TRABAJO DE FIN DE TITULACIÓN

DESARROLLO DE UNA HERRAMIENTA PARA EL DESPLIEGUE AUTOMATIZADO DE ESCENARIOS DE RED VIRTUALIZADOS APLICABLES A PLATAFORMAS CYBER RANGE

ETSIT UPM
ESCUELA TECNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

UNIVERSIDAD POLITÉCNICA MADRID
POLITÉCNICA

PRESENTACIÓN

Autor: Samuel García Sánchez
Tutor: Mario Sanz Rodrigo

5 JULIO 2022

Objetivos

Realizar despliegues de red heterogéneos virtualizados, aplicables a plataformas Cyber Range para la formación y entrenamiento en el campo de la ciberseguridad.

Determinar los escenarios a desplegar, de forma que reflejen situaciones que se ajusten a la realidad

Despliegue de infraestructura modelable mediante variables, escalable, portable y seguro

Diseñar y configurar la comunicación entre los elementos que componen los escenarios

Desarrollo de una herramienta que sirva como base para la configuración software de los escenarios

Tecnologías

VIRTUALIZACIÓN

KVM

VirtualBox

vmware

Linux Containers

APROVISIONAMIENTO

HashiCorp Vagrant

CHEF

ANSIBLE

BASH
THE BOURNE-AGAIN SHELL

ORQUESTACIÓN

Docker Compose

kubernetes

Google Cloud Platform

HashiCorp Terraform

Google Cloud Platform

GCP → todas las herramientas de Google disponibles en la nube

Google Cloud

Compute Engine: Hosting y procesamiento

Virtual Private Cloud: Networking

Ventajas del despliegue en cloud

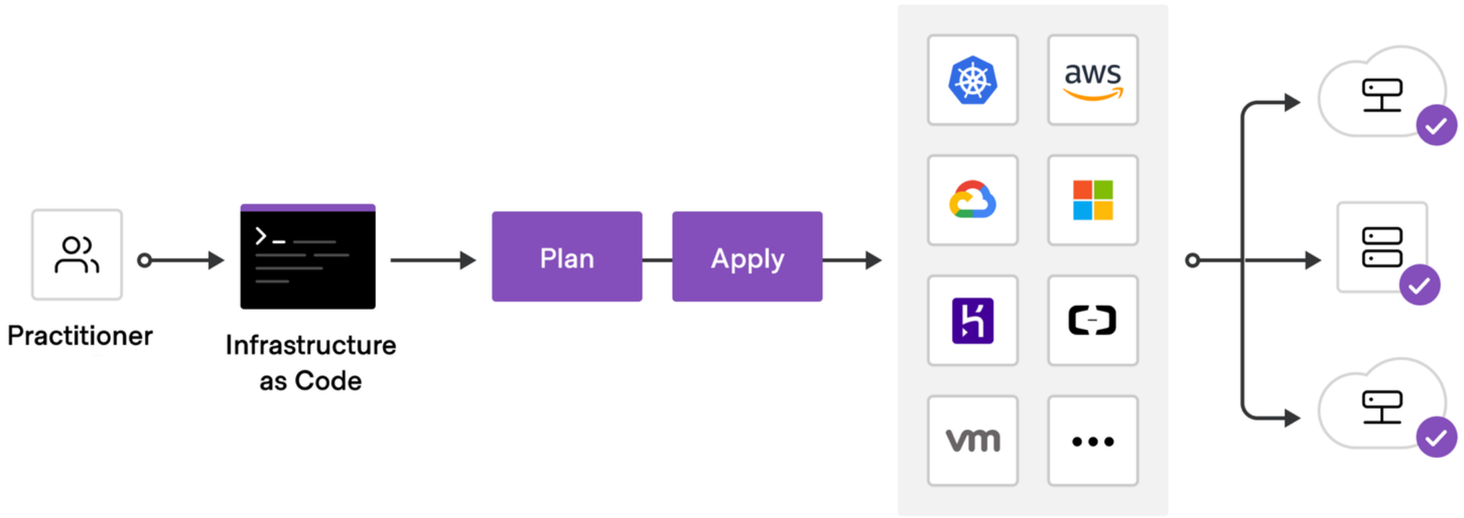
Entorno aislado. No se ponen en riesgo los sistemas en producción ni información sensible.

Se paga tan solo por lo que se usa y durante el tiempo que se usa. Ahorro en infraestructura, costes de operación y mantenimiento.

Escalabilidad (se asignan recursos bajo demanda) y flexibilidad (permite adaptarse a multitud de situaciones)

Terraform

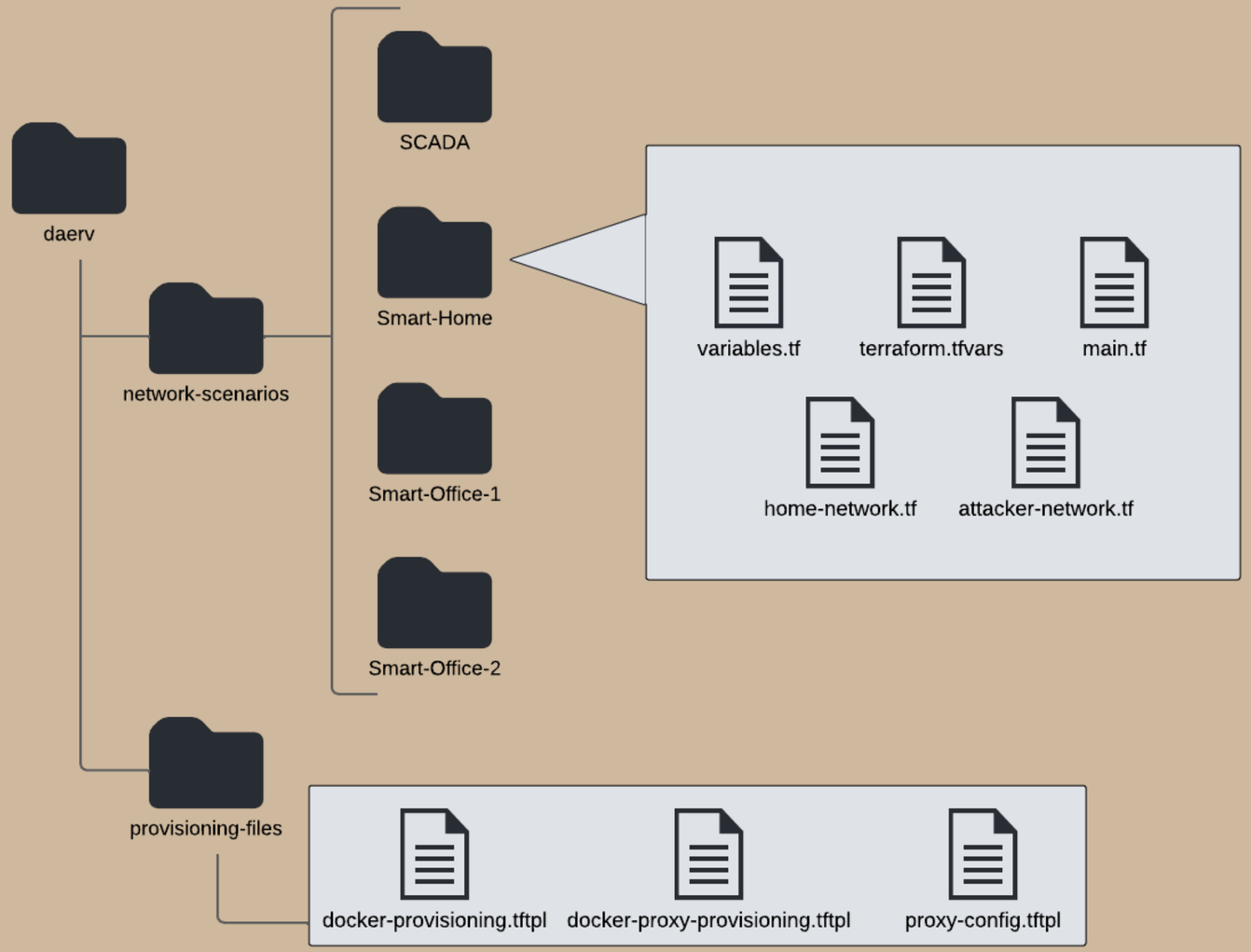
Herramienta IaC open source de codificación declarativa.



