



Monitoring the Google Cloud VPC



In this module, let's spend some time analyzing the Google Cloud Virtual Private Cloud.

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

Network Intelligence Center



Specifically, you learn to:

- Collect and analyze VPC Flow, Firewall Rule, and Cloud NAT logs so you can see what's happening to the traffic across your network.
- Enable Packet Mirroring so you can replicate packets at the virtual machine network interface, and forward it for further analysis.
- And explain the capabilities of the Network Intelligence Center.

Lecture Notes:

Most of these logs are huge and off by default. Should only be turned on for actively troubleshooting and switched off after troubleshooting

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

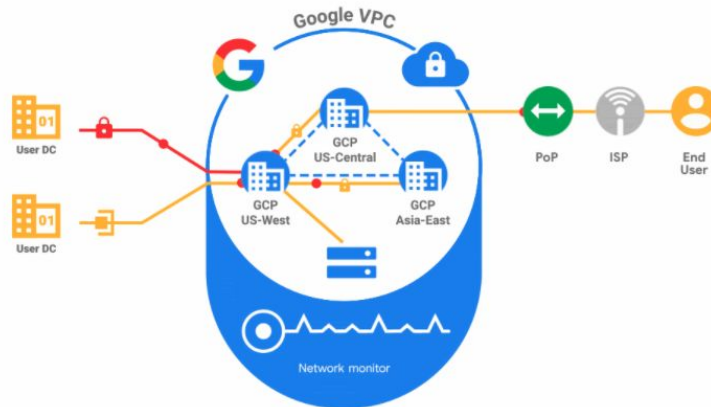
Packet Mirroring

Network Intelligence Center



Let's start with monitoring the network...

VPC Flow Logs record a sample of network flows



VPC Flow Logs record a sample (about 1 out of 10 packets) of network flows sent from and received by VM instances, including Kubernetes Engines nodes. These logs can be used for network monitoring, traffic analysis, forensics, real-time security analysis, and expense optimization.

VPC Flow Logs is part of Andromeda, the software that powers VPC networks. VPC Flow Logs introduces no delay or performance penalty when enabled.

Lecture Notes:

Flow logs are disabled by default.

If enabled, they can sample upto 10% of the packets flowing across the network

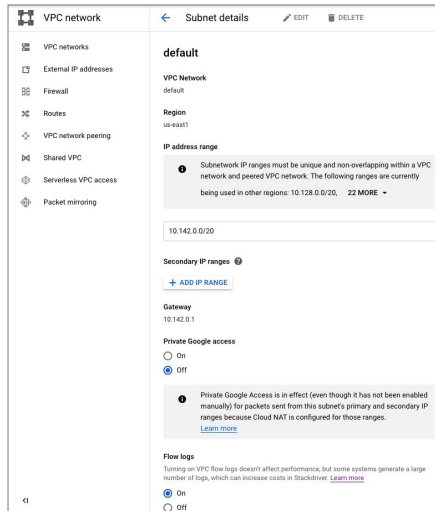
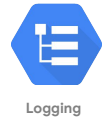
Why turn them on?

(a) Troubleshooting at network level

(b) Regulatory level

But since these are huge logs, be very careful as logging costs can skyrocket

Enable VPC Flow Logs per VPC subnet



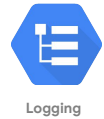
You can enable or disable VPC Flow Logs per VPC subnet. Once enabled for a subnet, VPC Flow Logs collect data from all VM instances in that subnet.

Lecture Notes:

Now there are some additional settings we can settable like:

Aggregation level (5 sec, 30 sec, 1 min.... 15 min)

Sampling percent (of the 10% max it can go)



Log entries contain many useful fields

Field	Type	Description
src_ip	string	Source IP address
src_port	int32	Source port
dest_ip	string	Destination IP address
dest_port	int32	Destination port
protocol	int32	IANA protocol number

Other fields:

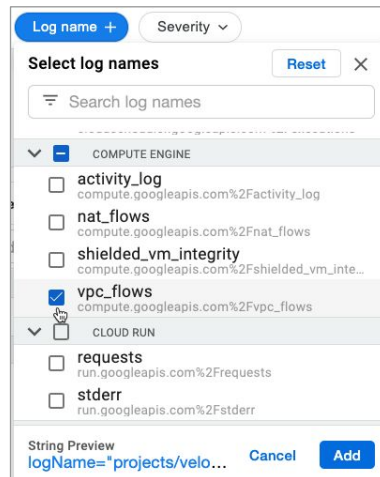
- Start/end time
- Bytes/packets sent
- Instance details
- VPC details
- Geographic details



Each log entry contains a record of different fields. For example, this table illustrates the IP connection information that is recorded. This consists of the source IP address and port, the destination IP address and port, and the protocol number. This set is commonly referred to as 5-tuple.

Other fields include the start and end time of the first and last observed packet, the bytes and packets sent, instance details including network tags, VPC details, and geographic details. For more information on all data recorded by VPC Flow Logs, please see the [documentation](#).

Use Logging to review your VPC Flow Logs



The Google Cloud Logs Viewer can be used to access the VPC Flow Logs. The entries will be `vpc_flows` under the Compute Engine section. Searching the log names for `vpc_flows` works well.

For a log query, use:

`logName="projects/[PROJECT_ID]/logs/compute.googleapis.com%2Fvpc_flows"`

Analyze logs in BigQuery and visualize in Data Studio



The screenshot shows the BigQuery interface with a query result table. The table has columns: Row, vpc_name, bytes, subnetwork_name, dest_ip, src_ip, dest_port, and protocol. The data is as follows:

Row	vpc_name	bytes	subnetwork_name	dest_ip	src_ip	dest_port	protocol
1	vpc-demo	23529368	vpc-demo-web	74.125.28.95	10.1.1.2	443.0	6.0
2	vpc-demo	15237089	vpc-demo-web	74.125.197.95	10.1.1.2	443.0	6.0
3	vpc-demo	4390076	vpc-demo-web	74.125.135.95	10.1.1.2	443.0	6.0
4	vpc-demo	1606002	vpc-demo-web	74.125.199.95	10.1.1.2	443.0	6.0
5	vpc-demo	1479280	vpc-demo-web	108.177.98.95	10.1.1.2	443.0	6.0
6	vpc-demo	828169	vpc-demo-web	173.194.202.95	10.1.1.2	443.0	6.0
7	null	150991	null	10.1.1.2	151.101.52.204	48668.0	6.0
8	null	18024	null	10.1.1.2	74.125.199.95	37910.0	6.0
9	null	17573	null	10.1.1.2	74.125.199.139	58010.0	6.0
10	null	16687	null	10.1.1.2	74.125.28.95	46118.0	6.0



Exporting VPC Flow logs to BigQuery allows you to analyze your network traffic with SQL, to understand traffic growth patterns and network usage better.

