Kandidnr: 163

DEPLOYMENT PLAN

GOAL

The goal is to secure and protect the company Strezilia's application, from both dataloss and vulnerabilities such as XSS, by moving it to a securly configured cloud solution with a secure infrastructure and backup possibilities.

PLAN

- Create a VM in GCP with a VPC
- create a VPC with a subnet for compute engine and activated flow logs
- Configurate the firewall to allow http traffic
- Create VPC with terraform with a subnet
- Snapshots for backup

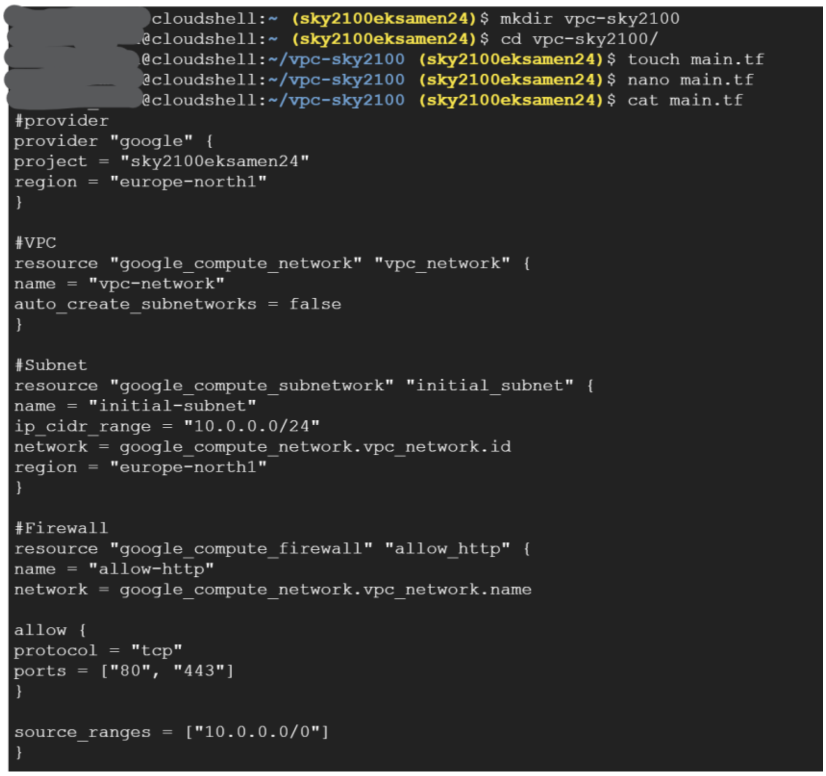
DOCUMENTATION

A1 Configuration:

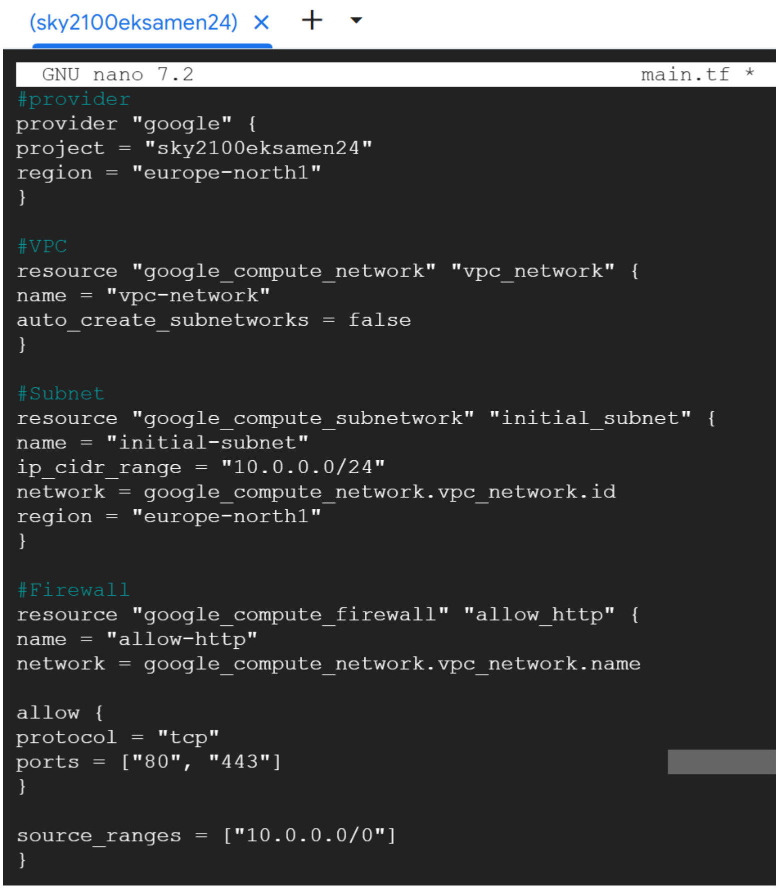
Started by creating a project in GCP and called it "SKY2100EKSAMEN", then I enabled compute engine API and opened up cloud shell. I checked and updated terraform to 1.10 and made a path for my terraform config files. I wanted to divide the components into different files, but found it easier to edit them all together in one file at first and then when I was done, divided them before applying.

Under you see how I originally started out on my code. I chose the region "Europe-north1" because it is the region closest to Norway. I used my own name as username, therefore I crossed it out.

Kandidnr: 163



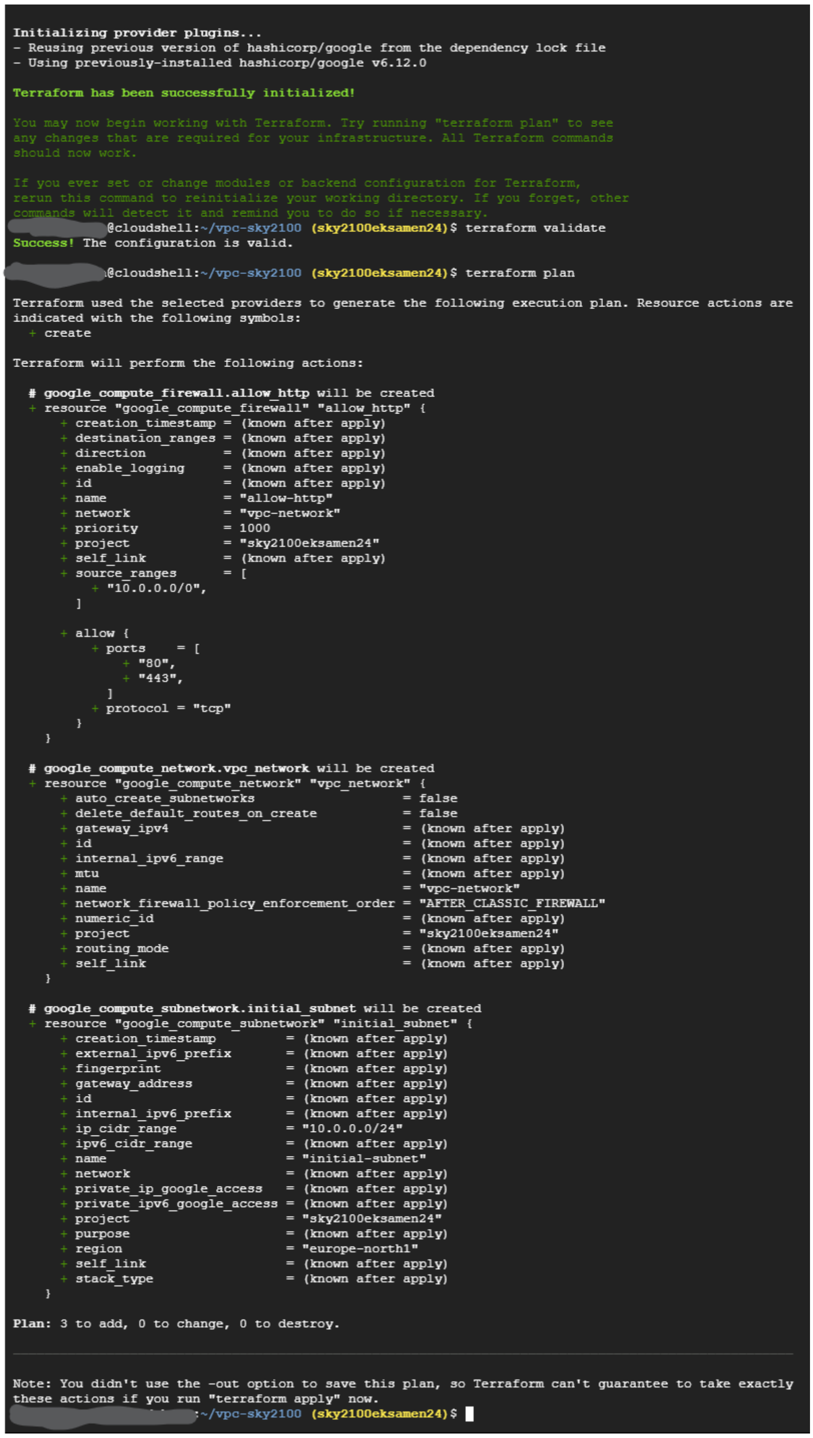
```
[redacted]cloudshell:~ (sky2100eksamen24)$ mkdir vpc-sky2100
@cloudshell:~ (sky2100eksamen24)$ cd vpc-sky2100/
@cloudshell:~/vpc-sky2100 (sky2100eksamen24)$ touch main.tf
@cloudshell:~/vpc-sky2100 (sky2100eksamen24)$ nano main.tf
@cloudshell:~/vpc-sky2100 (sky2100eksamen24)$ cat main.tf
#provider
provider "google" {
project = "sky2100eksamen24"
region = "europe-north1"
}

#VPC
resource "google_compute_network" "vpc_network" {
name = "vpc-network"
auto_create_subnetworks = false
}

#Subnet
resource "google_compute_subnetwork" "initial_subnet" {
name = "initial-subnet"
ip_cidr_range = "10.0.0.0/24"
network = google_compute_network.vpc_network.id
region = "europe-north1"
}

#Firewall
resource "google_compute_firewall" "allow_http" {
name = "allow-http"
network = google_compute_network.vpc_network.name

allow {
protocol = "tcp"
ports = ["80", "443"]
}

source_ranges = ["10.0.0.0/0"]
}
```



```
#provider
provider "google" {
project = "sky2100eksamen24"
region = "europe-north1"
}

#VPC
resource "google_compute_network" "vpc_network" {
name = "vpc-network"
auto_create_subnetworks = false
}

#Subnet
resource "google_compute_subnetwork" "initial_subnet" {
name = "initial-subnet"
ip_cidr_range = "10.0.0.0/24"
network = google_compute_network.vpc_network.id
region = "europe-north1"
}

#Firewall
resource "google_compute_firewall" "allow_http" {
name = "allow-http"
network = google_compute_network.vpc_network.name

allow {
protocol = "tcp"
ports = ["80", "443"]
}

source_ranges = ["10.0.0.0/0"]
}
```

I created a VPC named vpc-network and set auto_create_subnetworks to false, as I wanted to create my own subnetwork and set it to my region and make it possible for the company to create more with other regions later, if they were to expand globally as mentioned in the scenario.