- Plataforma agnóstica
- Infraestructura inmutable
- Lenguaje sencillo

Diseño y estructura

https://github.com/samugs13/daerv



Ficheros

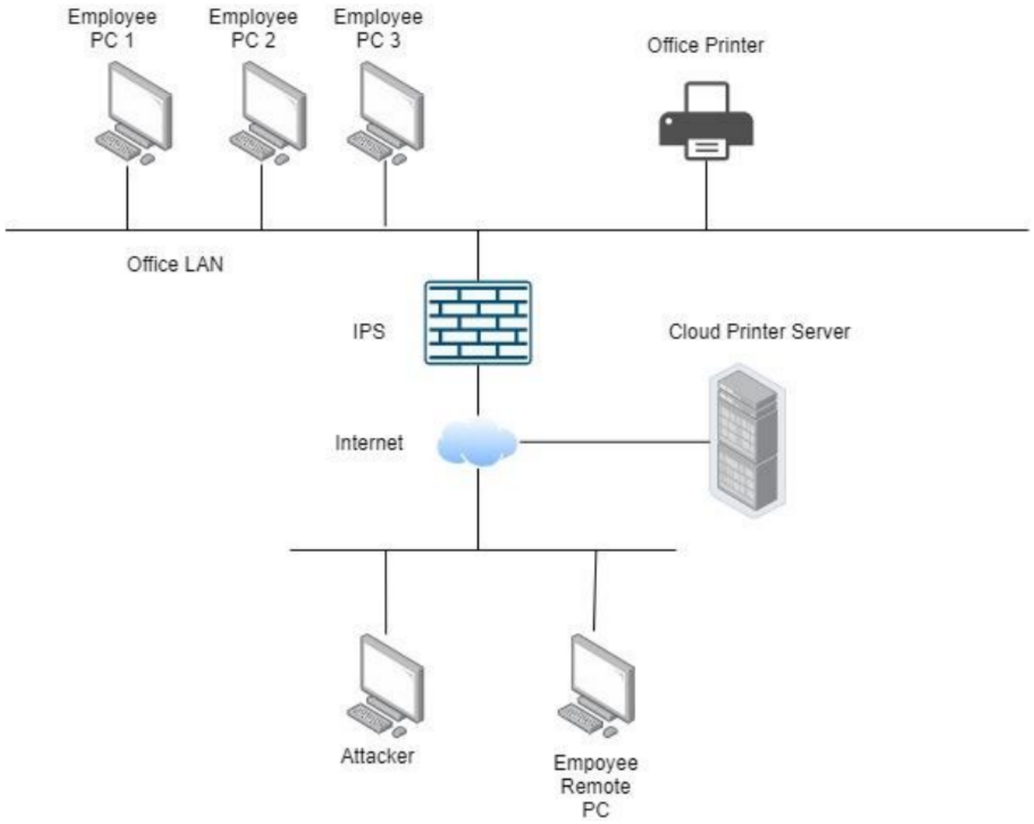
Fichero .tftpl

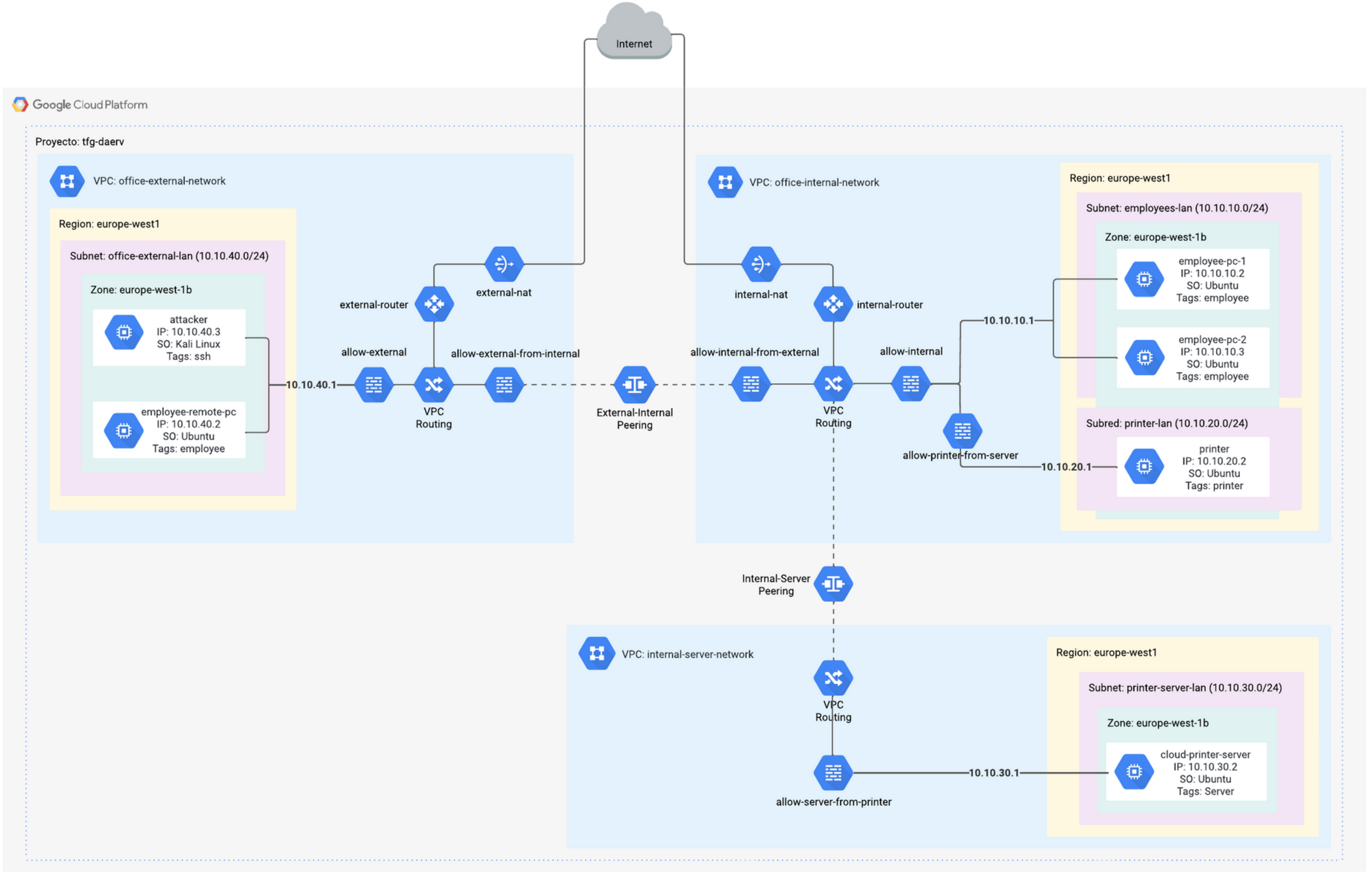
```
54 # Start Docker daemon and run Docker container
55 sudo systemctl start docker
56 sudo docker run ${args} ${image}:${tag}
```