For example, in this screenshot, we queried logs to identify the top IP addresses that have exchanged traffic with the webserver.

Depending on where these IP addresses are and who they belong to, we could relocate part of the infrastructure to reduce latency, or we could denylist some of these IP addresses if we don't want them to access the web server.

For more sophisticated visualizations, connect your BigQuery tables to Data Studio and transform the raw data into the metrics and dimensions needed to create end-user-friendly reports and dashboards.

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

Network Intelligence Center



Another essential part of knowing what's happening at the VPC network level is knowing what the firewall rules are doing.

Firewall Rules Logging



Did my firewall rules cause that application outage?



How many connections match the rule I just created?



Are my firewall rules stopping (or allowing) the correct traffic?



VPC firewall rules let you allow or deny connections to or from your virtual machine (VM) instances based on a configuration that you specify.

Enabled VPC firewall rules are always enforced, protecting your instances regardless of their configuration and operating system, even if they have not started up.

Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules.

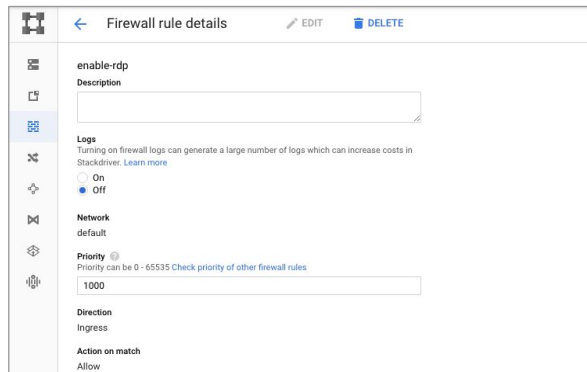
It can help answer questions like:

- Did my firewall rules cause that application outage?
- How many connections match the rule I just created?
- Are my firewall rules stopping (or allowing) the correct traffic?

See the Firewall Rule Logging [documentation](#) for details.

Enabling Firewall Rules Logging in the console

- Firewall Rules Logging is **disabled** by default
- You enable it on a per-rule basis



The screenshot shows the 'Firewall rule details' page in the Google Cloud console. The rule is named 'enable-rdp'. The 'Logs' section is expanded, showing a warning that turning on logs can increase costs and a radio button interface where 'Off' is selected. Other visible settings include 'Network' set to 'default', 'Priority' set to '1000', 'Direction' set to 'Ingress', and 'Action on match' set to 'Allow'.

Section	Value
Name	enable-rdp
Description	
Logs	Off
Network	default
Priority	1000
Direction	Ingress
Action on match	Allow

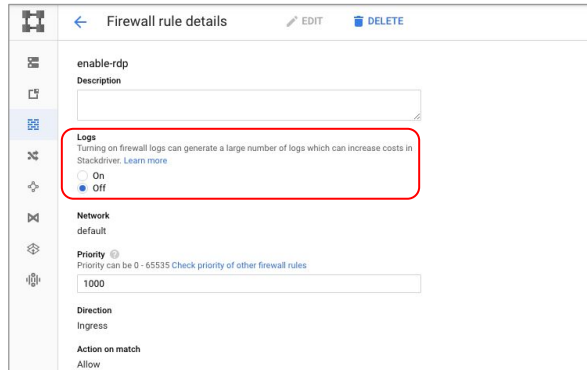


By default, Firewall Rules Logging is disabled.

You can enable it on a per-rule basis.

Enabling Firewall Rules Logging in the console

- Firewall Rules Logging is **disabled** by default
- You enable it on a per-rule basis



In the slide screenshot, the user is editing the firewall rule named *enable-rdp*. Selecting the radio button will enable firewall rules.

Caution: Firewall Rules Logging can generate a lot of data which may have a cost impact.

Enabling Firewall Rules Logging in the CLI

- Firewall Rules Logging can also be enabled or disabled using the following **gcloud** commands
- Substitute [NAME] for the name of your firewall rule

Enable:

```
gcloud compute firewall-rules update [NAME] --enable-logging
```

Disable:

```
gcloud compute firewall-rules update [NAME] --no-enable-logging
```



Firewall Rules Logging can also be enabled on existing firewall rules using the CLI.

See these two examples on this slide. In both, [NAME] would be the name of your firewall rule.

Viewing the Firewall Rules logs

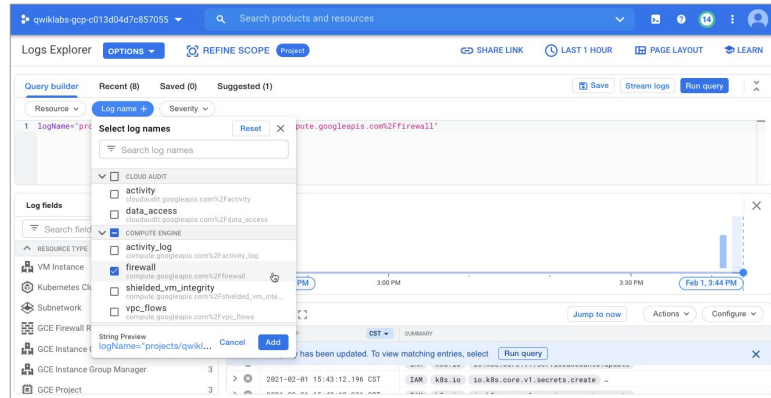
- In Logging, you can view the logs in real time
- Or, export the firewall logs to a BigQuery sink



Logging



BigQuery



Like all Google Cloud Logs, use the Logs Viewer to view logs in real time, or to configure exports.

BigQuery is frequently used to simplify firewall rules log analysis.