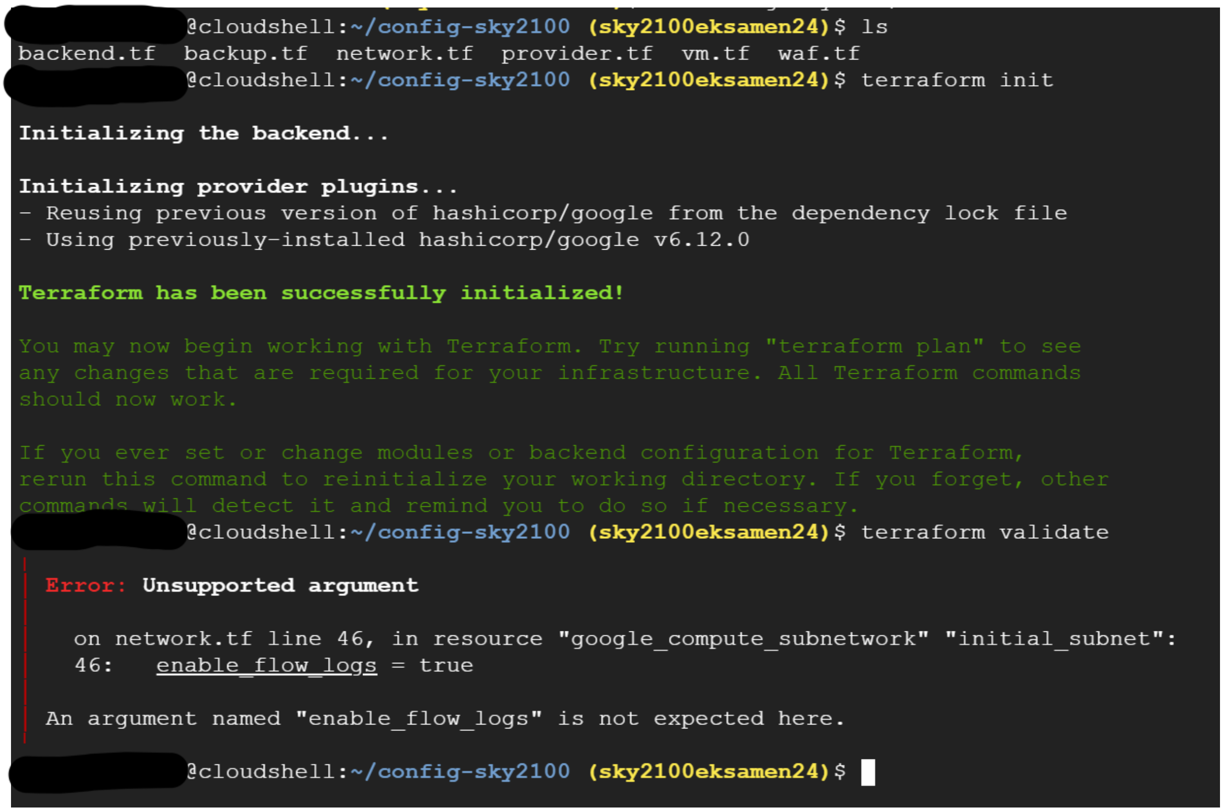
I also created a firewall for the vpc to allow http traffic through.



```
Initializing provider plugins...
- Reusing previous version of hashicorp/google from the dependency lock file
- Using previously-installed hashicorp/google v6.12.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
[redacted]@cloudshell:~/vpc-sky2100 (sky2100eksamen24)$ terraform validate
Success! The configuration is valid.

[redacted]@cloudshell:~/vpc-sky2100 (sky2100eksamen24)$ terraform plan

Terraform used the selected providers to generate the following execution plan. Resource actions are
indicated with the following symbols:
  + create

Terraform will perform the following actions:

  # google_compute_firewall.allow_http will be created
  + resource "google_compute_firewall" "allow_http" {
      + creation_timestamp = (known after apply)
      + destination_ranges = (known after apply)
      + direction          = (known after apply)
      + enable_logging     = (known after apply)
      + id                 = (known after apply)
      + name               = "allow-http"
      + network            = "vpc-network"
      + priority           = 1000
      + project            = "sky2100eksamen24"
      + self_link          = (known after apply)
      + source_ranges      = [
          + "10.0.0.0/0",
        ]

      + allow {
          + ports    = [
              + "80",
              + "443",
            ]
          + protocol = "tcp"
        }
    }

  # google_compute_network.vpc_network will be created
  + resource "google_compute_network" "vpc_network" {
      + auto_create_subnetworks                   = false
      + delete_default_routes_on_create           = false
      + gateway_ipv4                              = (known after apply)
      + id                                        = (known after apply)
      + internal_ipv6_range                       = (known after apply)
      + mtu                                       = (known after apply)
      + name                                      = "vpc-network"
      + network_firewall_policy_enforcement_order = "AFTER_CLASSIC_FIREWALL"
      + numeric_id                                = (known after apply)
      + project                                   = "sky2100eksamen24"
      + routing_mode                              = (known after apply)
      + self_link                                 = (known after apply)
    }

  # google_compute_subnetwork.initial_subnet will be created
  + resource "google_compute_subnetwork" "initial_subnet" {
      + creation_timestamp         = (known after apply)
      + external_ipv6_prefix       = (known after apply)
      + fingerprint                = (known after apply)
      + gateway_address            = (known after apply)
      + id                         = (known after apply)
      + internal_ipv6_prefix       = (known after apply)
      + ip_cidr_range              = "10.0.0.0/24"
      + ipv6_cidr_range            = (known after apply)
      + name                       = "initial-subnet"
      + network                    = (known after apply)
      + private_ip_google_access   = (known after apply)
      + private_ipv6_google_access = (known after apply)
      + project                    = "sky2100eksamen24"
      + purpose                    = (known after apply)
      + region                     = "europe-north1"
      + self_link                  = (known after apply)
      + stack_type                 = (known after apply)
    }

Plan: 3 to add, 0 to change, 0 to destroy.

─────────────────────────────────────────────────────────────────────────────

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly
these actions if you run "terraform apply" now.
[redacted]:~/vpc-sky2100 (sky2100eksamen24)$ █
```

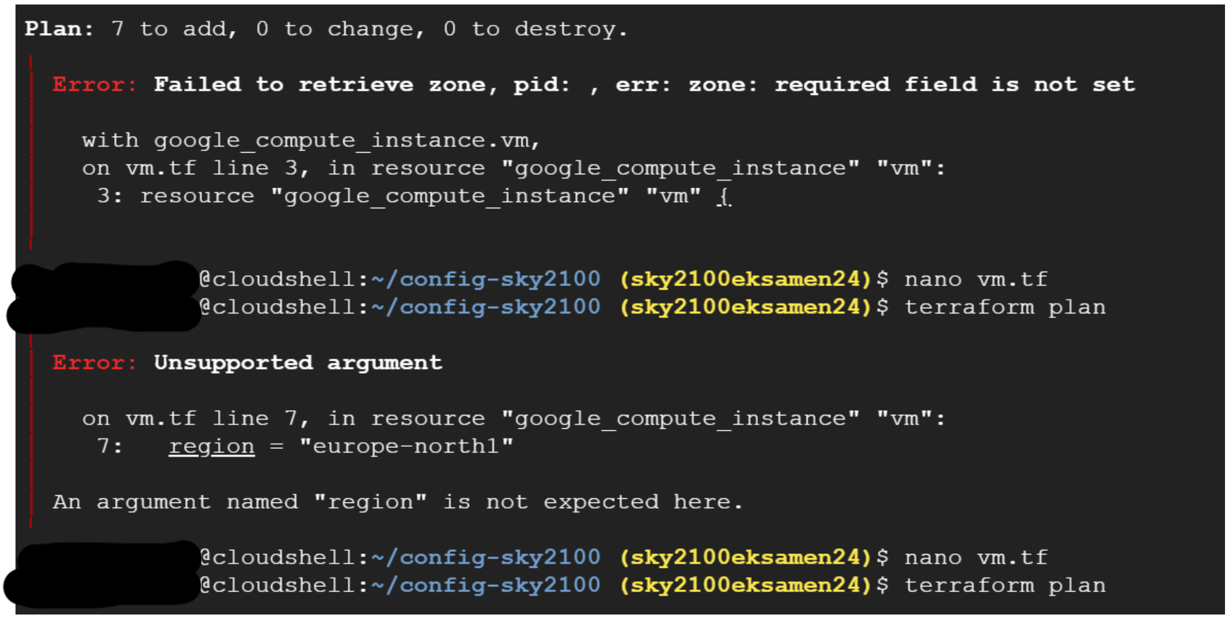
Over i tested my code with terraform validate and terraform plan to check if I had any syntax errors. I also decided to add some features and change some before applying, such as changing to an cloud armor as a firewall instead of the one I originally had. The code I ended up with before testing is attached as “terraform code before applying”

With the new code I had some errors when validating and trying to apply, so the code changed a lot before being able to apply it.



```
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ ls
backend.tf  backup.tf  network.tf  provider.tf  vm.tf  waf.tf
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of hashicorp/google from the dependency lock file
- Using previously-installed hashicorp/google v6.12.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ terraform validate
╷
│ Error: Unsupported argument
│
│   on network.tf line 46, in resource "google_compute_subnetwork" "initial_subnet":
│   46:   enable_flow_logs = true
│
│ An argument named "enable_flow_logs" is not expected here.
╵
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$
```

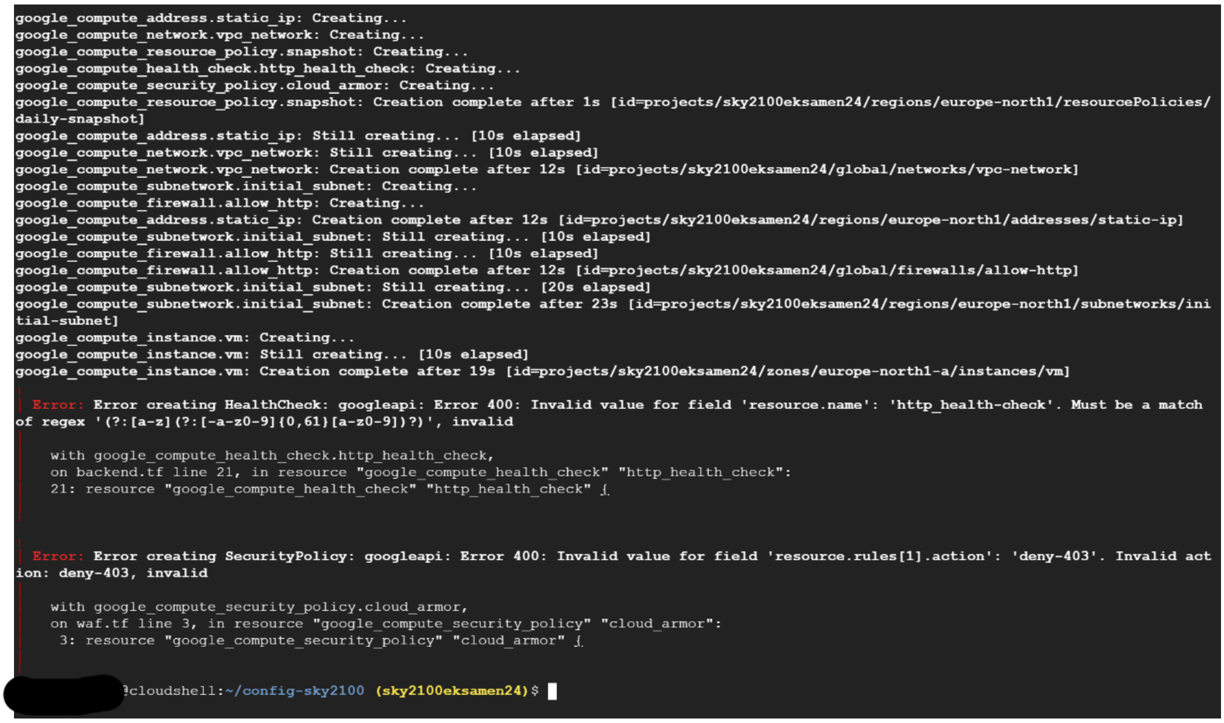
Problems with how flow logs are implemented



```
Plan: 7 to add, 0 to change, 0 to destroy.
╷
│ Error: Failed to retrieve zone, pid: , err: zone: required field is not set
│
│   with google_compute_instance.vm,
│   on vm.tf line 3, in resource "google_compute_instance" "vm":
│    3: resource "google_compute_instance" "vm" {
│
╵
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ nano vm.tf
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ terraform plan
╷
│ Error: Unsupported argument
│
│   on vm.tf line 7, in resource "google_compute_instance" "vm":
│    7:   region = "europe-north1"
│
│ An argument named "region" is not expected here.
╵
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ nano vm.tf
[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ terraform plan
```