Fichero .tf

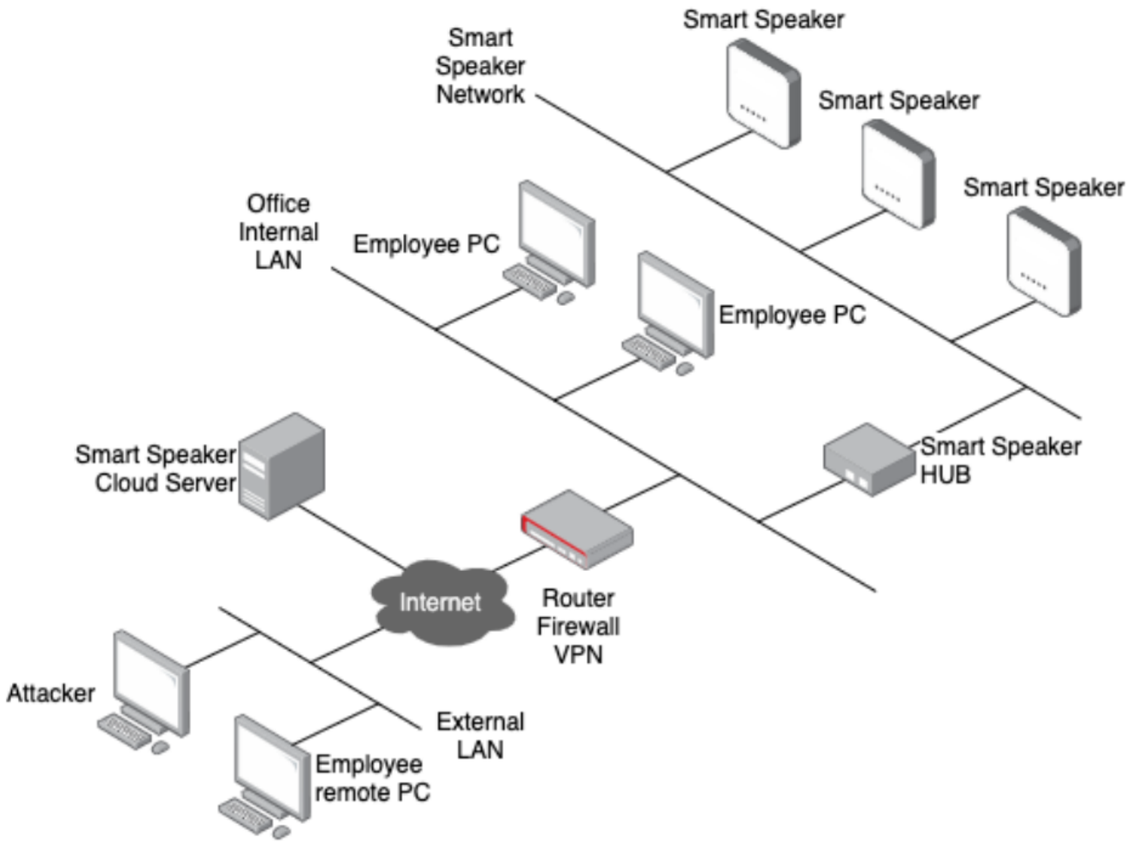
```
60 resource "google_compute_instance" "web_server" {
61   name         = "web-server"
62   machine_type = var.machine_type
63   project      = var.project_id
64   zone         = var.zone
65   tags         = ["web-server"]
66
67   boot_disk {
68     initialize_params {
69       image = var.debian_image
70     }
71   }
72
73   network_interface {
74     subnetwork = google_compute_subnetwork.internet_dmz.self_link
75     access_config {}
76   }
77
78   metadata_startup_script = templatefile(var.docker_provisioning_path, { args = "-p 80:80", image = "nginx", tag = "latest" })
79 }
```