Viewing the Firewall Rules logs

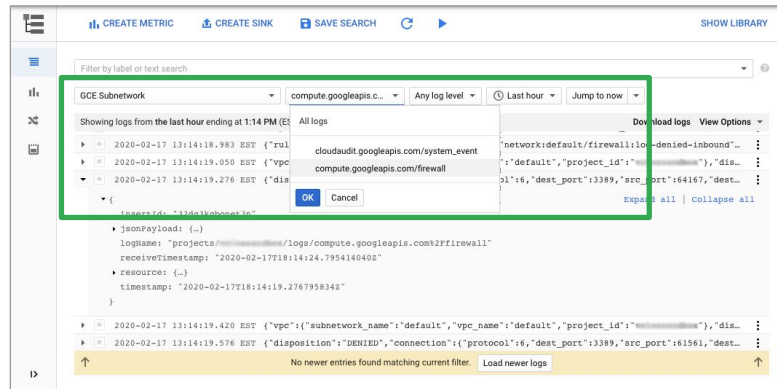
- In Logging, you can view the logs in real time
- Or, export the firewall logs to a BigQuery sink



Logging



BigQuery

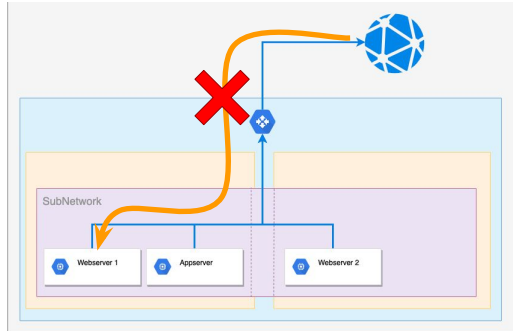


To filter for firewall logs, set the resource to **GCE Subnet**, and the log file to **firewall**.

Lecture Notes: Old view

Firewall Rules provide microsegmentation

Segmentation/Gateway-centric



A lot of users are familiar with classic segmentation or gateway-centric firewalls.

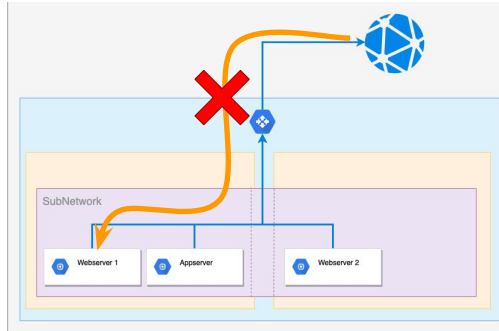
In this example, you can see a private network, possibly at your office or home.

At the network boundary, where the private network meets the outside internet, sits a firewall.

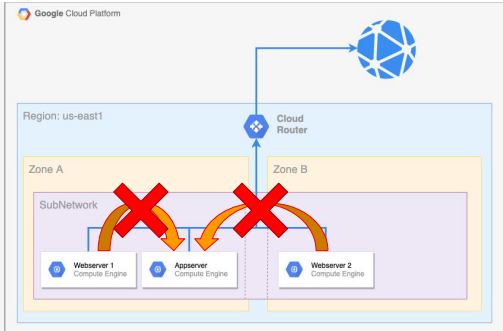
A segmentation firewall is designed to segment and secure a protected network from an outside insecure network.

Firewall Rules provide microsegmentation

Segmentation/Gateway-centric



Microsegmentation/VM-centric



Google Cloud VPC Firewalls are micro-segmentation firewalls.

These function more like a bunch of micro-firewalls, each sitting on the NIC of every VM connected to the VPC.

The micro-firewalls can then grant or deny any configured incoming or outgoing traffic.

Now, imagine we have an issue.

We have two different web servers, and after some configuration changes by a particular DevOps team, the web servers can no longer access the application server they both share.

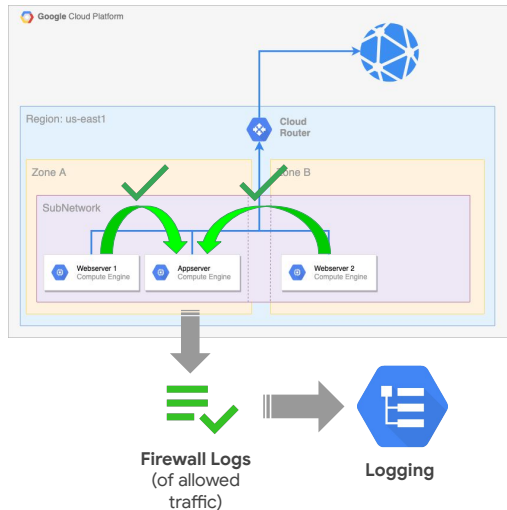
How can we tell if this is a firewall-related issue? Let's see.

Lecture notes:

Micro-segmentation can only be setup on SDN

Troubleshooting: using rules to catch incorrect traffic

- Logging all denied connections will create too many log entries
- Temporarily create a low-priority rule to allow traffic to the server
 - Enable logging
- If traffic now gets through, examine the logs as to why



If the connectivity issue is related to a firewall, then there are two major possibilities.

1) There's a firewall rule that's actively blocking the incoming connections from the web servers.

Or

2) Since network traffic is blocked by default in most networks, there could be a firewall rule that isn't allowing the traffic from the web servers as it should.

Two sides of the same coin.

Logging all denied connections could generate a lot of data that would take time and effort to go through. So, instead of starting with option one, let's start with option two.

Create a temporary low-priority rule specifically designed to allow the web server traffic through to the app server. Enable logging on it so you can examine the entries.

Suddenly the traffic is getting through, so you know it's firewall related. Now examine the log entries. Also, find the existing rule that's supposed to be allowing the traffic and see what you can find out.

Hey, look at that! The rule that's supposed to be allowing the traffic is based on a network tag named *webserver*, and the web server machines are actually using the

network tag *web-server*. There it is, that's your problem.

Agenda

VPC Flow Logs

Firewall Rules Logging

[Load Balancer Logs](#)

Cloud NAT Logs

Packet Mirroring

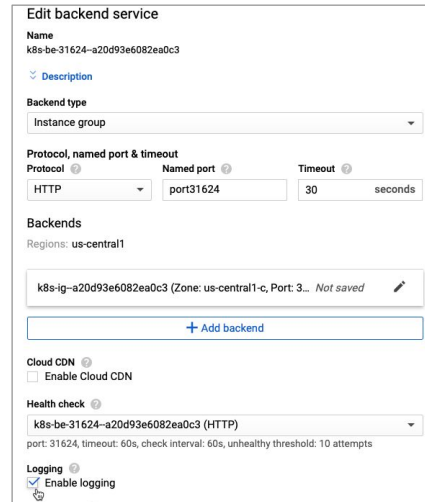
Network Intelligence Center



Several of Google Cloud's load balancers support monitoring and/or logging.