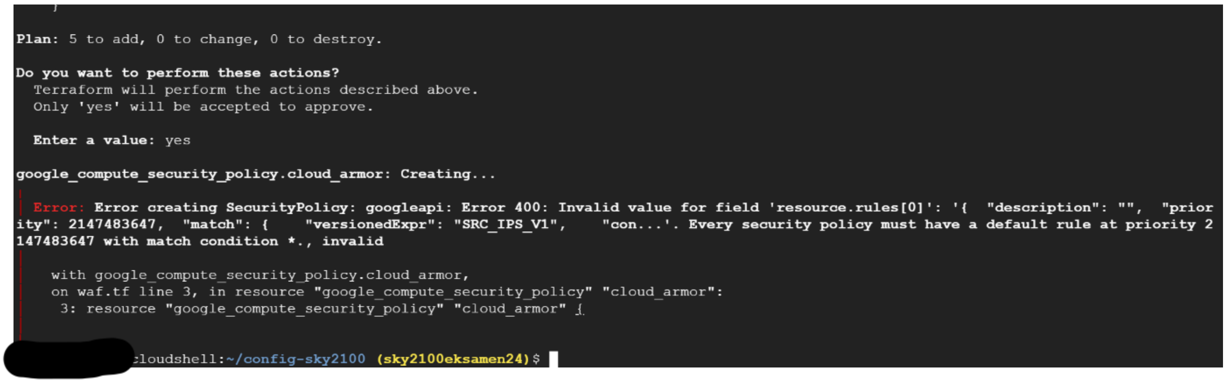
Missing zone and region not being expected in VM.

Kandidnr: 163



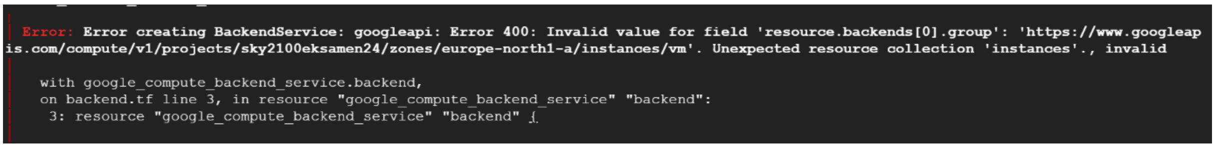
```
google_compute_address.static_ip: Creating...
google_compute_network.vpc_network: Creating...
google_compute_resource_policy.snapshot: Creating...
google_compute_health_check.http_health_check: Creating...
google_compute_security_policy.cloud_armor: Creating...
google_compute_resource_policy.snapshot: Creation complete after 1s [id=projects/sky2100eksamen24/regions/europe-north1/resourcePolicies/
daily-snapshot]
google_compute_address.static_ip: Still creating... [10s elapsed]
google_compute_network.vpc_network: Still creating... [10s elapsed]
google_compute_network.vpc_network: Creation complete after 12s [id=projects/sky2100eksamen24/global/networks/vpc-network]
google_compute_subnetwork.initial_subnet: Creating...
google_compute_firewall.allow_http: Creating...
google_compute_address.static_ip: Creation complete after 12s [id=projects/sky2100eksamen24/regions/europe-north1/addresses/static-ip]
google_compute_subnetwork.initial_subnet: Still creating... [10s elapsed]
google_compute_firewall.allow_http: Still creating... [10s elapsed]
google_compute_firewall.allow_http: Creation complete after 12s [id=projects/sky2100eksamen24/global/firewalls/allow-http]
google_compute_subnetwork.initial_subnet: Still creating... [20s elapsed]
google_compute_subnetwork.initial_subnet: Creation complete after 23s [id=projects/sky2100eksamen24/regions/europe-north1/subnetworks/ini
tial-subnet]
google_compute_instance.vm: Creating...
google_compute_instance.vm: Still creating... [10s elapsed]
google_compute_instance.vm: Creation complete after 19s [id=projects/sky2100eksamen24/zones/europe-north1-a/instances/vm]

│ Error: Error creating HealthCheck: googleapi: Error 400: Invalid value for field 'resource.name': 'http_health-check'. Must be a match
of regex '(?:[a-z](?:[-a-z0-9]{0,61}[a-z0-9])?)', invalid
│
│   with google_compute_health_check.http_health_check,
│   on backend.tf line 21, in resource "google_compute_health_check" "http_health_check":
│   21: resource "google_compute_health_check" "http_health_check" {
│
│

│ Error: Error creating SecurityPolicy: googleapi: Error 400: Invalid value for field 'resource.rules[1].action': 'deny-403'. Invalid act
ion: deny-403, invalid
│
│   with google_compute_security_policy.cloud_armor,
│   on waf.tf line 3, in resource "google_compute_security_policy" "cloud_armor":
│    3: resource "google_compute_security_policy" "cloud_armor" {
│

[redacted]@cloudshell:~/config-sky2100 (sky2100eksamen24)$ █
```

Syntax error



```
    }

Plan: 5 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes

google_compute_security_policy.cloud_armor: Creating...
│
│ Error: Error creating SecurityPolicy: googleapi: Error 400: Invalid value for field 'resource.rules[0]': '{  "description": "",  "prior
ity": 2147483647,  "match": {    "versionedExpr": "SRC_IPS_V1",    "con...'. Every security policy must have a default rule at priority 2
147483647 with match condition *., invalid
│
│   with google_compute_security_policy.cloud_armor,
│   on waf.tf line 3, in resource "google_compute_security_policy" "cloud_armor":
│    3: resource "google_compute_security_policy" "cloud_armor" {
│

[redacted]cloudshell:~/config-sky2100 (sky2100eksamen24)$ █
```

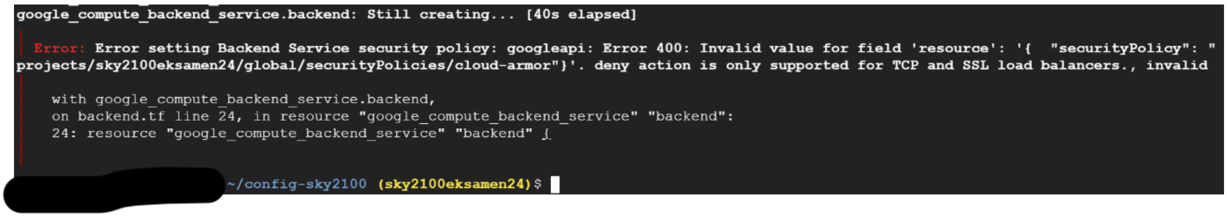
Forgot a default rule in cloud armor



```
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field 'resource.backends[0].group': 'https://www.googleap
is.com/compute/v1/projects/sky2100eksamen24/zones/europe-north1-a/instances/vm'. Unexpected resource collection 'instances'., invalid
│
│   with google_compute_backend_service.backend,
│   on backend.tf line 3, in resource "google_compute_backend_service" "backend":
│    3: resource "google_compute_backend_service" "backend" {
│
```

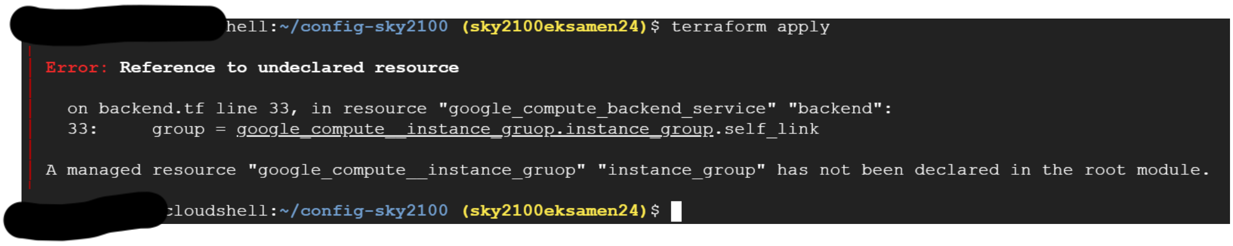
Problems with creating an instance group for a single VM to have a load balancer.

Kandidnr: 163



```
google_compute_backend_service.backend: Still creating... [40s elapsed]

│ Error: Error setting Backend Service security policy: googleapi: Error 400: Invalid value for field 'resource': '{  "securityPolicy": "
projects/sky2100eksamen24/global/securityPolicies/cloud-armor"}'. deny action is only supported for TCP and SSL load balancers., invalid
│
│   with google_compute_backend_service.backend,
│   on backend.tf line 24, in resource "google_compute_backend_service" "backend":
│   24: resource "google_compute_backend_service" "backend" {
│
[redacted]~/config-sky2100 (sky2100eksamen24)$ 
```

Problems implementing deny rules for cloud armor

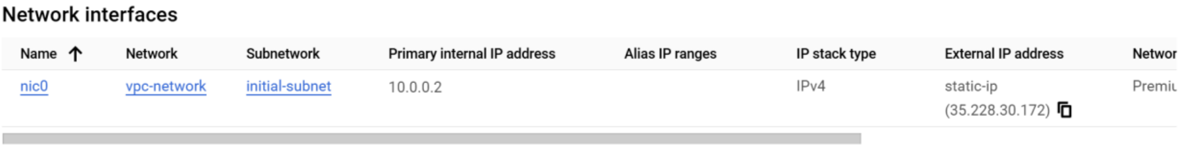


```
[redacted]hell:~/config-sky2100 (sky2100eksamen24)$ terraform apply

 Error: Reference to undeclared resource

   on backend.tf line 33, in resource "google_compute_backend_service" "backend":
   33:     group = google_compute__instance_gruop.instance_group.self_link

 A managed resource "google_compute__instance_gruop" "instance_group" has not been declared in the root module.

[redacted]cloudshell:~/config-sky2100 (sky2100eksamen24)$ 
```

Syntax error in google_compute_instance_group.

After I fixed all of theese, I was able to apply my terraform code. (final code is attached as terraform files) I also attached a file with my code under edititng.

