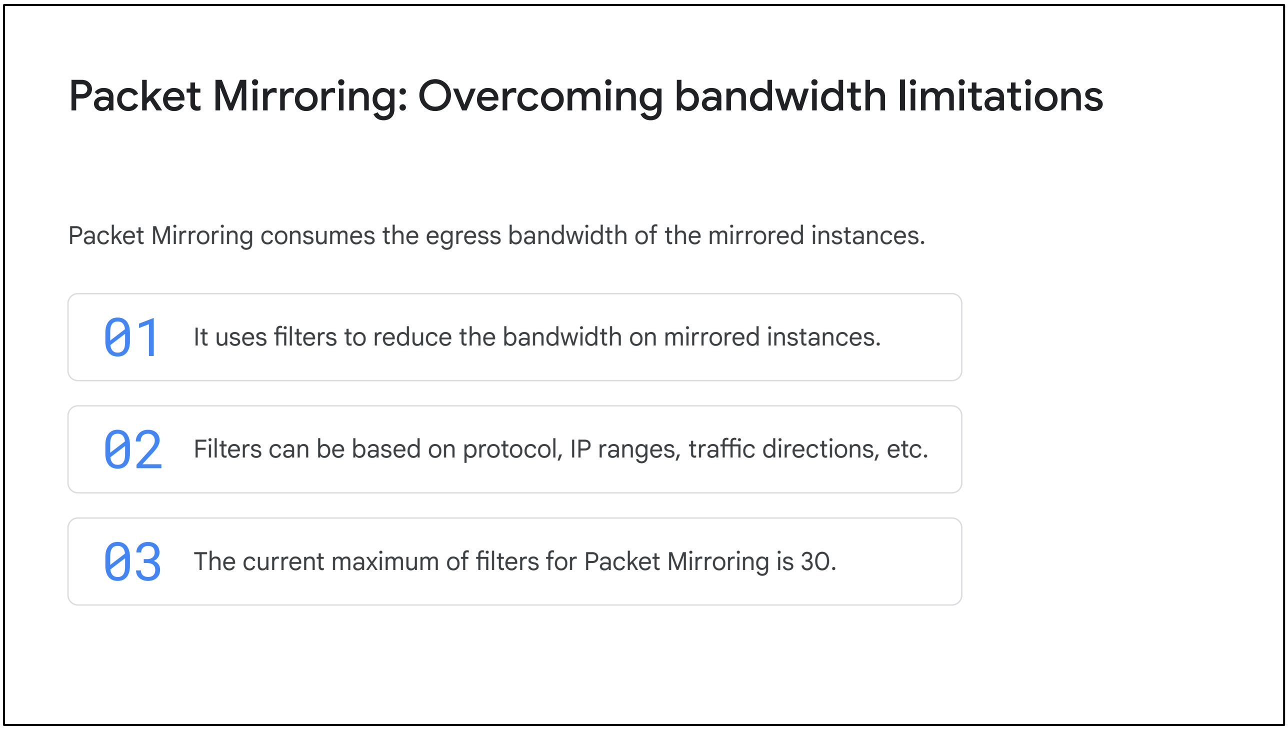
Packet Mirroring clones the traffic of specific instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all ingress and egress traffic and packet data, such as payloads and headers.

The mirroring happens on the virtual machine (VM) instances, not on the network. Therefore, Packet Mirroring consumes additional bandwidth on the hosts.

Packet Mirroring is useful when you need to monitor and analyze your security status. It exports all traffic, not only the traffic between sampling periods. For example, you can use security software that analyzes mirrored traffic to detect all threats or anomalies.

Also, you can inspect the full traffic flow to detect application performance issues and to provide network forensics for Payment Card Industry Data Security Standards (PCI DSS) compliance and other regulatory use cases. We will elaborate on this further in the next few slides.

Obviously, Packet Mirroring can generate significant data, so collector destination is generally an instance group behind a internal load balance or equivalent technology.



Packet Mirroring: Overcoming bandwidth limitations

Packet Mirroring consumes the egress bandwidth of the mirrored instances.