The internal and external HTTP(s) load balancers support logging

- Enabled on a per backend service basis
 - URL map may reference more than one
 - Will have to enable for each
- Enabled by default



Edit backend service

Name
k8s-be-31624-a20d93e6082ea0c3

Description

Backend type
Instance group

Protocol, named port & timeout

Protocol	Named port	Timeout
HTTP	port31624	30 seconds

Backends

Regions: us-central1

k8s-ig-a20d93e6082ea0c3 (Zone: us-central1-c, Port: 3... Not saved)

+ Add backend

Cloud CDN

☐ Enable Cloud CDN

Health check

k8s-be-31624-a20d93e6082ea0c3 (HTTP)

port: 31624, timeout: 60s, check interval: 60s, unhealthy threshold: 10 attempts

Logging

☒ Enable logging



You can enable logging on a per backend service basis. A single internal HTTP(S) load balancer's URL map can reference more than one backend service, so you might need to enable logging for more than one backend service, depending on your configuration. It will be enabled by default for all new load balancers backends, but backends created before the GA release of load balancer logging may require manual configuration.

Lecture Notes:

This is enabled by default. Since big logs, think about partial exclusion at log router level

Choosing a Load Balancer: <https://cloud.google.com/load-balancing/docs/choosing-load-balancer>

Load Balancer graphic: <https://thecloudgirl.dev/images/CLB.jpg>

Load Balancer logging: <https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring>

Several ways to classify load balancers:

* Proxy (Layer 7) Vs Passthrough (Layer 4)

Layer 4 load balancer does low level package manipulation. does not throw any logs. (passthrough)

Layer 7 load balancers is at the application level and hence is recognized as a stop of its own.

External service in Kubernetes is a Layer 4 LB

Ingress in Kubernetes is a Layer 7 LB

Google microservice demo: <https://github.com/GoogleCloudPlatform/microservices-demo>
is a big fancy demo that builds a storefront on Kubernetes

Log entries contain the following types of information:

- General information including:
 - Severity, project ID, project number, and timestamp.
- HttpRequest log fields, including:
 - Method, URL, status, remote ip, and user agent.
- A `statusDetails` containing a string explaining why the load balancer returned the HTTP status that it did, cache and failure information.
- Redirects (HTTP response status code 302 found) issued from the load balancer are not logged. Redirects issued from the backend instances are logged.



HTTP(S) load balancing log entries contain information useful for monitoring and debugging your HTTP(S) traffic. Make sure to [check the documentation for details](#).

Log entries contain the following types of information:

- General information shown in most logs, such as severity, project ID, project number, timestamp, and so on.
- `HttpRequest` log fields. However, `HttpRequest.protocol` is not populated for HTTP(S) load balancing Cloud Logging logs.
- A `statusDetails` field inside the `structPayload`. This field holds a string that explains why the load balancer returned the HTTP status that it did.
- Redirects (HTTP response status code 302 Found) issued from the load balancer are *not* logged. Redirects issued from the backend instances *are* logged.

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

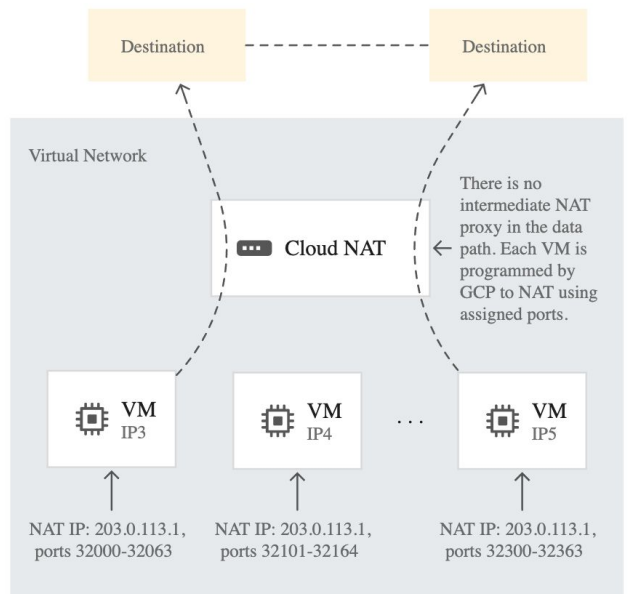
Network Intelligence Center



Another piece of the network telemetry features in Google Cloud is Cloud NAT logs.

Cloud NAT overview

- Allows GCE VMs with no external IP to send packets to the internet
- Fully managed, software defined, grounded in Andromeda
- Benefits include:
 - Security
 - Availability
 - Scalability
 - Performance



Cloud NAT ([network address translation](#)) allows Google Cloud virtual machine (VM) instances without external IP addresses and private Google Kubernetes Engine (GKE) clusters to send outbound packets to the internet and receive any corresponding established inbound response packets.

Cloud NAT is a distributed, software-defined, fully managed service, grounded in the [Andromeda software](#) that powers your VPC network. It provides source network address translation (SNAT) for VMs without external IP addresses, as well as destination network address translation (DNAT) for established inbound response packets.

Cloud NAT benefits include:

- **Security:** You can reduce the need for individual VMs to have external IP addresses, lessening the surface area for attack. You can also confidently share a set of common external source IP addresses with a destination party.
- **Availability:** Cloud NAT is a distributed, software-defined, managed Google Cloud service. It doesn't depend on any VMs in your project or a single physical gateway device.
- **Scalability:** Cloud NAT can be configured to automatically scale the number of NAT IP addresses it uses, and it supports VMs that belong to managed instance groups, including those with [autoscaling](#) enabled.
- **Performance:** Cloud NAT does not reduce the network bandwidth per VM. Cloud NAT works directly with Google's Andromeda software-defined

- networking.