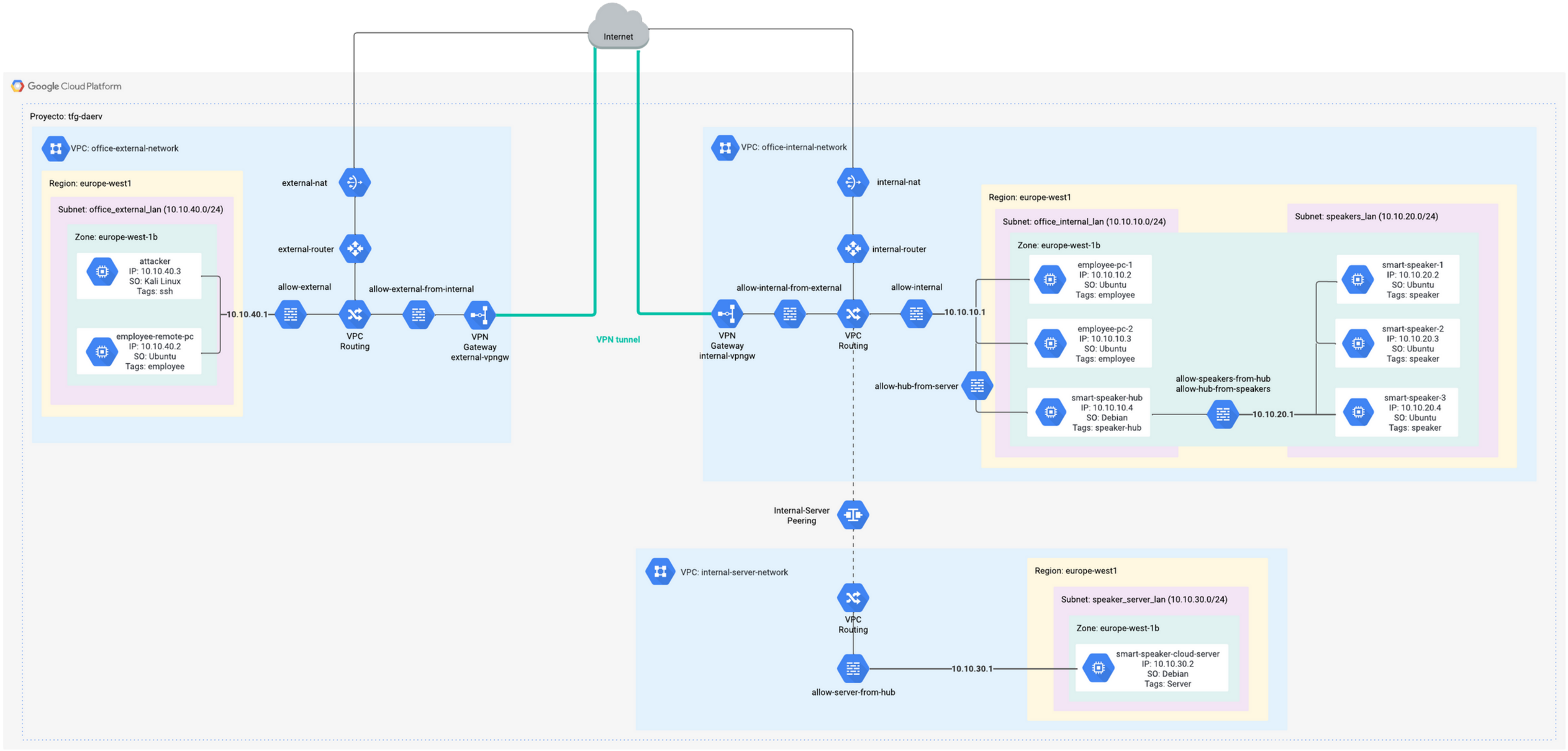
Escenario Smart Office I



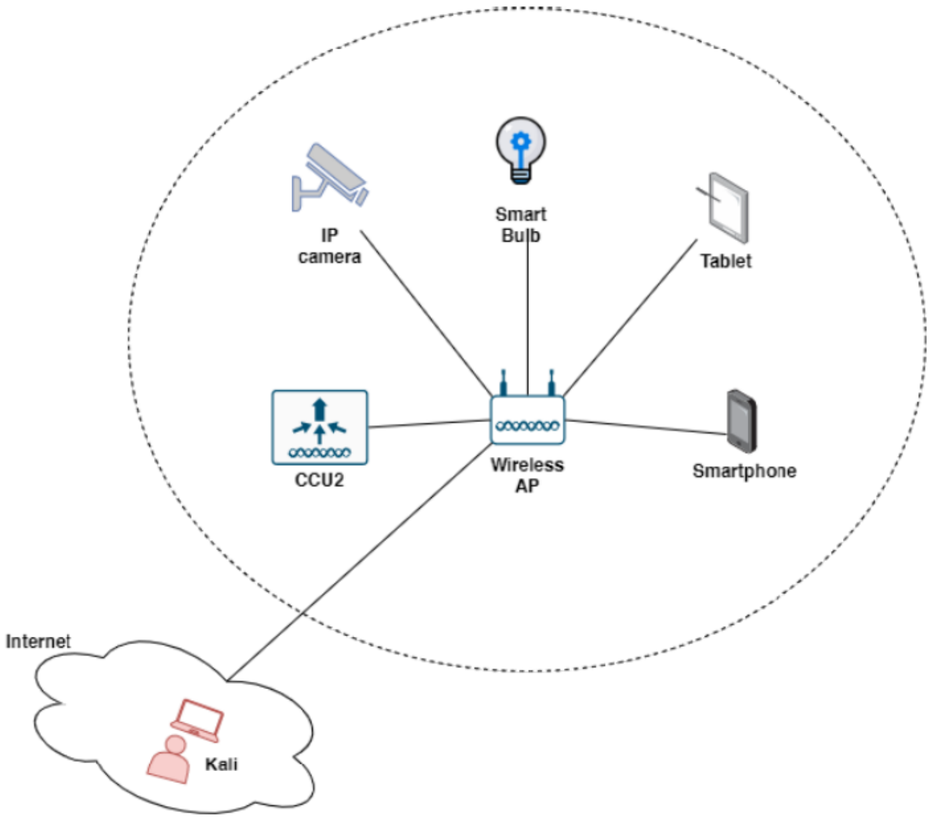

Internet
Google Cloud Platform
Proyecto: tfg-daerv
VPC: office-external-network
Region: europe-west1
Subnet: office-external-lan (10.10.40.0/24)
Zone: europe-west-1b
attacker
IP: 10.10.40.3
SO: Kali Linux
Tags: ssh
employee-remote-pc
IP: 10.10.40.2
SO: Ubuntu
Tags: employee
10.10.40.1
external-router
external-nat
allow-external
allow-external-from-internal
VPC
Routing
External-Internal
Peering
VPC: office-internal-network
internal-nat
internal-router
allow-internal-from-external
allow-internal
VPC
Routing
10.10.10.1
allow-printer-from-server
10.10.20.1
Region: europe-west1
Subnet: employees-lan (10.10.10.0/24)
Zone: europe-west-1b
employee-pc-1
IP: 10.10.10.2
SO: Ubuntu
Tags: employee
employee-pc-2
IP: 10.10.10.3
SO: Ubuntu
Tags: employee
Subred: printer-lan (10.10.20.0/24)
printer
IP: 10.10.20.2
SO: Ubuntu
Tags: printer
Internal-Server
Peering
VPC: internal-server-network
VPC
Routing
allow-server-from-printer
10.10.30.1
Region: europe-west1
Subnet: printer-server-lan (10.10.30.0/24)
Zone: europe-west-1b
cloud-printer-server
IP: 10.10.30.2
SO: Ubuntu
Tags: Server