01 It uses filters to reduce the bandwidth on mirrored instances.

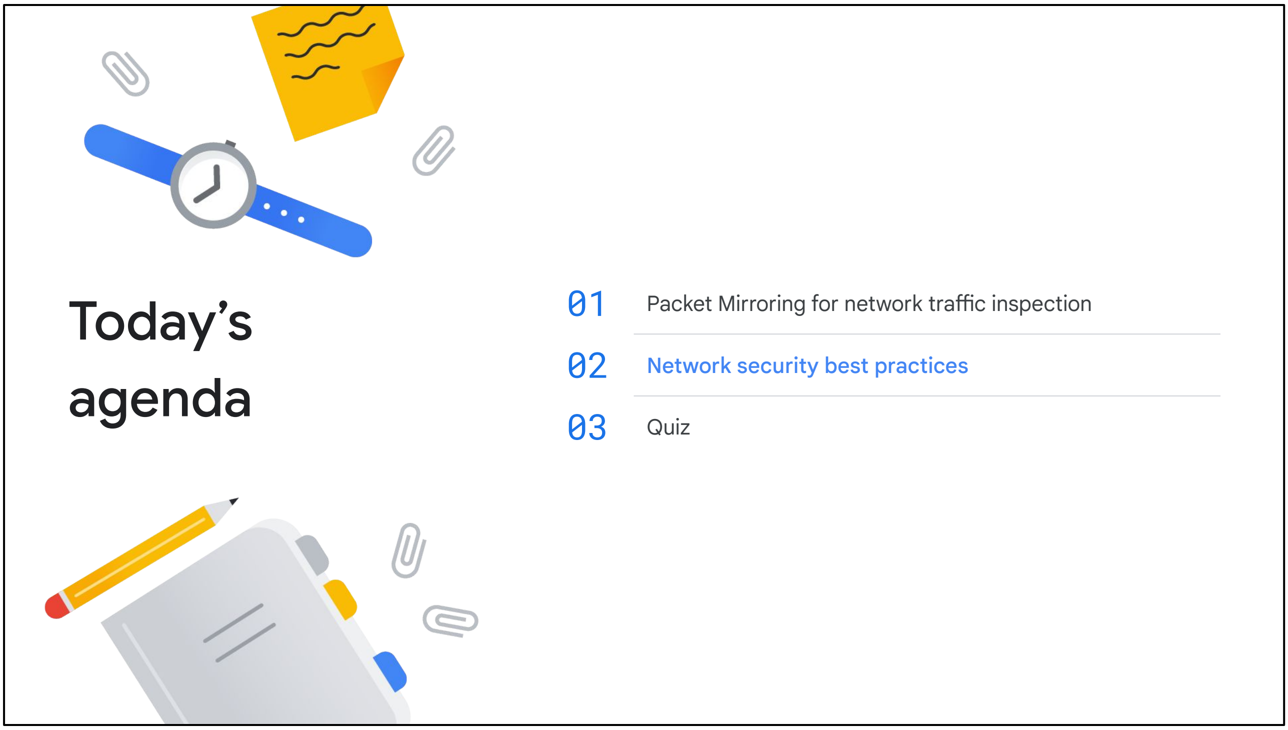
02 Filters can be based on protocol, IP ranges, traffic directions, etc.

03 The current maximum of filters for Packet Mirroring is 30.

One of the major limitations of Packet Mirroring is bandwidth consumption. Packet Mirroring consumes the egress bandwidth of the mirrored instances. However, there is a work-around. Use filters to reduce the traffic collected for mirrored instances. This filter can be used for IP address ranges, protocols, traffic directions, and a lot more.

The current maximum number of filters that can be used for Packet Mirroring is 30.

For more information, refer to the documentation.