Cloud NAT logging

- Allows you to log NAT **connections** and/or **errors**
 - TCP and UDP traffic only
 - 50-100 entries per second, per vCPU
- Enable logging by editing the Cloud NAT settings
- View by filtering the Logs Viewer:
 - Resource: Cloud NAT Gateway
 - (optional) Restrict to region or NAT Gateway

Logging, minimum ports, timeout

Stackdriver logging ?

Export Cloud NAT logs to Stackdriver

- ☐ No logging
- ☒ Translation and errors
- ☐ Translation only
- ☐ Errors only



Cloud NAT logging allows you to log NAT TCP and UDP connections and errors. When Cloud NAT logging is enabled, a log entry can be generated when a network connection using NAT is created, and/or when an egress packet is dropped because no port was available for NAT.

You can opt to log both kinds of events, or just one or the other. Logs contain TCP and UDP traffic only, and the log rate threshold will max out at 50-100 log events per vCPU before log filtering.

Cloud NAT logging may be enabled when a new Cloud NAT gateway is first created, or by editing an existing gateway's settings.

To view the collected logs in the Logs Viewer, filter to the Cloud NAT Gateway resource and optionally, restrict to a particular region or Gateway.

The full query will look something like:

```
resource.type="nat_gateway"  
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fnat_flows"
```

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

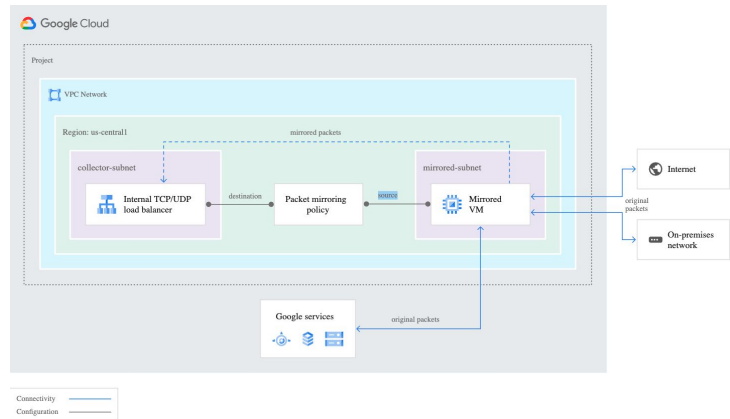
Network Intelligence Center



Another way to monitor the network traffic flowing in and out of your Compute Engine virtual machines is to use packet mirroring.

Packet Mirroring: visualize and protect your network

- Clones VPC instance traffic and forwards for examination
- Happens at NIC not as part of VPC
- Can monitor and analyze security status
- Provides access to full traffic flow for regulatory or performance analysis



Packet Mirroring clones the traffic of specified 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. Consequently, 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.

Additionally, you can inspect the full traffic flow to detect application performance issues and to provide network forensics for PCI compliance and other regulatory use cases.

Obviously, this can generate a lot of data, so the recommended target is a load-balanced Compute Engine Managed Instance Group or equivalent technology.

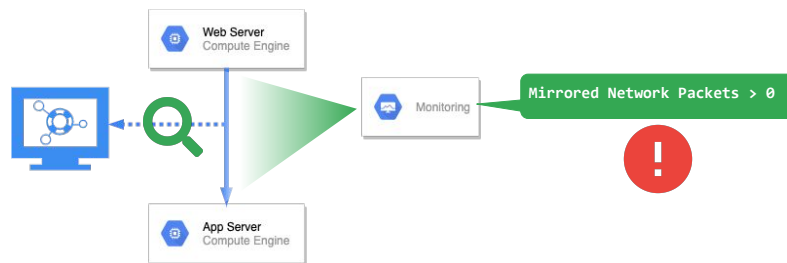
Lecture Notes:

Used for SIEM analysis (for regulatory/cyber)

WARNING: Lots of data. Adversely affects network throughput for VMs. (since there is a limit on network throughput per CPU (upto a max), but mirroring packets just reduce it half)

Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended



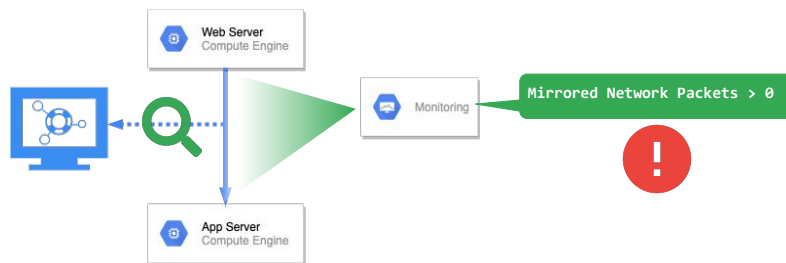
Packet Mirroring exports monitoring data about mirrored traffic to Cloud Monitoring.

You can use monitoring metrics to check whether traffic from a VM instance is being mirrored as intended.

For example, you can view the mirrored packet or byte count for a particular instance.

Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended
 - Mirrored Packets count
 - Mirrored Bytes Count
 - Dropped Packets Count

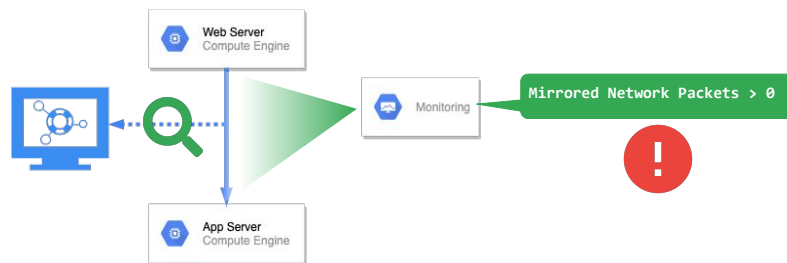


You can view the monitoring metrics of mirrored VM instances or instances that are part of the collector destination (internal load balancer).

For mirrored VM instances, Packet Mirroring provides metrics specific to mirrored packets, such as `/mirroring/mirrored_packets_count`, `/mirroring/mirrored_bytes_count`, and `/mirroring/dropped_packets_count`.

Monitoring Packet Mirroring

- Metrics can verify that instances are being monitored as intended
 - Mirrored Packets count
 - Mirrored Bytes Count
 - Dropped Packets Count
- Can also spot where packet mirroring shouldn't be happening



Monitoring can also spot where packet mirroring is being used unnecessarily or unexpectedly.