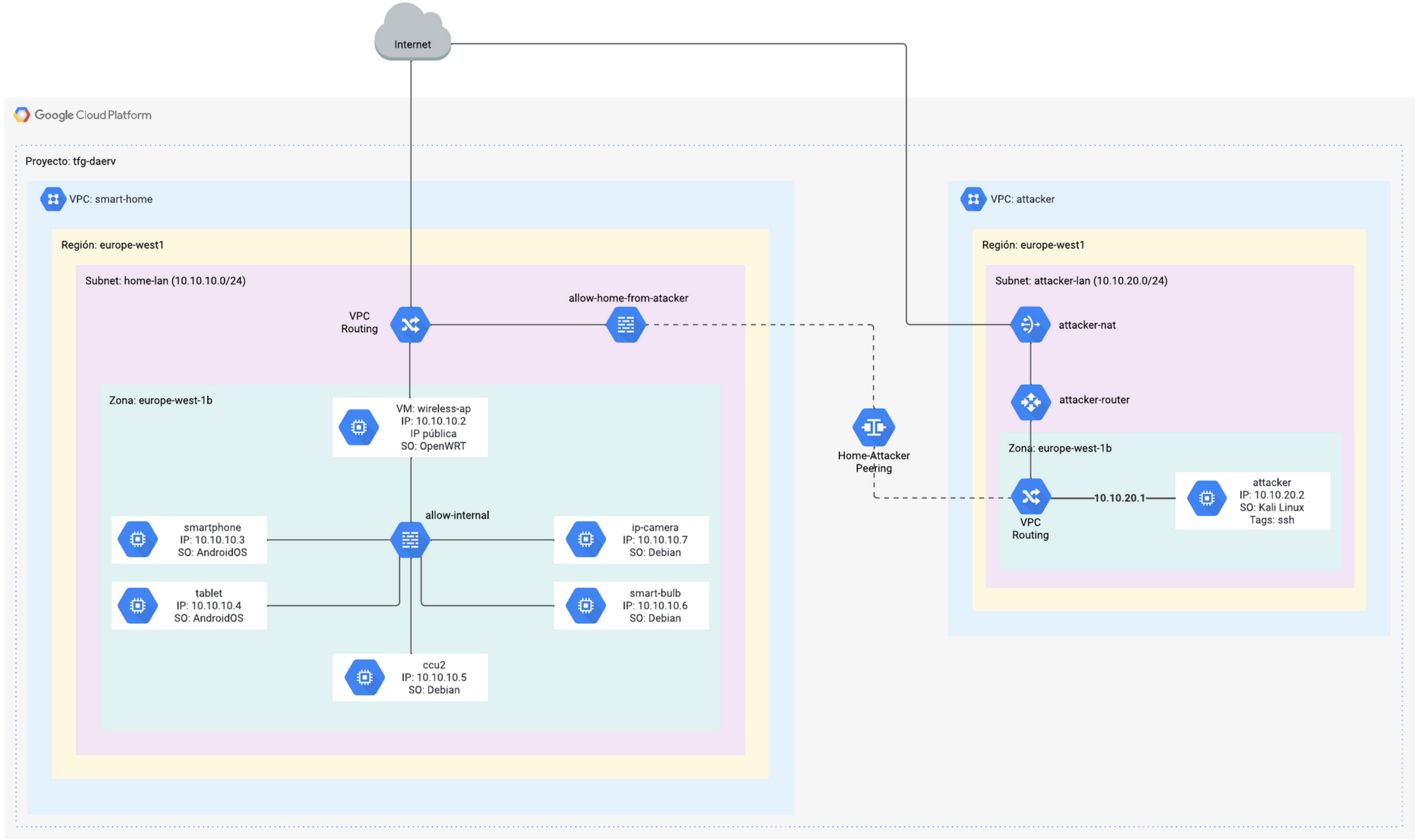
Escenario Smart Office 2




Internet
Google Cloud Platform
Proyecto: tfg-daerv
VPC: office-external-network
Region: europe-west1
Subnet: office_external_lan (10.10.40.0/24)
Zone: europe-west-1b
attacker
IP: 10.10.40.3
SO: Kali Linux
Tags: ssh
employee-remote-pc
IP: 10.10.40.2
SO: Ubuntu
Tags: employee
10.10.40.1
external-nat
external-router
allow-external
allow-external-from-internal
VPC
Routing
VPN
Gateway
external-vpngw
VPN tunnel
VPC: office-internal-network
internal-nat
internal-router
allow-internal-from-external
allow-internal
VPN
Gateway
internal-vpngw
VPC
Routing
10.10.10.1
Region: europe-west1
Subnet: office_internal_lan (10.10.10.0/24)
Zone: europe-west-1b
employee-pc-1
IP: 10.10.10.2
SO: Ubuntu
Tags: employee
employee-pc-2
IP: 10.10.10.3
SO: Ubuntu
Tags: employee
smart-speaker-hub
IP: 10.10.10.4
SO: Debian
Tags: speaker-hub
allow-hub-from-server
Subnet: speakers_lan (10.10.20.0/24)
allow-speakers-from-hub
allow-hub-from-speakers
10.10.20.1
smart-speaker-1
IP: 10.10.20.2
SO: Ubuntu
Tags: speaker
smart-speaker-2
IP: 10.10.20.3
SO: Ubuntu
Tags: speaker
smart-speaker-3
IP: 10.10.20.4
SO: Ubuntu
Tags: speaker
Internal-Server
Peering
VPC: internal-server-network
VPC
Routing
10.10.30.1
allow-server-from-hub
Region: europe-west1
Subnet: speaker_server_lan (10.10.30.0/24)
Zone: europe-west-1b
smart-speaker-cloud-server
IP: 10.10.30.2
SO: Debian
Tags: Server