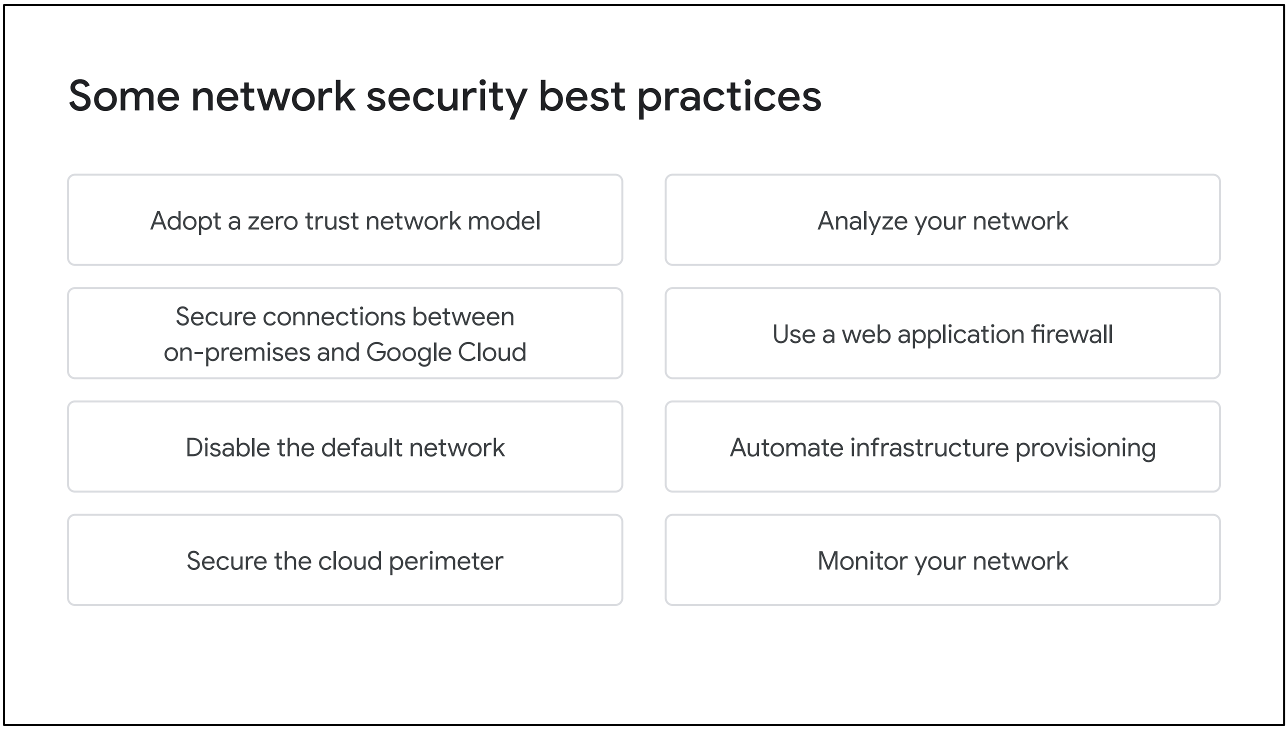


Today’s agenda

01 Packet Mirroring for network traffic inspection

02 Network security best practices

03 Quiz



Some network security best practices

Adopt a zero trust network model

Analyze your network

Secure connections between on-premises and Google Cloud

Use a web application firewall

Disable the default network

Automate infrastructure provisioning

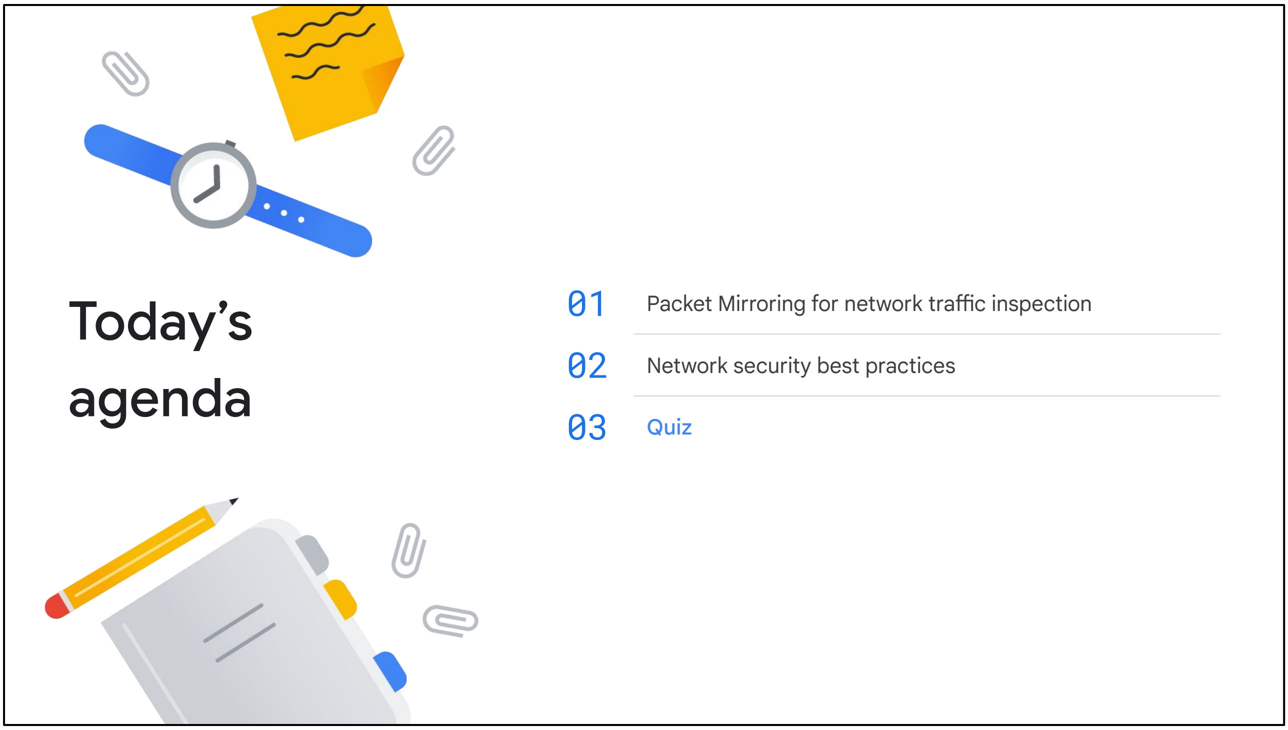
Secure the cloud perimeter

Monitor your network

Some of the network security best practices are listed on the slide. This list varies on a case-by-case basis based on the environment.

1. Adopt a zero trust network model. This approach ensures that no user or device is implicitly trusted, regardless of their location inside or outside the organization's network. By verifying both user identity and context during access requests, you shift security controls from the network perimeter to individual users and devices, providing a more robust and granular approach to security.
2. Secure connections between on-prem and Google Cloud: For organizations operating in hybrid or multi-cloud environments, prioritize secure connectivity between all environments to ensure data protection and minimize risks. Leverage Google Cloud's private access options like Cross-Cloud Interconnect, Dedicated/Partner Interconnect, and IPsec VPNs to establish secure, high-speed connections between your on-premises infrastructure and various cloud environments. Additionally, explore Private Service Connect for accessing Google APIs and published services with enhanced security, ensuring seamless communication while maintaining robust security measures.
3. Disable default networks: to enhance network security and avoid IP address conflicts, disable the creation of default networks in Google Cloud projects. Plan your network and IP address allocation strategically across connected deployments and projects to ensure efficient and secure communication. As a best practice, limit the number of VPC networks per project to one for more