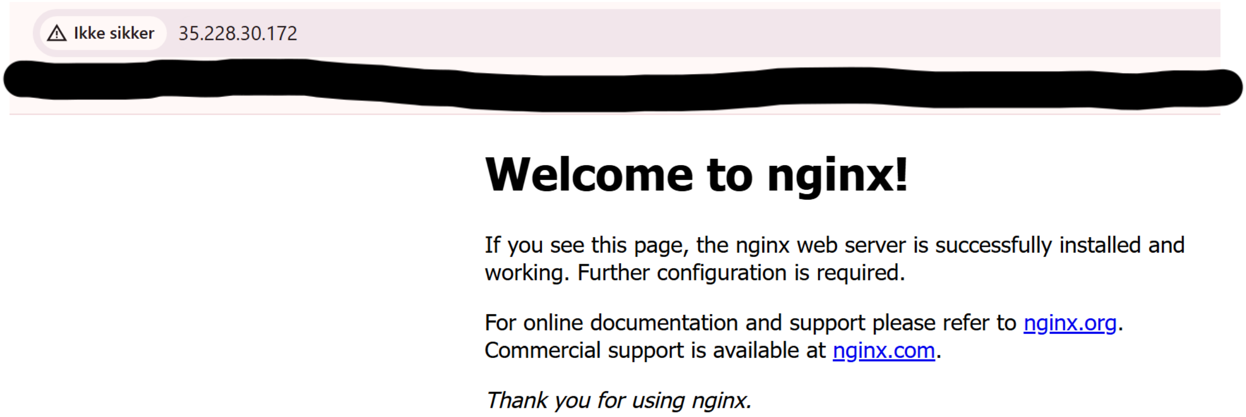
A1 Testing and improving:



Network interfaces

Name ↑	Network	Subnetwork	Primary internal IP address	Alias IP ranges	IP stack type	External IP address	Networ
nic0	vpc-network	initial-subnet	10.0.0.2		IPv4	static-ip (35.228.30.172)	Premiu

Found the ip-adress to my VM



⚠ Ikke sikker 35.228.30.172

[redacted]

Welcome to nginx!

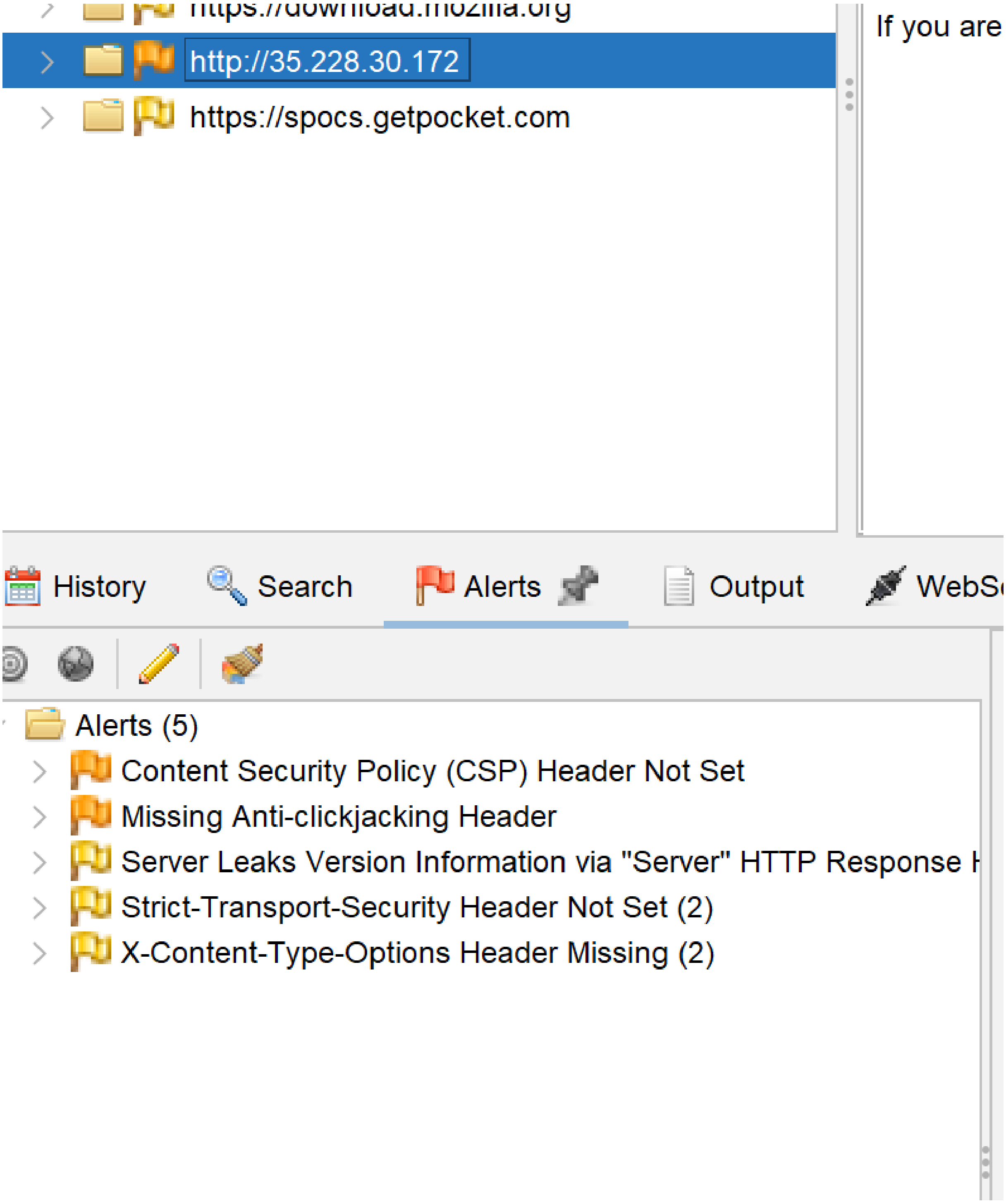
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Kandidnr: 163

Opened it up in a web browser



https://download.mozilla.org

http://35.228.30.172

https://spocs.getpocket.com

If you are

Alerts (5)

Content Security Policy (CSP) Header Not Set

Missing Anti-clickjacking Header

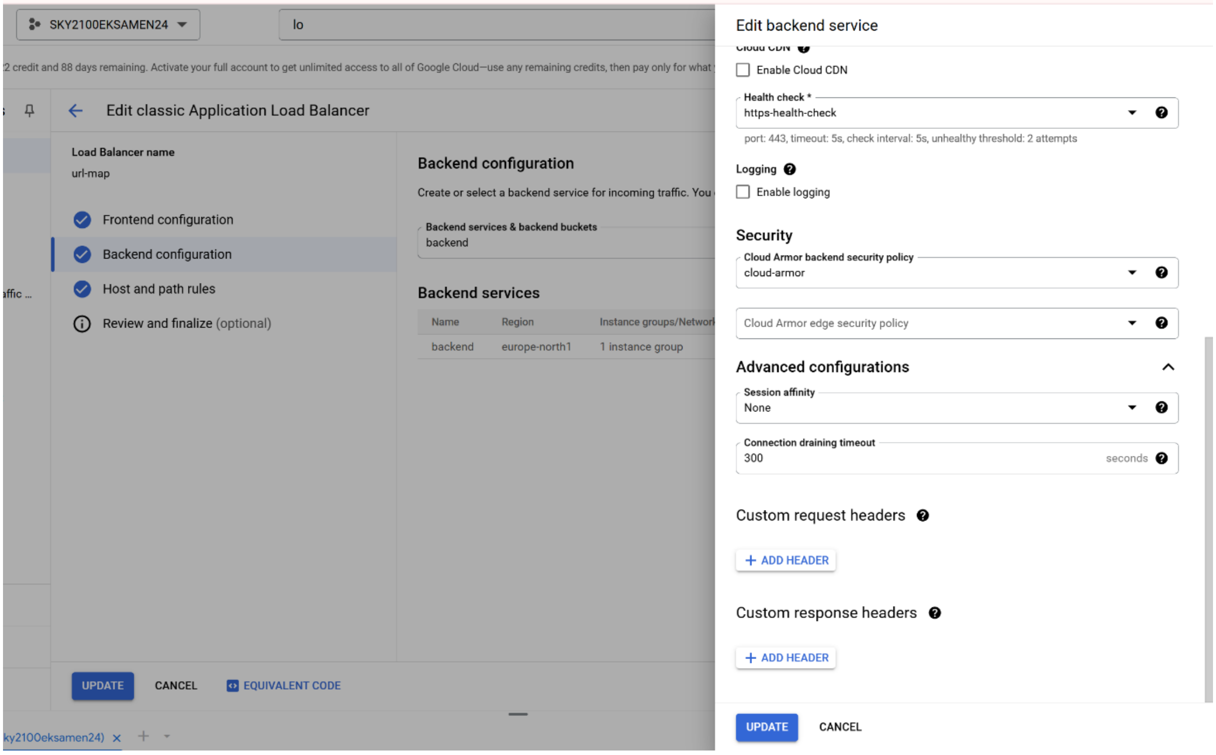
Server Leaks Version Information via "Server" HTTP Response H

Strict-Transport-Security Header Not Set (2)

X-Content-Type-Options Header Missing (2)

Ran a owasp zap scan and got 5 alerts, 4 of which headers were missing.

Kandidnr: 163



SKY2100EKSAMEN24 ▾ lo

2 credit and 88 days remaining. Activate your full account to get unlimited access to all of Google Cloud—use any remaining credits, then pay only for what

← Edit classic Application Load Balancer

Load Balancer name
url-map

- ✓ Frontend configuration
- ✓ Backend configuration
- ✓ Host and path rules
- ⓘ Review and finalize (optional)