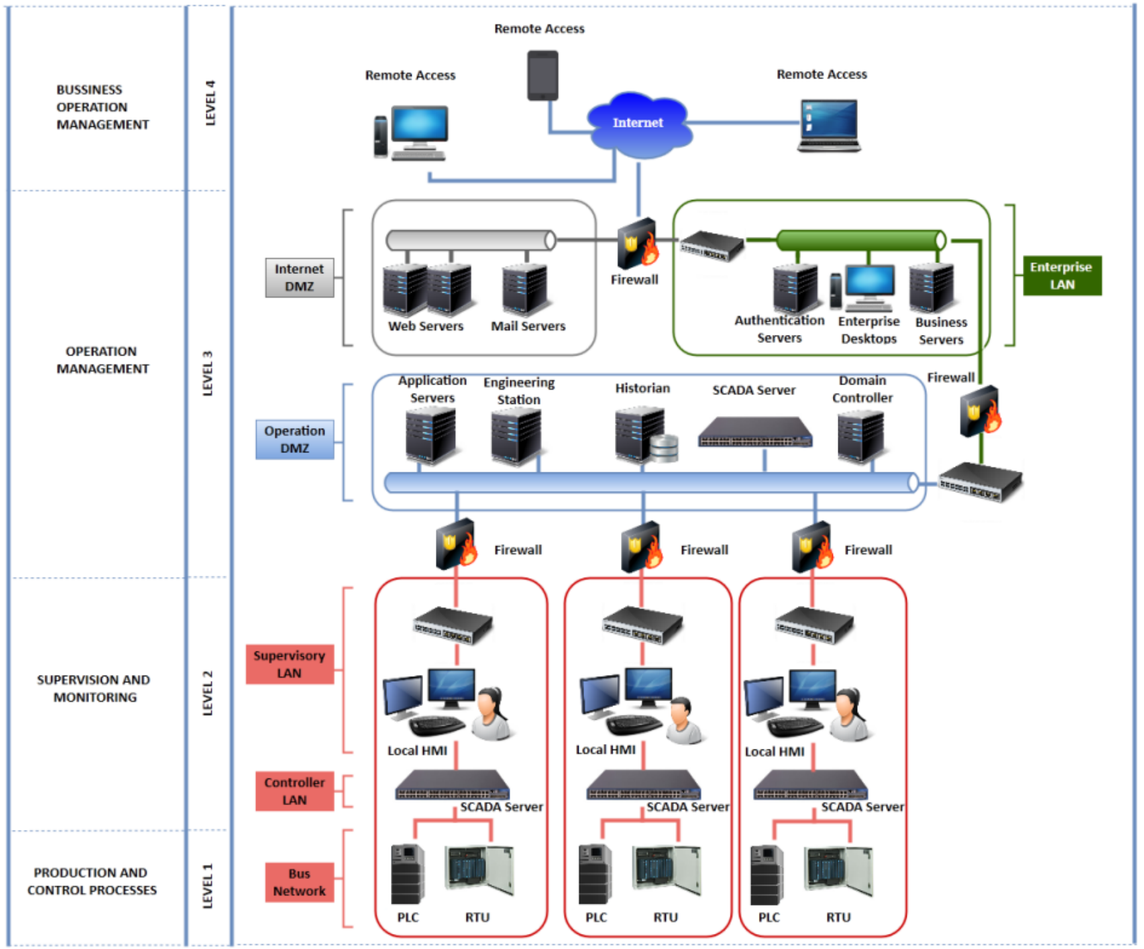
Escenario Smart Home

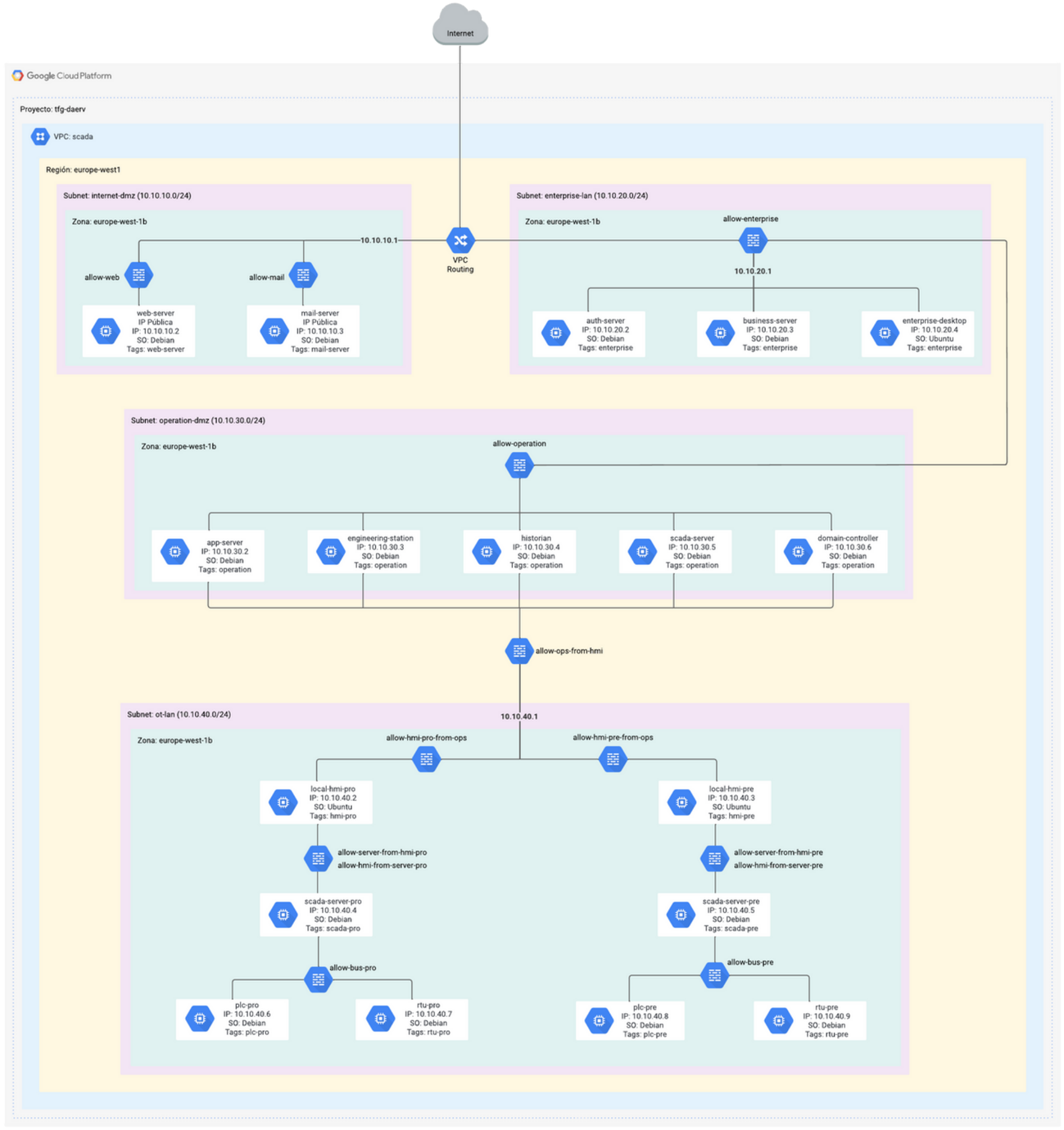



Internet
Google Cloud Platform
Proyecto: tfg-daerv
VPC: smart-home
Región: europe-west1
Subnet: home-lan (10.10.10.0/24)
VPC Routing
allow-home-from-atacker
Zona: europe-west-1b
VM: wireless-ap
IP: 10.10.10.2
IP pública
SO: OpenWRT
allow-internal
smartphone
IP: 10.10.10.3
SO: AndroidOS
ip-camera
IP: 10.10.10.7
SO: Debian
tablet
IP: 10.10.10.4
SO: AndroidOS
smart-bulb
IP: 10.10.10.6
SO: Debian
ccu2
IP: 10.10.10.5
SO: Debian
Home-Attacker Peering
VPC: attacker
Región: europe-west1
Subnet: attacker-lan (10.10.20.0/24)
attacker-nat
attacker-router
Zona: europe-west-1b
VPC Routing
10.10.20.1
attacker
IP: 10.10.20.2
SO: Kali Linux
Tags: ssh

Escenario SCADA

Figure 2: ISA95 levels applied to a SCADA architecture.