Keep in mind that, as noted, mirroring generates a lot of data that requires storage and processing, but also note that it slows the network throughput of the virtual machines being monitored and may accidentally expose sensitive data.

Agenda

VPC Flow Logs

Firewall Rules Logging

Load Balancer Logs

Cloud NAT Logs

Packet Mirroring

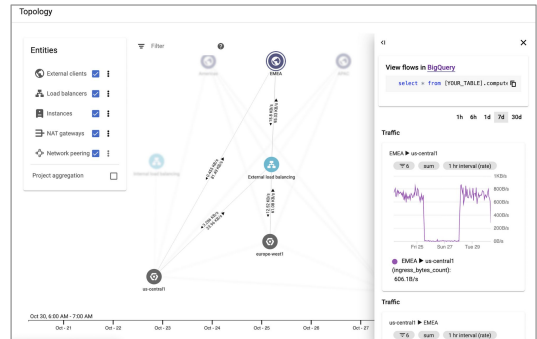
[Network Intelligence Center](#)



This section is a bit of a detour, but let's at least mention the Network Intelligence Center and how it helps with network analysis.

Network Intelligence Center

Centralized Network monitoring and visibility



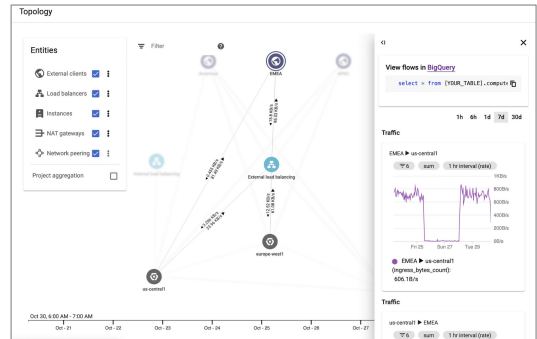
Google's Network Intelligence Center is all about giving you centralized monitoring and visibility into your network, reducing troubleshooting time and effort, increasing network security, all while improving the overall user experience.

Currently, it offers four modules: network topology, connectivity testing, a performance dashboard, and firewall insights.

Network Intelligence Center

Centralized Network monitoring and visibility

- Topology: view VPC topology and associated metrics



Network Topology is a visualization tool for viewing the topology of your VPC networks and the metrics that are associated with their Google Cloud resources.

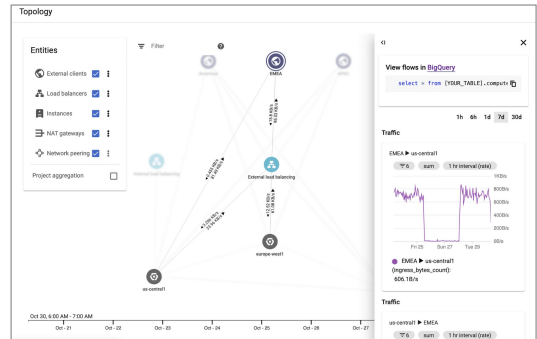
Lecture Notes:

Anthos observability is like Istio/Kiali dashboard

Network Intelligence Center

Centralized Network monitoring and visibility

- Topology: view VPC topology and associated metrics
- Connectivity Tests: Evaluate connectivity to and from VPC resources

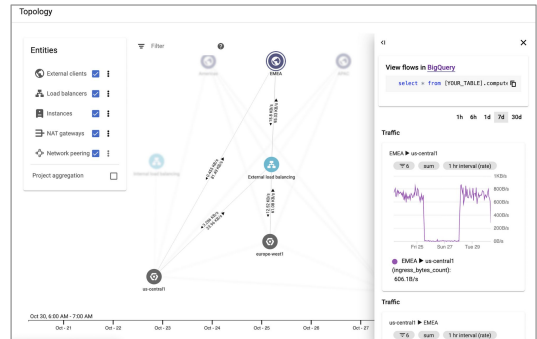


Connectivity Tests enables you to evaluate connectivity to and from Google Cloud resources in your Virtual Private Cloud (VPC) network, by performing a static analysis of your resource configurations.

Network Intelligence Center

Centralized Network monitoring and visibility

- Topology: view VPC topology and associated metrics
- Connectivity Tests: Evaluate connectivity to and from VPC resources
- Performance Dashboard: VPC packet loss and latency metrics



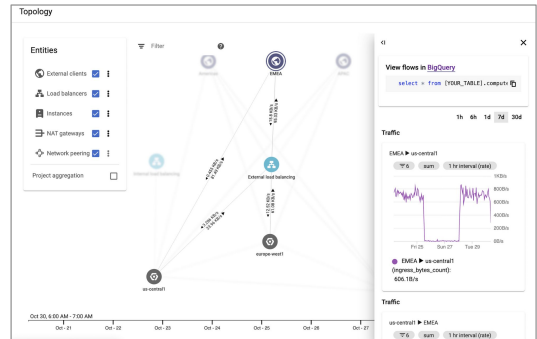
Performance Dashboard gives you visibility into the performance of your VPC network.

It provides packet loss and latency (Round Trip Time) metrics between the zones where you have VMs.

Network Intelligence Center

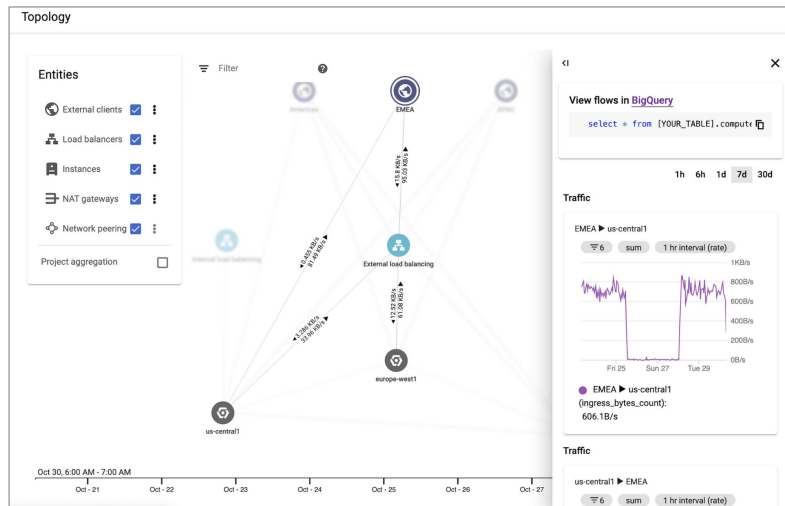
Centralized Network monitoring and visibility

- Topology: view VPC topology and associated metrics
- Connectivity Tests: Evaluate connectivity to and from VPC resources
- Performance Dashboard: VPC packet loss and latency metrics
- Firewall Insights: Visibility into firewall usage and configuration issues



Firewall Insights provides visibility into firewall usage and detects firewall configuration issues.