Backend configuration

Create or select a backend service for incoming traffic. You

Backend services & backend buckets: backend

Backend services

Name	Region	Instance groups/Networl
backend	europe-north1	1 instance group

UPDATE CANCEL EQUIVALENT CODE

ky2100eksamen24) ×

Edit backend service

Cloud CDN

□ Enable Cloud CDN

Health check *: https-health-check

port: 443, timeout: 5s, check interval: 5s, unhealthy threshold: 2 attempts

Logging

□ Enable logging

Security

Cloud Armor backend security policy: cloud-armor

Cloud Armor edge security policy

Advanced configurations

Session affinity: None

Connection draining timeout: 300 seconds

Custom request headers

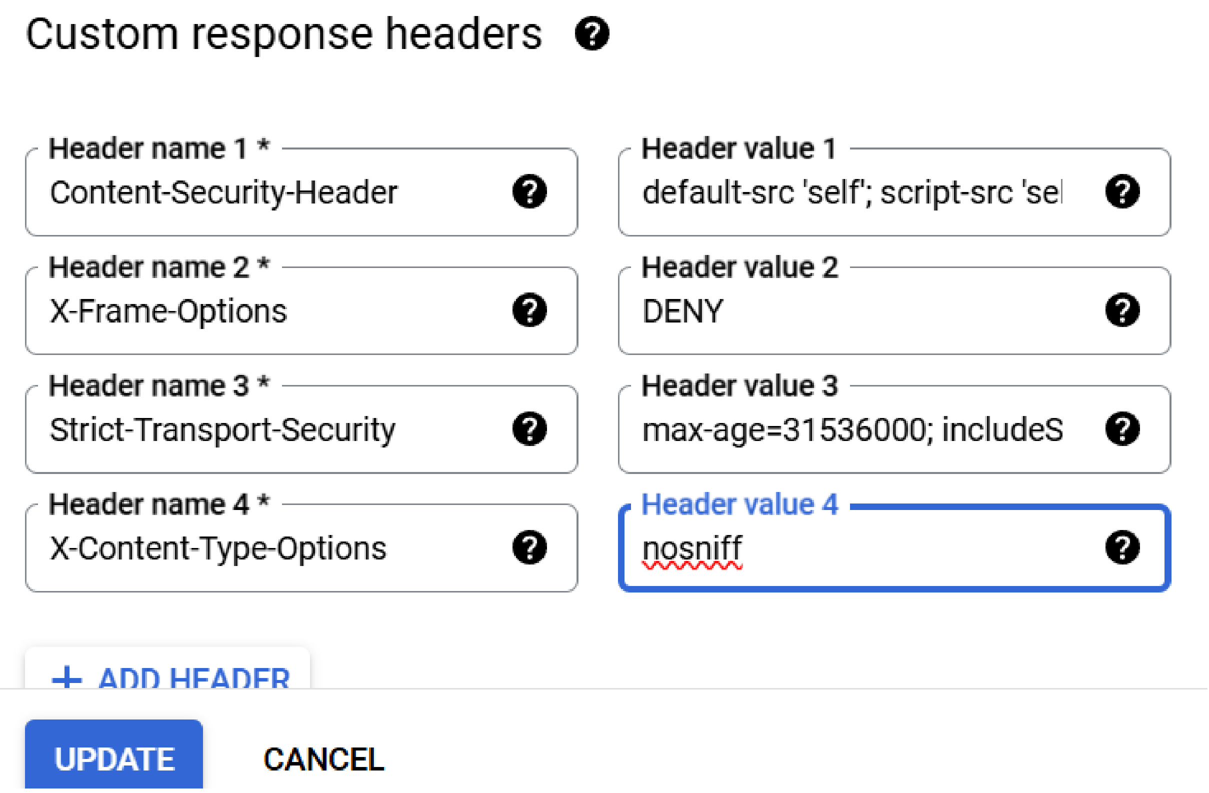
+ ADD HEADER

Custom response headers

+ ADD HEADER

UPDATE CANCEL

Decided to do the rest in clickops, adding missing headers to backend in the load balancer under costum headers.

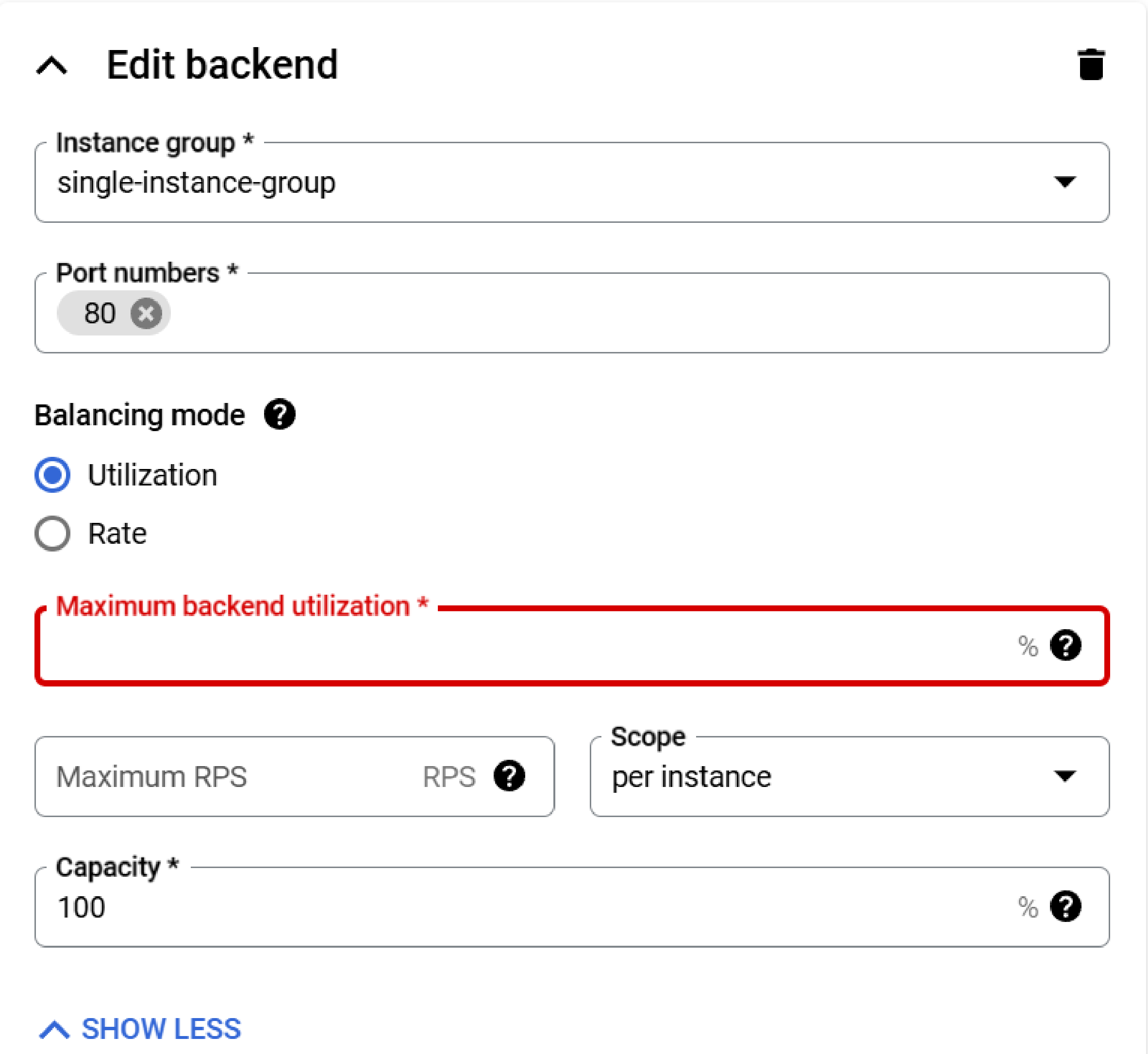


Custom response headers

Header name 1 * Content-Security-Header	Header value 1 default-src 'self'; script-src 'sel
Header name 2 * X-Frame-Options	Header value 2 DENY
Header name 3 * Strict-Transport-Security	Header value 3 max-age=31536000; includeS
Header name 4 * X-Content-Type-Options	Header value 4 nosniff

Adding headers missing in backend under url-map load balancing.