Internet
Google Cloud Platform
Proyecto: tfg-daerv
VPC: scada
Región: europe-west1
Subnet: internet-dmz (10.10.10.0/24)
Zona: europe-west-1b
10.10.10.1
VPC Routing
allow-web
allow-mail
web-server
IP Pública
IP: 10.10.10.2
SO: Debian
Tags: web-server
mail-server
IP Pública
IP: 10.10.10.3
SO: Debian
Tags: mail-server
Subnet: enterprise-lan (10.10.20.0/24)
Zona: europe-west-1b
allow-enterprise
10.10.20.1
auth-server
IP: 10.10.20.2
SO: Debian
Tags: enterprise
business-server
IP: 10.10.20.3
SO: Debian
Tags: enterprise
enterprise-desktop
IP: 10.10.20.4
SO: Ubuntu
Tags: enterprise
Subnet: operation-dmz (10.10.30.0/24)
Zona: europe-west-1b
allow-operation
app-server
IP: 10.10.30.2
SO: Debian
Tags: operation
engineering-station
IP: 10.10.30.3
SO: Debian
Tags: operation
historian
IP: 10.10.30.4
SO: Debian
Tags: operation
scada-server
IP: 10.10.30.5
SO: Debian
Tags: operation
domain-controller
IP: 10.10.30.6
SO: Debian
Tags: operation
allow-ops-from-hmi
Subnet: ot-lan (10.10.40.0/24)
10.10.40.1
Zona: europe-west-1b
allow-hmi-pro-from-ops
allow-hmi-pre-from-ops
local-hmi-pro
IP: 10.10.40.2
SO: Ubuntu
Tags: hmi-pro
local-hmi-pre
IP: 10.10.40.3
SO: Ubuntu
Tags: hmi-pre
allow-server-from-hmi-pro
allow-hmi-from-server-pro
allow-server-from-hmi-pre
allow-hmi-from-server-pre
scada-server-pro
IP: 10.10.40.4
SO: Debian
Tags: scada-pro
scada-server-pre
IP: 10.10.40.5
SO: Debian
Tags: scada-pre
allow-bus-pro
allow-bus-pre
plc-pro
IP: 10.10.40.6
SO: Debian
Tags: plc-pro
rtu-pro
IP: 10.10.40.7
SO: Debian
Tags: rtu-pro
plc-pre
IP: 10.10.40.8
SO: Debian
Tags: plc-pre
rtu-pre
IP: 10.10.40.9
SO: Debian
Tags: rtu-pre

Despliegue

```
.../daerv/network-scenarios/Smart-Office-1 ❱❱❱ terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of hashicorp/google from the dependency lock file
- Using previously-installed hashicorp/google v4.20.0

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.
```

```
.../daerv/network-scenarios/Smart-Office-1 ❱❱❱ terraform apply

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_external will be created
  + resource "google_compute_firewall" "allow_external" {
      + creation_timestamp = (known after apply)
      + destination_ranges = (known after apply)
      + direction          = "INGRESS"
      + enable_logging     = (known after apply)
      + id                 = (known after apply)
      + name               = "allow-external"
      + network            = (known after apply)
```

```
Plan: 31 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_network.office_external_network: Creating...
google_compute_network.office_internal_network: Creating...
google_compute_network.internal_server_network: Creating...
```

Despliegue II

```
google_compute_firewall.allow_server_from_printer: Still creating... [20s el
google_compute_firewall.allow_internal_from_external: Creation complete afte
google_compute_firewall.allow_server_from_printer: Creation complete after 2

Apply complete! Resources: 31 added, 0 changed, 0 destroyed.
.../daerv/network-scenarios/Smart-Office-1 ❱❱❱ terraform state list
google_compute_firewall.allow_external
google_compute_firewall.allow_external_from_internal
google_compute_firewall.allow_internal
google_compute_firewall.allow_internal_from_external
google_compute_firewall.allow_printer_from_server
google_compute_firewall.allow_server_from_printer
google_compute_firewall.allow_ssh_external
google_compute_firewall.allow_ssh_internal
google_compute_firewall.allow_ssh_server
google_compute_instance.attacker
google_compute_instance.cloud_printer_server
google_compute_instance.employee_pc_1
google_compute_instance.employee_pc_2
google_compute_instance.employee_pc_3
google_compute_instance.employee_remote_pc
google_compute_instance.office_printer
google_compute_network.internal_server_network
google_compute_network.office_external_network
google_compute_network.office_internal_network
google_compute_network_peering.peer_external_to_internal
google_compute_network_peering.peer_internal_office_to_server
google_compute_network_peering.peer_internal_server_to_office
google_compute_network_peering.peer_internal_to_external
google_compute_router.office_external_router
google_compute_router.office_internal_router
google_compute_router_nat.office_external_nat
google_compute_router_nat.office_internal_nat
google_compute_subnetwork.employees_lan
google_compute_subnetwork.office_external_lan
google_compute_subnetwork.printer_lan
google_compute_subnetwork.printer_server_lan
.../daerv/network-scenarios/Smart-Office-1 ❱❱❱
```

Status	Name ↑	Zone	Recommendations	In use by	Internal IP
✓	attacker	europe-west1-b			10.10.40.2 (nic0)
✓	cloud-printer-server	europe-west1-b			10.10.30.2 (nic0)
✓	employee-pc-1	europe-west1-b			10.10.10.4 (nic0)
✓	employee-pc-2	europe-west1-b			10.10.10.2 (nic0)
✓	employee-pc-3	europe-west1-b			10.10.10.3 (nic0)
✓	employee-remote-pc	europe-west1-b			10.10.40.3 (nic0)
✓	office-printer	europe-west1-b			10.10.20.2 (nic0)

Conectividad

Name	Protocol	Source	Destination	Destination port	Last test time	Last packet transmission result
attacker-to-internal	tcp	attacker	office-printer	80	2022-06-16 (18:48:24)	0/50 packets delivered
external-to-server	tcp	attacker	cloud-printer-server	80	2022-06-16 (18:53:04)	0/50 packets delivered
internal-to-attacker	tcp	employee-pc-1	attacker	80	2022-06-16 (18:48:48)	0/50 packets delivered
internal-to-remote-employee	tcp	employee-pc-2	employee-remote-pc	80	2022-06-16 (18:48:01)	50/50 packets delivered
internal-to-server	tcp	employee-pc-2	cloud-printer-server	80	2022-06-16 (18:49:29)	0/50 packets delivered
printer-to-server	tcp	office-printer	cloud-printer-server	80	2022-06-16 (18:46:09)	50/50 packets delivered
remote-employee-to-internal	tcp	employee-remote-pc	employee-pc-1	80	2022-06-16 (18:47:25)	50/50 packets delivered
server-to-internal	tcp	cloud-printer-server	employee-pc-1	80	2022-06-16 (18:49:51)	0/50 packets delivered
server-to-printer	tcp	cloud-printer-server	office-printer	80	2022-06-16 (18:46:43)	50/50 packets delivered

Conectividad II

Connectivity test result

Test name
internal-to-remote-employee

Protocol
tcp

Source
employee-pc-2

Source project
tfg-daerv

Destination
employee-remote-pc

Destination project
tfg-daerv

Destination port
80

Result

Configuration analysis trace path

- VM instance (employee-pc-2)
- Default egress firewall rule
- Peering subnet route
- VM instance (employee-remote-pc)
- Ingress firewall rule
  - Name: allow-external-from-internal
  - Network: office-external-network
  - Action: ALLOW
  - Priority: 1000
- Packet could be delivered
  - Configuration analysis determines that the packet could be delivered to VM instance (employee-remote-pc)