1. effective access control.
2. Secure your cloud perimeter with Google Cloud's tools like firewalls and VPC Service Controls. Employ Shared VPC to centralize network management and isolate workloads into separate projects, enhancing security and control. Create firewall policies and rules at multiple levels (organization, folder, VPC network) to allow or deny traffic based on various criteria, including IP addresses, protocols, ports, service accounts, and secure tags.
3. Analyze your network. Google Cloud provides two tools, Cloud IDS and Packet Mirroring, to help you monitor and secure your network traffic in Compute Engine and Google Kubernetes Engine. Cloud IDS provides visibility into your VPC network traffic, while Packet Mirroring allows you to clone and forward specific VM traffic for further analysis and inspection with security tools.
4. Use a web application firewall: strengthen the security of your external web applications and services by implementing Google Cloud Armor, a web application firewall (WAF) that also provides protection against DDoS attacks. For optimal protection of critical workloads, leverage the advanced features offered by Google Cloud Armor's Managed Protection Plus tier.
5. Adopt automated infrastructure provisioning using tools like Terraform, Jenkins, or Cloud Build to create immutable environments for enhanced security and streamlined operations. Leverage Google Cloud's security blueprints as a foundation, or build upon them with your own automation to align with security best practices and guidelines.
6. Monitor your network. Implement VPC Flow Logs and Firewall Rules Logging to gain near real-time visibility into your Google Cloud network traffic and firewall activity. Utilize tools like Cloud Logging, Cloud Monitoring, Firewall Insights, and Network Intelligence Center to track, analyze, and optimize your network security and performance.