Kandidnr: 163



Edit backend

Instance group *: single-instance-group

Port numbers *: 80

Balancing mode

● Utilization

○ Rate

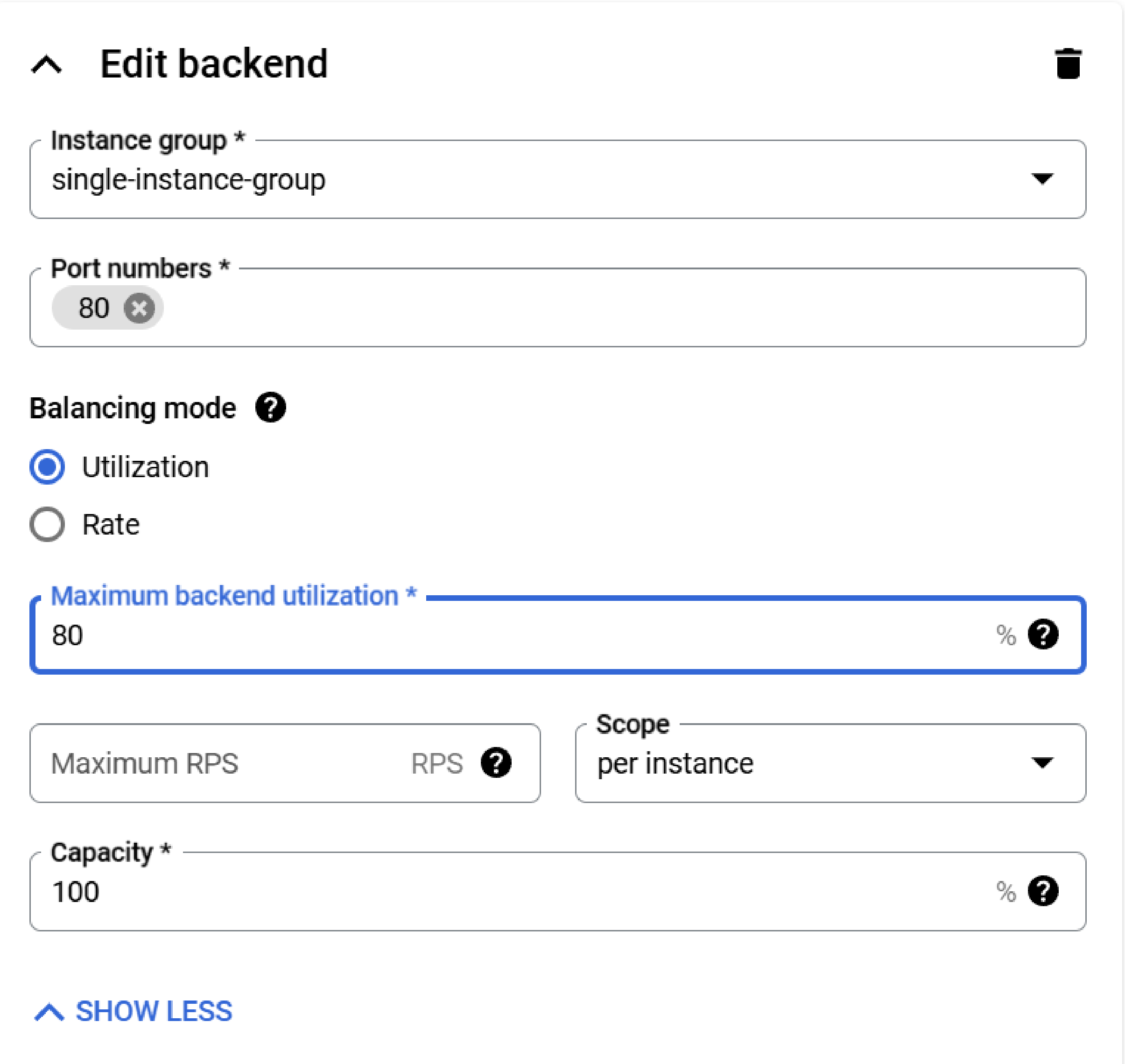
Maximum backend utilization *

Scope: per instance

Capacity *: 100

Had to add a maximum backend utilization

Kandidnr: 163



Edit backend

Instance group *: single-instance-group

Port numbers *: 80

Balancing mode

● Utilization

○ Rate

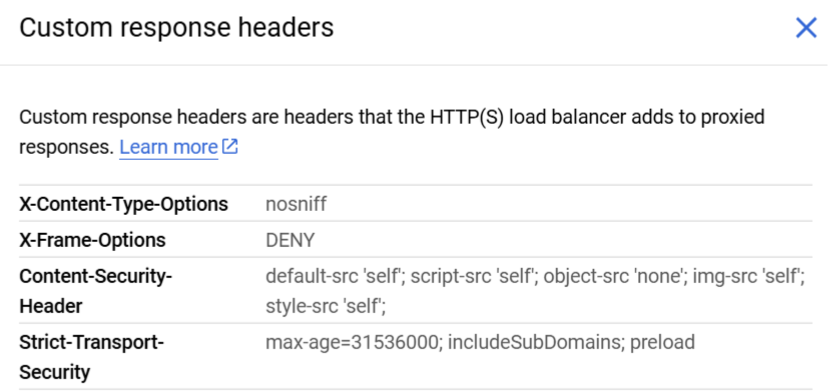
Maximum backend utilization *: 80 %

Maximum RPS: RPS

Scope: per instance

Capacity *: 100 %

Set it to 80%



Custom response headers

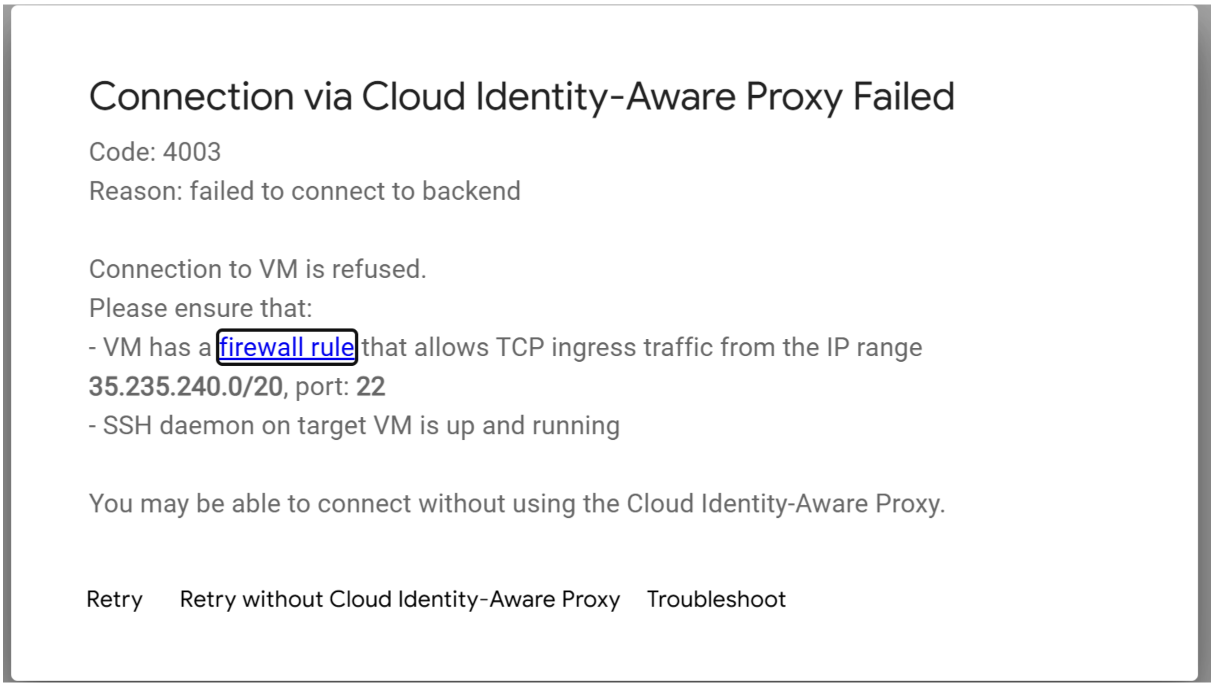
Custom response headers are headers that the HTTP(S) load balancer adds to proxied responses. Learn more

X-Content-Type-Options	nosniff
X-Frame-Options	DENY
Content-Security-Header	default-src 'self'; script-src 'self'; object-src 'none'; img-src 'self'; style-src 'self';
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload

This is a better representation of the custom headers.

Kandidnr: 163

Found out that the headers was not fully implemented and that I had to add them ti the nginx server as well.



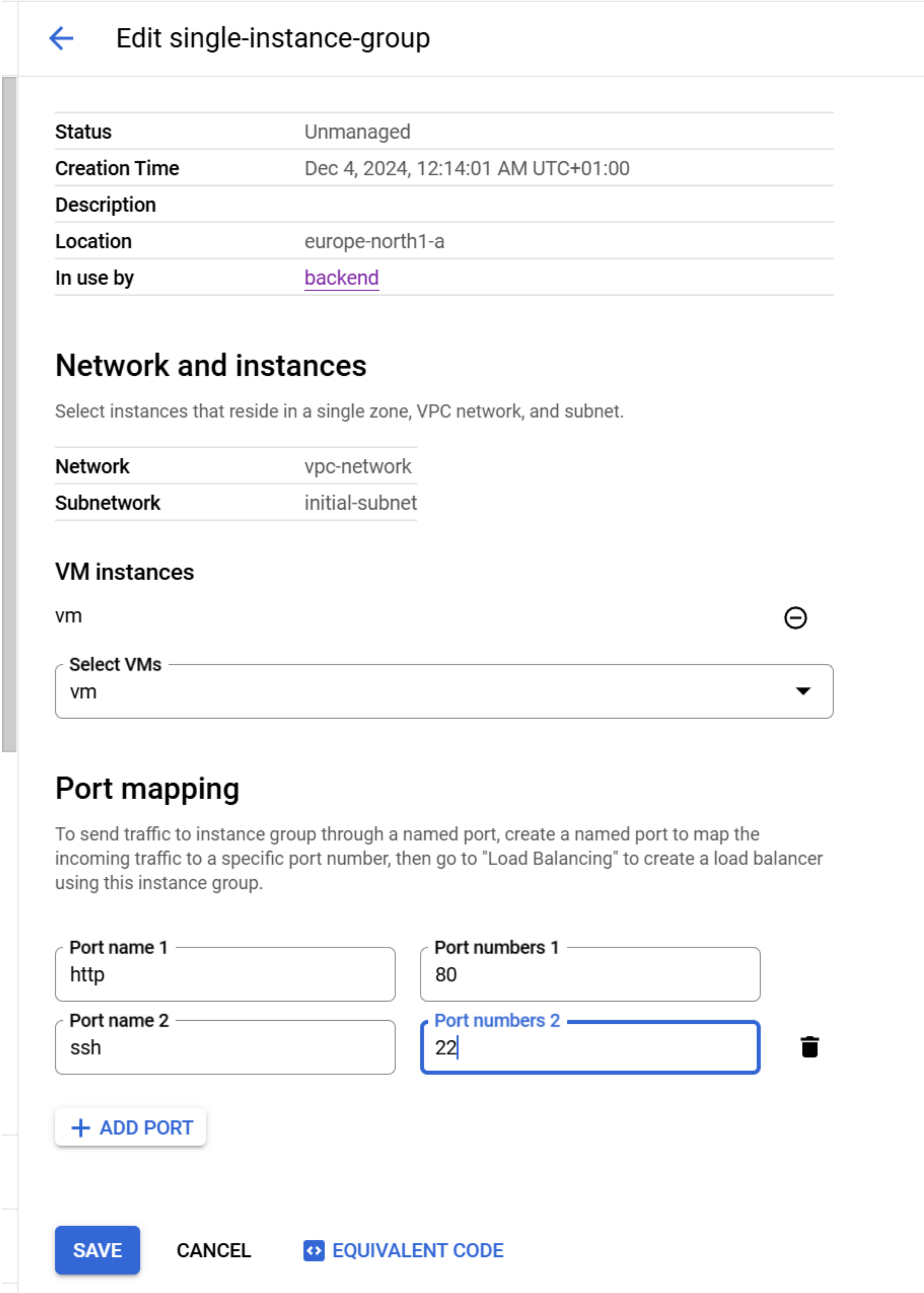
Connection via Cloud Identity-Aware Proxy Failed

Code: 4003
Reason: failed to connect to backend

Connection to VM is refused.
Please ensure that:
- VM has a firewall rule that allows TCP ingress traffic from the IP range **35.235.240.0/20**, port: **22**
- SSH daemon on target VM is up and running

You may be able to connect without using the Cloud Identity-Aware Proxy.

Had problems when trying to access the VM through ssh, had to open the port and make a firewall rule allowing traffic.



Edit single-instance-group

Status	Unmanaged
Creation Time	Dec 4, 2024, 12:14:01 AM UTC+01:00
Description	
Location	europe-north1-a
In use by	backend

Network and instances

Select instances that reside in a single zone, VPC network, and subnet.

Network	vpc-network
Subnetwork	initial-subnet

VM instances

vm ⊖

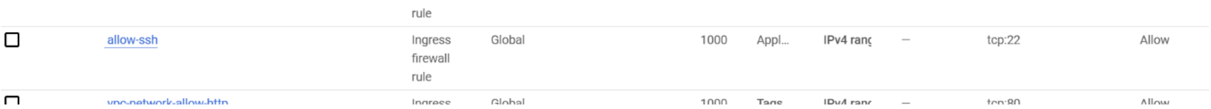
Select VMs: vm

Port mapping

To send traffic to instance group through a named port, create a named port to map the incoming traffic to a specific port number, then go to "Load Balancing" to create a load balancer using this instance group.