Topology



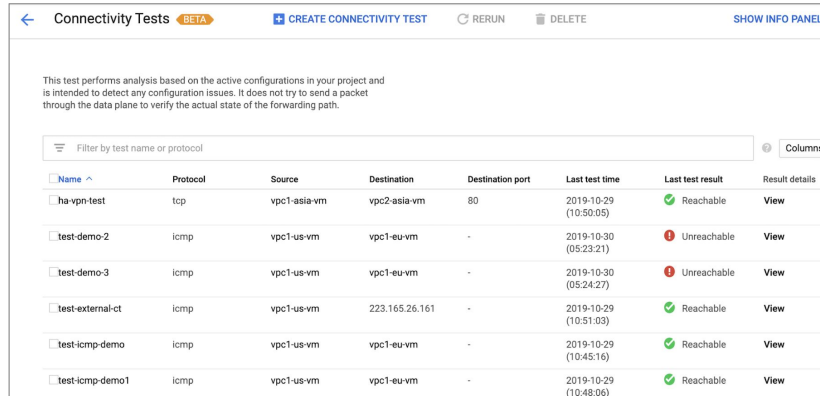
Network Topology visualizes your Google Cloud network as a graph.

You can use the graph to explore your existing configurations and quickly troubleshoot networking issues.

You can select network entities, filter, see lines of communication with bandwidth information, expand and collapse hierarchies, select time boundaries, and see details for the item selected.

Connectivity tests

- Quickly diagnose connectivity issues and prevent outages
- Verify configuration change impact to help prevent outages



Connectivity Tests BETA [+ CREATE CONNECTIVITY TEST](#) [RERUN](#) [DELETE](#) [SHOW INFO PANEL](#)

This test performs analysis based on the active configurations in your project and is intended to detect any configuration issues. It does not try to send a packet through the data plane to verify the actual state of the forwarding path.

Filter by test name or protocol Columns

Name ^	Protocol	Source	Destination	Destination port	Last test time	Last test result	Result details
<input type="checkbox"/> ha-vpn-test	tcp	vpc1-asia-vm	vpc2-asia-vm	80	2019-10-29 (10:58:05)	✓ Reachable	View
<input type="checkbox"/> test-demo-2	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-30 (05:23:21)	✗ Unreachable	View
<input type="checkbox"/> test-demo-3	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-30 (05:24:27)	✗ Unreachable	View
<input type="checkbox"/> test-external-ct	icmp	vpc1-us-vm	223.165.26.161	-	2019-10-29 (10:51:03)	✓ Reachable	View
<input type="checkbox"/> test-icmp-demo	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-29 (10:45:16)	✓ Reachable	View
<input type="checkbox"/> test-icmp-demo1	icmp	vpc1-us-vm	vpc1-eu-vm	-	2019-10-29 (10:48:06)	✓ Reachable	View



Network Intelligence Center [Connectivity Tests](#) help to quickly diagnose connectivity issues and prevent outages.

These tests enable you to self-diagnose connectivity issues within Google Cloud or Google Cloud to an external IP address (which could be on-premises or in another cloud) helping to isolate whether the issue is in Google Cloud or not.

Run tests to help verify the impact of configuration changes and ensure that network intent captured by these tests is not violated, proactively preventing network outages.

These tests also help assure network security and compliance.

Lecture Notes:

Network Management API needs to be enabled.

Can do scheduled connectivity test. Specify protocol, IP, port, etc. Can script them as well.

Costs: First 20 per month, free, then \$0.15 per test

Performance dashboard

- Packet loss metrics aggregated across zones



Performance Dashboard gives you visibility into the performance of your VPC.

The **Packet Loss** tab shows the results of active probing between your VMs in a given VPC.

To get this data, it runs workers on the physical hosts that house your VMs.

These workers insert and receive probe packets that run on the same network as your traffic, revealing issues on that network.

Because the workers run on the physical host and not on your VM, these workers do not consume VM resources and the traffic is not visible on your VMs.

Packet loss is aggregated for all zone pairs.

Lecture Notes:

Shows packet loss and latencies between regions

Performance dashboard

- Packet loss metrics aggregated across zones
- Median Latency summaries aggregated across zones



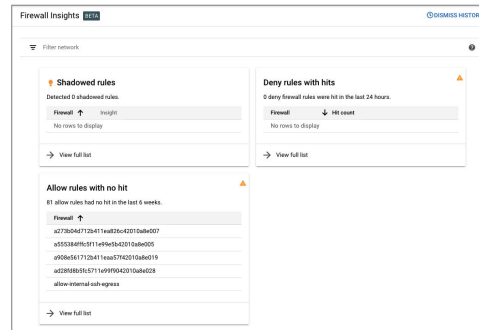
The **Latency** tab aggregates latency information based on a sample of your actual TCP VM traffic, using a method similar to the one used for [VPC Flow Logs](#).

The latency is calculated as the time that elapses between sending a TCP sequence number (SEQ) and receiving a corresponding ACK that contains the network RTT and TCP stack related delay.

The latency metric is only available if TCP traffic is around 1000 packets per minute or higher.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
 - Based on data collected by Firewall Rules Logging



The screenshot displays the 'Firewall Insights' dashboard. At the top, there's a 'Filter network' dropdown and a 'HISTORY' link. The dashboard is divided into three main sections:

- Shadowed rules:** A section with a warning icon indicating 'Detected 0 shadowed rules.' It contains a table with columns 'Firewall' and 'Insight', showing 'No rows to display'. A 'View full list' link is at the bottom.
- Deny rules with hits:** A section with a warning icon indicating '0 deny firewall rules were hit in the last 24 hours.' It contains a table with columns 'Firewall' and 'Hit count', showing 'No rows to display'. A 'View full list' link is at the bottom.
- Allow rules with no hit:** A section with a warning icon indicating '81 allow rules had no hit in the last 6 weeks.' It contains a table with columns 'Firewall' and 'Insight', listing several rule IDs and their insights. A 'View full list' link is at the bottom.