Today's agenda

01 Packet Mirroring for network traffic inspection

02 Network security best practices

03 Quiz

Quiz | Question 1

Question

What is the primary purpose of Packet Mirroring in network security?

A. To redirect traffic to a different network interface.

B. To create a duplicate copy of network traffic for analysis.

C. To filter out unwanted traffic from a network.

D. To encrypt network traffic for privacy.

Quiz | Question 2

Question

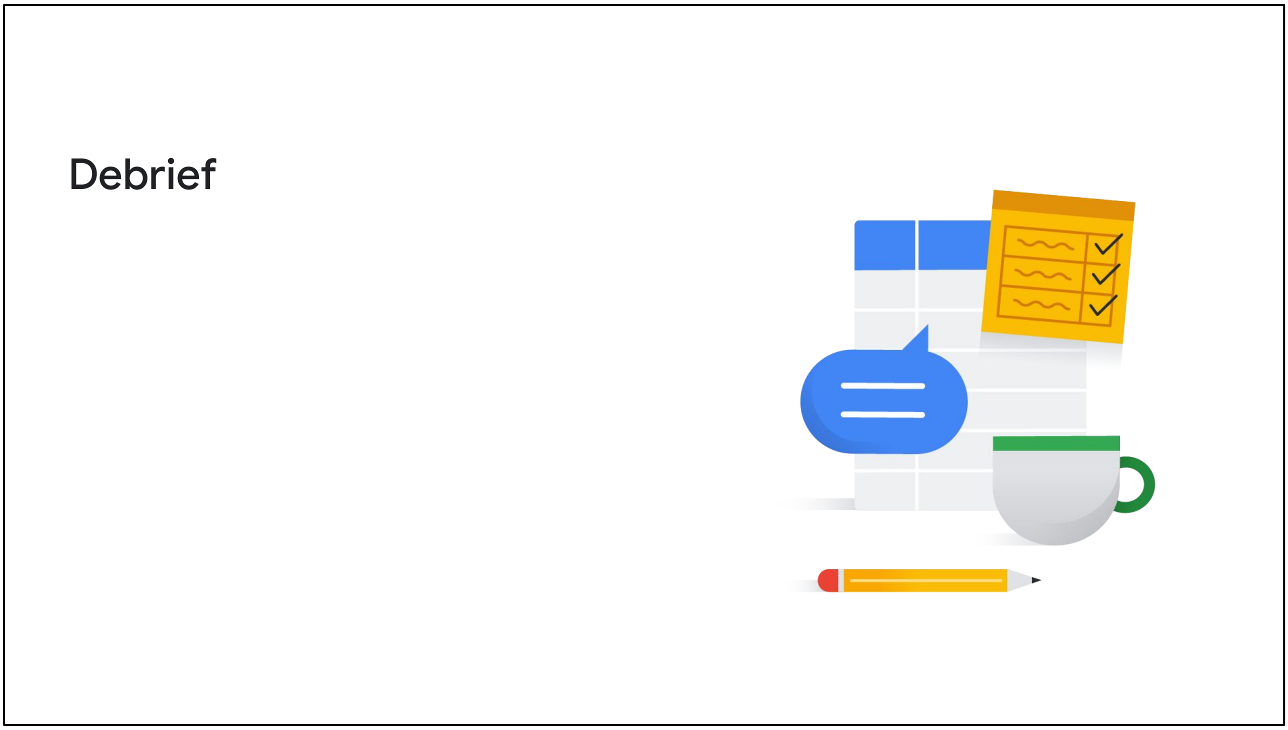
Which of the following is a key benefit of using Packet Mirroring for network security analysis?

A. It directly prevents cyberattacks.

B. It reduces network bandwidth usage.

C. It enables the capture and inspection of traffic without impacting network performance.

D. It automatically patches vulnerabilities in software.



Debrief

This module provided an overview of packet mirroring for enhanced network security. You learned how to leverage this tool for traffic inspection, threat detection, and troubleshooting. The module also covered essential network security best practices and tested your knowledge with a quiz.

Thank you.

THANK YOU

Google Cloud