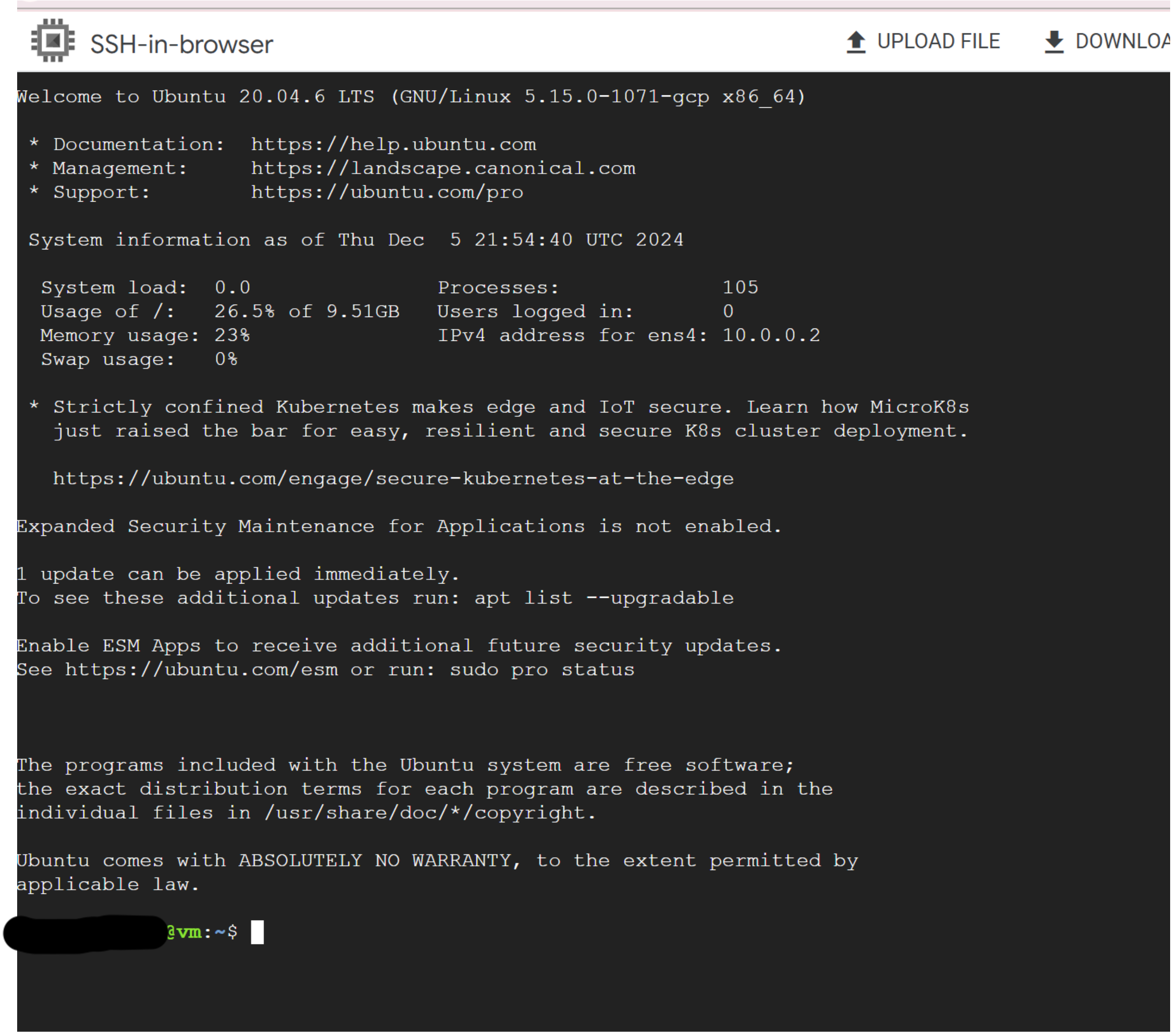
Port name 1: http
Port numbers 1: 80

Port name 2: ssh
Port numbers 2: 22



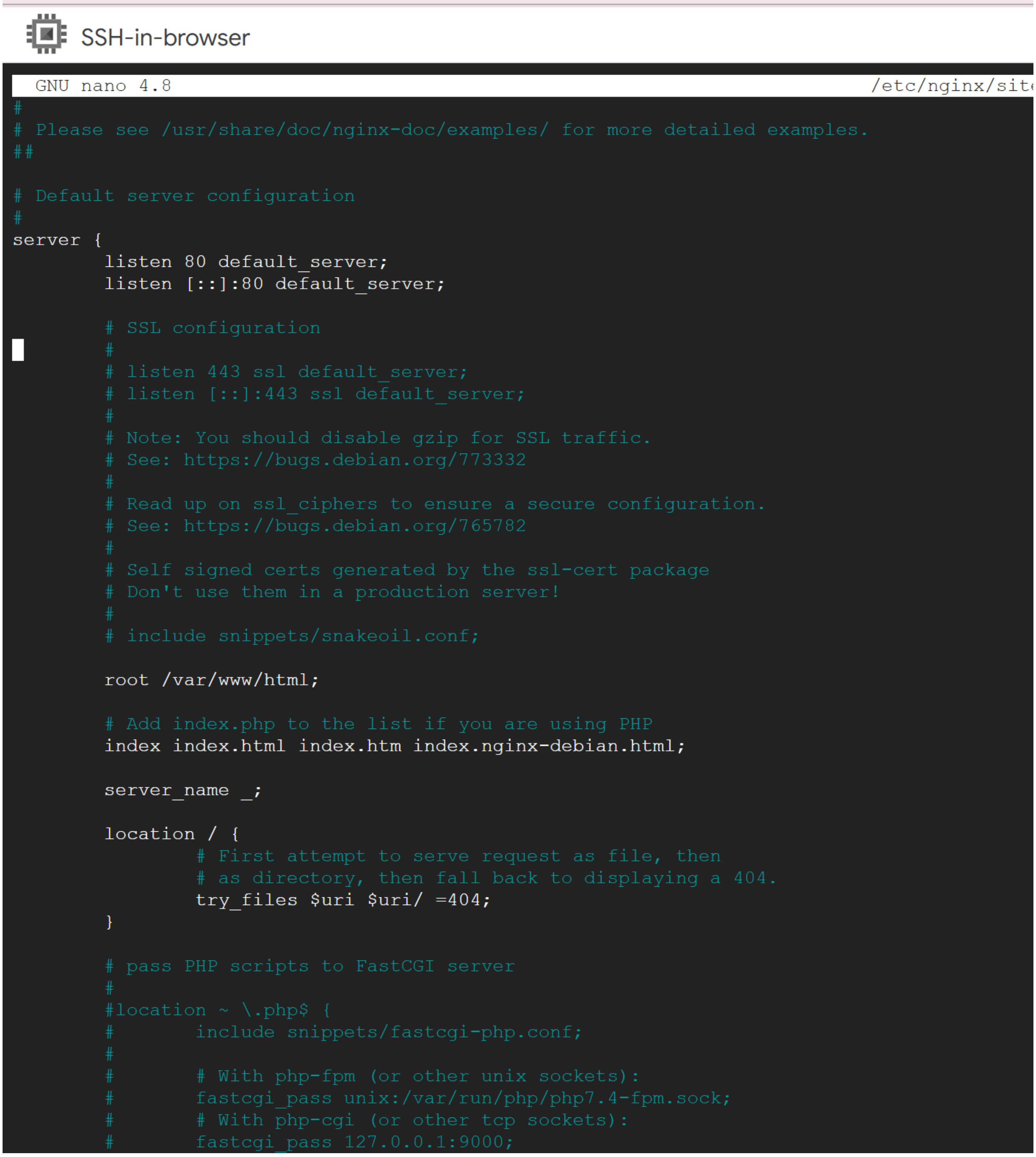
		rule							
□	allow-ssh	Ingress firewall rule	Global	1000	Appl...	IPv4 ranc	–	tcp:22	Allow
□	vpc-network-allow-http	Ingress	Global	1000	Tags	IPv4 ranc	–	tcp:80	Allow

Kandidnr: 163



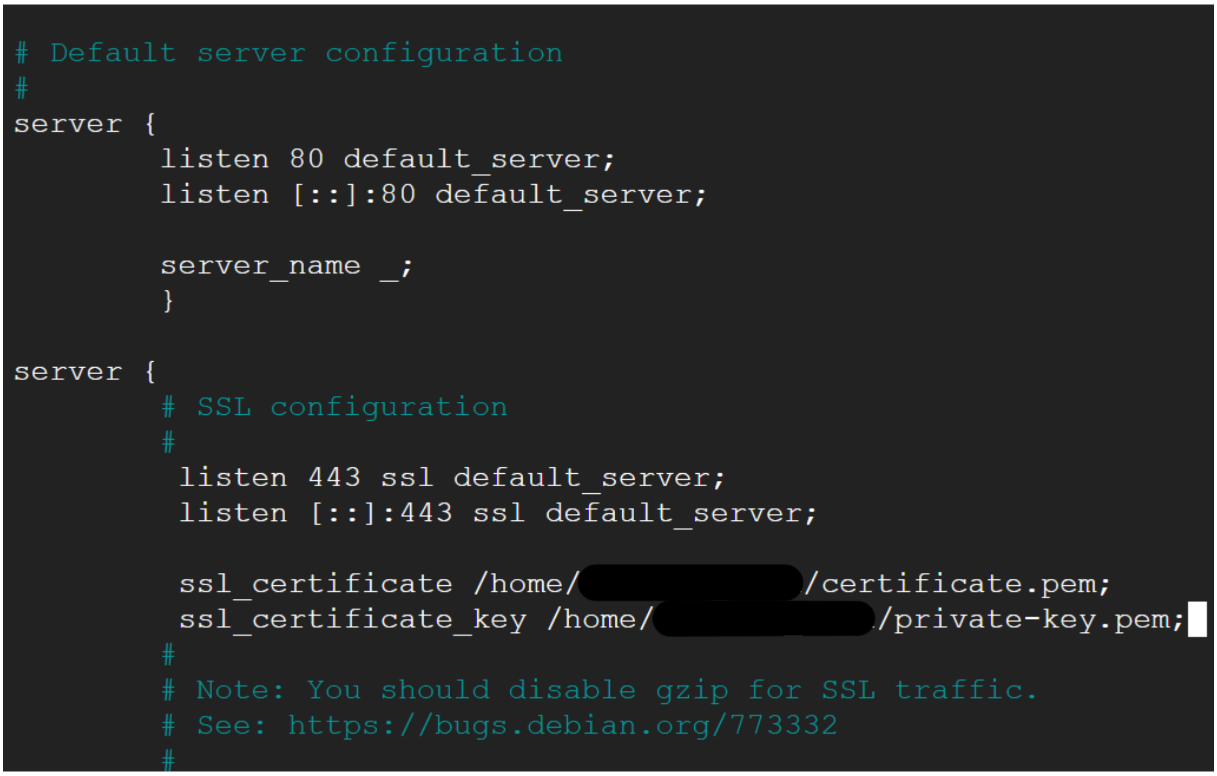
```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1071-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Dec  5 21:54:40 UTC 2024

  System load:  0.0                Processes:             105
  Usage of /:   26.5% of 9.51GB   Users logged in:       0
  Memory usage: 23%                IPv4 address for ens4: 10.0.0.2
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[redacted]@vm:~$ 
```

Accessed the vm through ssh.



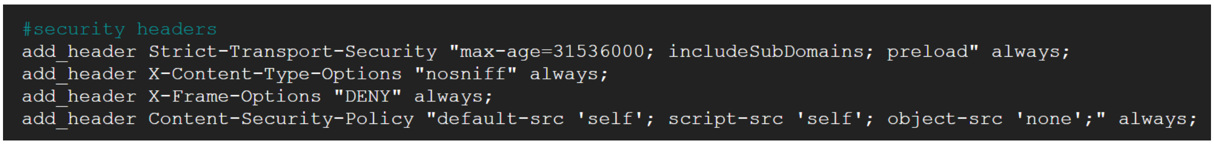
```
  GNU nano 4.8                                                         /etc/nginx/site
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        # pass PHP scripts to FastCGI server
        #
        #location ~ \.php$ {
        #       include snippets/fastcgi-php.conf;
        #
        #       # With php-fpm (or other unix sockets):
        #       fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
```

Edited the config file.