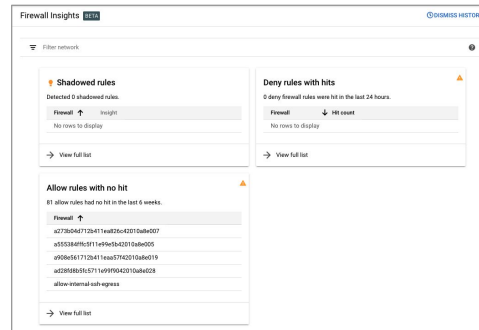
Firewall Insights enables you to better understand and safely optimize your firewall configurations by analyzing Firewall Rules logs and providing reports on firewall usage, and the impact of various firewall rules on your VPC.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
 - Based on data collected by Firewall Rules Logging

Reports included for every firewall with logging enabled

- Allow/deny counts



The screenshot shows the 'Firewall Insights' dashboard. It has a header with 'Firewall Insights' and a 'HISTORY' link. Below the header is a 'Filter network' dropdown. The main content area is divided into three sections:

- Shadowed rules:** A section with a warning icon. It says 'Detected 0 shadowed rules.' Below this is a table with columns 'Firewall' and 'Insight'. It shows 'No rows to display' and a 'View full list' link.
- Deny rules with hits:** A section with a warning icon. It says '0 deny firewall rules were hit in the last 24 hours.' Below this is a table with columns 'Firewall' and 'Hit count'. It shows 'No rows to display' and a 'View full list' link.
- Allow rules with no hit:** A section with a warning icon. It says '81 allow rules had no hit in the last 6 weeks.' Below this is a table with columns 'Firewall'. It lists several firewall IDs: 'a27804067120411eaa576c42010ba0027', 'a5553844f6c5f11e49f95b42010ba0025', 'a906a5617120411eaa576c42010ba0019', and 'a62898365c5711e49f95b42010ba0028'. It also includes the rule name 'allow-internal-sub-egress'. There is a 'View full list' link at the bottom.



For each firewall rule with logging enabled, you can see:

- How many times the firewall rule has blocked or allowed connections.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
 - Based on data collected by Firewall Rules Logging

Reports included for every firewall with logging enabled

- Allow/deny counts
- Last used

The screenshot shows the 'Firewall Insights' dashboard with a 'Filter network' dropdown and a 'VIEW HISTORY' link. It contains three main sections:

- Shadowed rules:** A table with columns 'Firewall' and 'Insight'. It shows 'Detected 0 shadowed rules.' and 'No rows to display'.
- Deny rules with hits:** A table with columns 'Firewall' and 'Hit count'. It shows '0 deny firewall rules were hit in the last 24 hours.' and 'No rows to display'.
- Allow rules with no hit:** A table with columns 'Firewall'. It shows '81 allow rules had no hit in the last 6 weeks.' and lists several firewall IDs.



- The last time a particular firewall rule was applied to allow or deny traffic.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
 - Based on data collected by Firewall Rules Logging

Reports included for every firewall with logging enabled

- Allow/deny counts
- Last used
- Unused rules

The screenshot shows the 'Firewall Insights' dashboard. It has a 'Filter network' dropdown at the top left and a 'CHANGES HISTORY' link at the top right. The dashboard is divided into three main sections:

- Shadowed rules:** A section with a warning icon indicating 'Detected 0 shadowed rules.' It contains a table with columns 'Firewall' and 'Insight', showing 'No rows to display' and a 'View full list' link.
- Deny rules with hits:** A section with a warning icon indicating '0 deny firewall rules were hit in the last 24 hours.' It contains a table with columns 'Firewall' and 'Hit count', showing 'No rows to display' and a 'View full list' link.
- Allow rules with no hit:** A section with a warning icon indicating '81 allow rules had no hit in the last 6 weeks.' It contains a table with a 'Firewall' column listing several rule IDs (e.g., a278054067120411, a5553844f6c5f11e49f9e5b4c32010ba6d027) and a 'View full list' link.



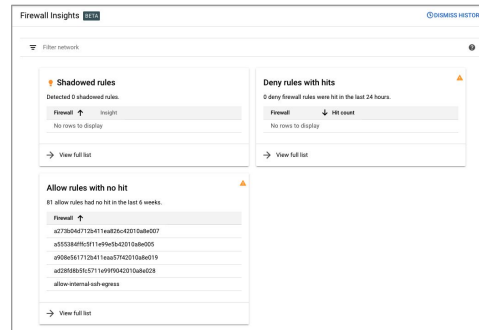
- A list of firewall rules that haven't been used in the last six weeks.

Firewall Insights

- Metrics to help understand and optimize firewall configurations
 - Based on data collected by Firewall Rules Logging

Reports included for every firewall with logging enabled

- Allow/deny counts
- Last used
- Unused rules
- Shadowed rules



- And Shadowed firewall rules. (A *shadowed rule* is a firewall rule that has all of its relevant attributes, such as IP address range and ports, overlapped by attributes from one or more other firewall rules with higher or equal priority. A firewall doesn't evaluate a shadowed rule because of the overlap and because the shadowed rule has a lower priority than its shadowing rules.)

Lecture Notes:

Can help to optimize firewall rules. For e.g. shows firewall rules which are never used or have not been used in some time (max 6 weeks)

Have to keep the firewall logs on.

Lab Intro

Analyzing Network Traffic with VPC Flow Logs (Optional)



In this lab, you configure a network to record traffic to and from an Apache web server using VPC Flow Logs. You then export the logs to BigQuery to analyze them.

Learned how to...

- Collect and analyze VPC Flow, Firewall Rules, and Cloud NAT logs
- Enable Packet Mirroring
- Explain the capabilities of Network Intelligence Center



Very good. After this module, you now know how to:

- Collect and analyze VPC Flow and Firewall Rule logs so you can see what's happening to the traffic across your network.
- Enable and monitor Packet Mirroring so you can replicate packets at the virtual machine network interface.
- And explain the capabilities of the Network Intelligence Center.

Fantastic job.