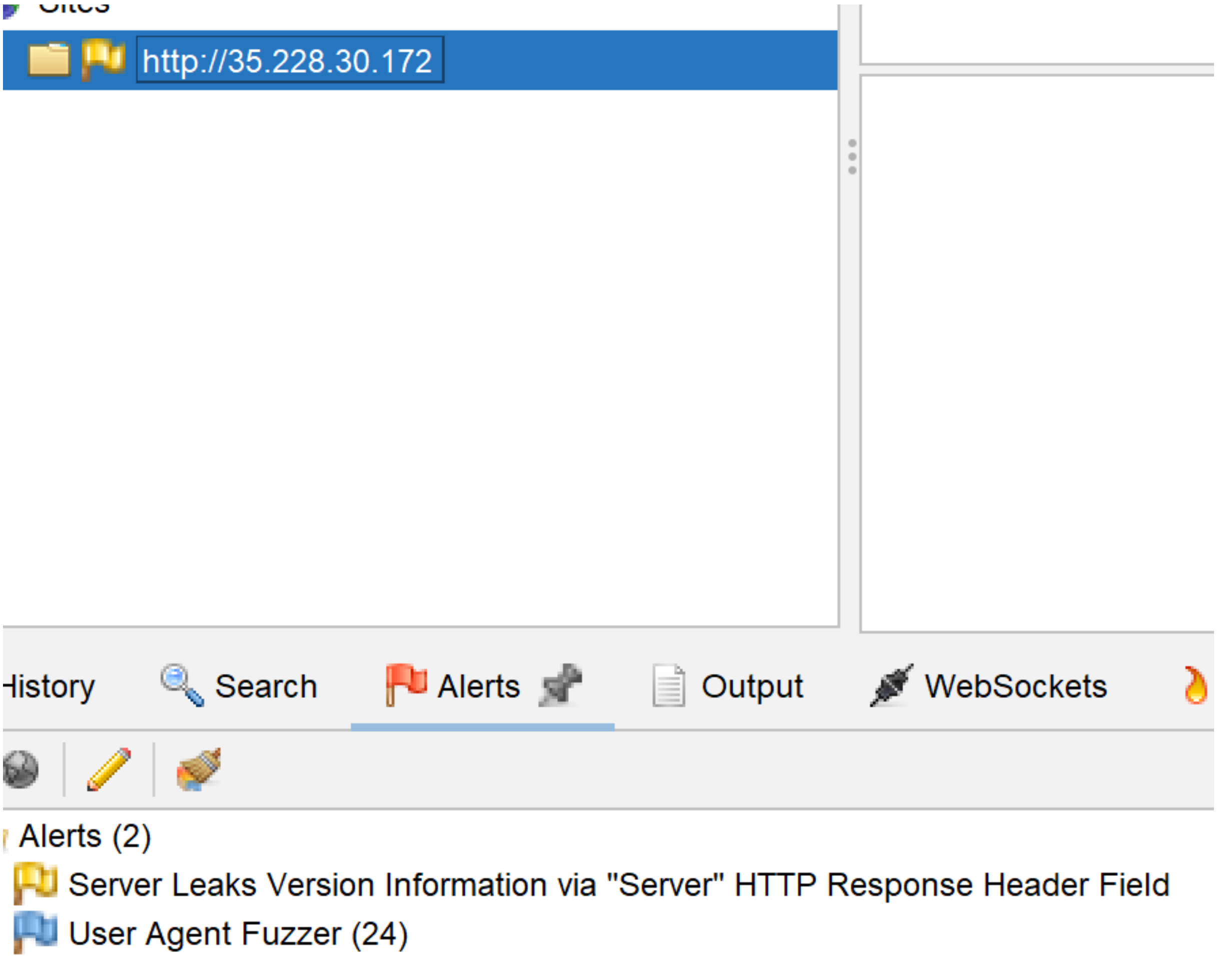
```
# Default server configuration
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        server_name _;
        }

server {
        # SSL configuration
        #
         listen 443 ssl default_server;
         listen [::]:443 ssl default_server;

         ssl_certificate /home/[redacted]/certificate.pem;
         ssl_certificate_key /home/[redacted]/private-key.pem;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
```

Added the ssl certificate to the nginx server as well.



```
#security headers
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
add_header X-Content-Type-Options "nosniff" always;
add_header X-Frame-Options "DENY" always;
add_header Content-Security-Policy "default-src 'self'; script-src 'self'; object-src 'none';" always;
```

And added the missing security headers to the server.

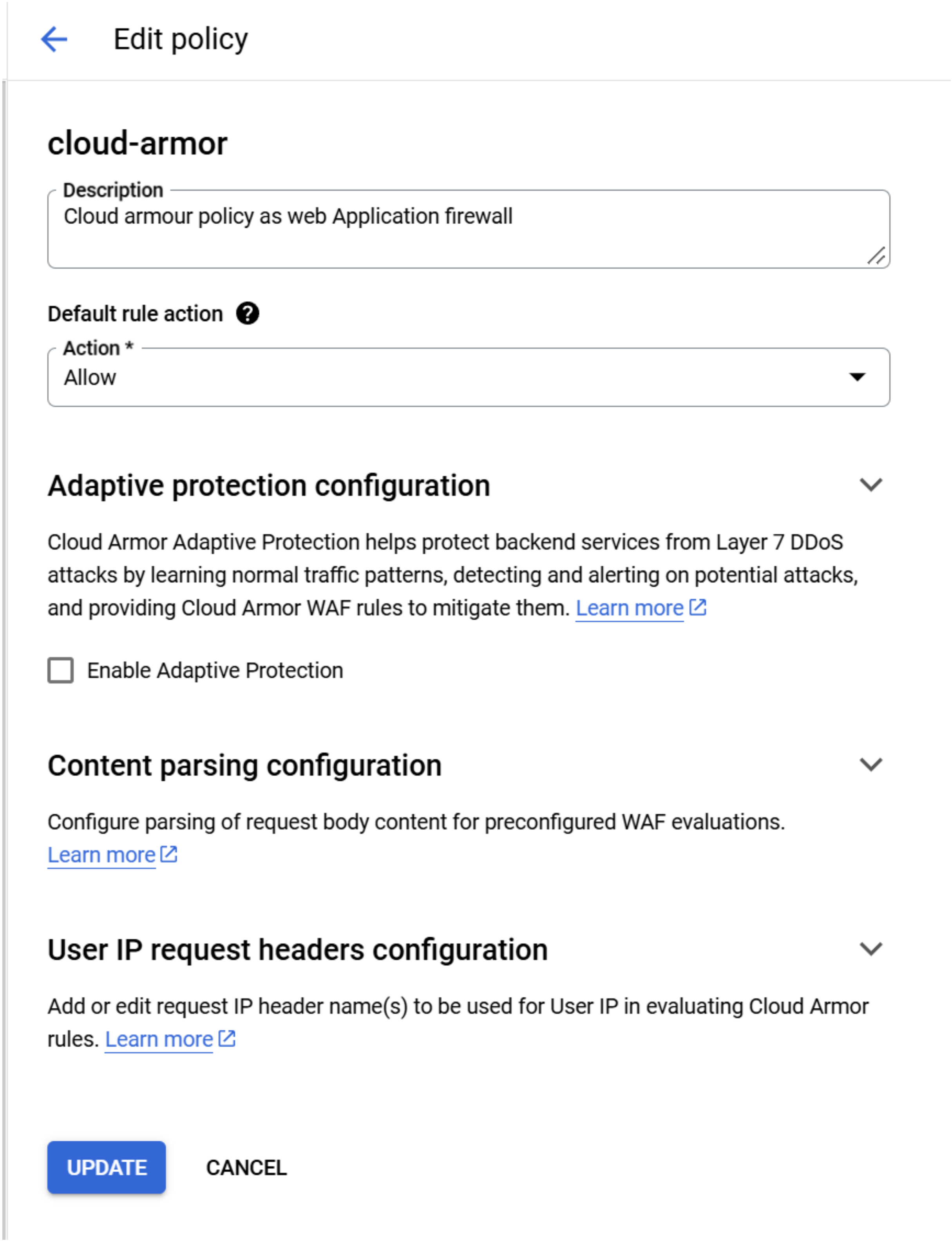


Alerts (2)

Server Leaks Version Information via "Server" HTTP Response Header Field

User Agent Fuzzer (24)

Scanning results after implementing the headers.



Edit policy

cloud-armor

Description
Cloud armour policy as web Application firewall

Default rule action

Action *
Allow

Adaptive protection configuration

Cloud Armor Adaptive Protection helps protect backend services from Layer 7 DDoS attacks by learning normal traffic patterns, detecting and alerting on potential attacks, and providing Cloud Armor WAF rules to mitigate them. Learn more

□ Enable Adaptive Protection

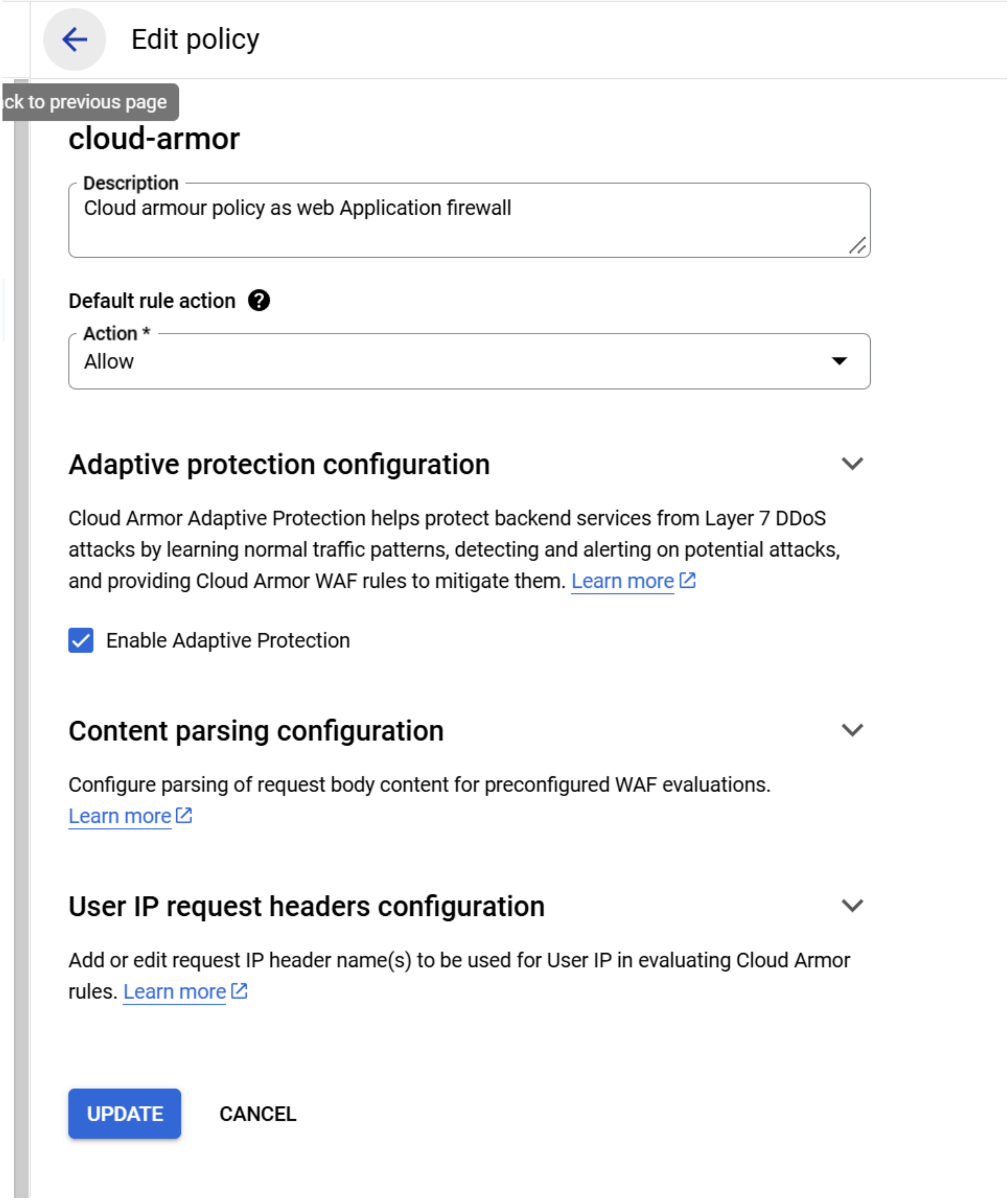
Content parsing configuration

Configure parsing of request body content for preconfigured WAF evaluations. Learn more

User IP request headers configuration

Add or edit request IP header name(s) to be used for User IP in evaluating Cloud Armor rules. Learn more

Kandidnr: 163



cloud-armor

Description: Cloud armour policy as web Application firewall

Default rule action

Action *: Allow

Adaptive protection configuration

Cloud Armor Adaptive Protection helps protect backend services from Layer 7 DDoS attacks by learning normal traffic patterns, detecting and alerting on potential attacks, and providing Cloud Armor WAF rules to mitigate them. Learn more

☑ Enable Adaptive Protection

Content parsing configuration

Configure parsing of request body content for preconfigured WAF evaluations. Learn more

User IP request headers configuration

Add or edit request IP header name(s) to be used for User IP in evaluating Cloud Armor rules. Learn more

Added adaptive protection configuration.