Connectivity test result

Test name
attacker-to-internal

Protocol
tcp

Source
attacker

Source project
tfg-daerv

Destination
office-printer

Destination project
tfg-daerv

Destination port
80

Result

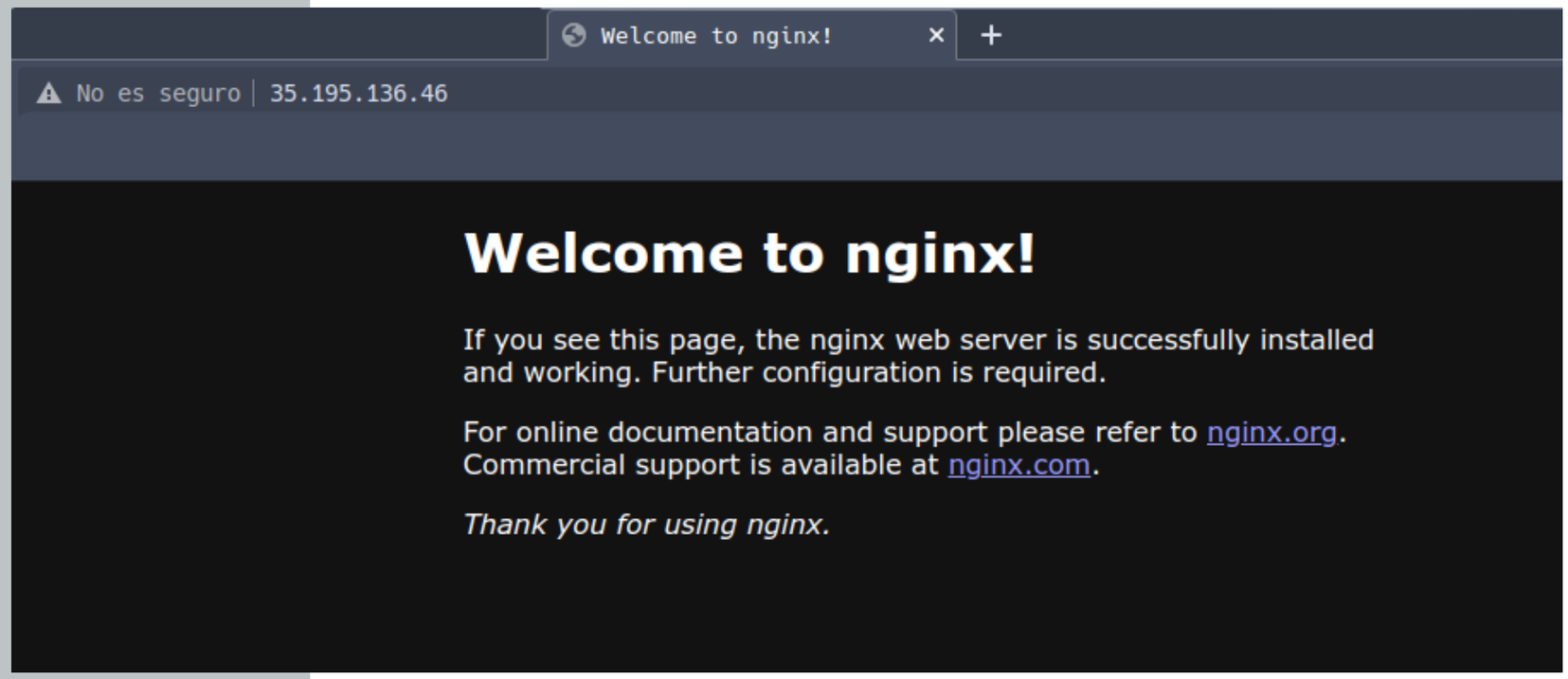
Configuration analysis trace path

- VM instance (attacker)
- Default egress firewall rule
- Peering subnet route
- VM instance (office-printer)
- Default ingress firewall rule
- Packet could be dropped
  - Configuration analysis determines that the packet could be dropped due to a firewall rule unless allowed due to connection tracking
  - Learn how to fix the issue

Software

```
garciasanchezsamu@ccu2:~$ which docker
/usr/bin/docker
garciasanchezsamu@ccu2:~$ curl -x http://10.10.10.6:3128 -L http://ip.me
34.140.221.213
garciasanchezsamu@ccu2:~$
```

proxy-config.tftpl
docker-proxy-provisioning.tftpl



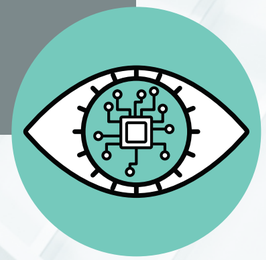
docker-provisioning.tftpl

Conclusiones

- Ahorro en infraestructura y mantenimiento
- Escalabilidad y flexibilidad en la configuración de los escenarios
- Despliegue rápido, seguro y parametrizable
- Portabilidad entre proveedores cloud

Líneas futuras

- Configuración software de los escenarios
- Capacidad multinube



Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network
allow-external-from-internal	Ingress	employee	IP ranges: 10.10.20.0/24, 10.10.10.0/24	tcp:0-65535 udp:0-65535 icmp	Allow	1000	office-external-network
allow-external	Ingress	Apply to all	IP ranges: 10.10.40.0/24	tcp:0-65535 udp:0-65535 icmp	Allow	65534	office-external-network
allow-internal-from-external	Ingress	employee, printer	IP ranges: 10.10.40.2	tcp:0-65535 udp:0-65535 icmp	Allow	1000	office-internal-network
allow-printer-from-server	Ingress	printer	IP ranges: 10.10.30.0/24	tcp:0-65535 udp:0-65535 icmp	Allow	1000	office-internal-network
allow-internal	Ingress	Apply to all	IP ranges: 10.10.20.0/24, 10.10.10.0/24	tcp:0-65535 udp:0-65535 icmp	Allow	65534	office-internal-network
allow-server-from-printer	Ingress	server	IP ranges: 10.10.20.0/24	tcp:0-65535 udp:0-65535 icmp	Allow	1000	server-network

Reglas de firewalll

Name	Region	Subnets	MTU	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Firewall Rules
default		35	1460	Auto	None				0
office-external-network		1	1460	Custom	None				3
	europe-west1	office-external-lan			10.10.40.0/24	None	None	10.10.40.1	
office-internal-network		2	1460	Custom	None				4
	europe-west1	employees-lan			10.10.10.0/24	None	None	10.10.10.1	
	europe-west1	printer-lan			10.10.20.0/24	None	None	10.10.20.1	
server-network		1	1460	Custom	None				2
	europe-west1	printer-server-lan			10.10.30.0/24	None	None	10.10.30.1	

VPC

Subproceso	Horas
Estudio de las diferentes tecnologías (Terraform, Google Cloud)	90
Análisis de los escenarios (vector de ataque y conexiones necesarias entre los elementos)	40
Diseño e implementación de los escenarios en Google Cloud	130
Desarrollo de herramientas de configuración	30
Pruebas	40
Elaboración de la memoria	75
Total	**405**

Tabla B.1: Horas asociadas a cada una de los subprocesos de realización del proyecto

Costes totales

Concepto		Coste
Costes directos	Mano de obra	4.969,35€
	Material	206,77€
	Total	**5.176,12€**
Costes indirectos		1.035,22€
Total antes de beneficios e impuestos		6.211,34€
Beneficio industrial (10 %)		621,13€
Total antes de impuestos		6.832,48€
IVA (21 %)		1.434,82€
Total		**8.267,30€**

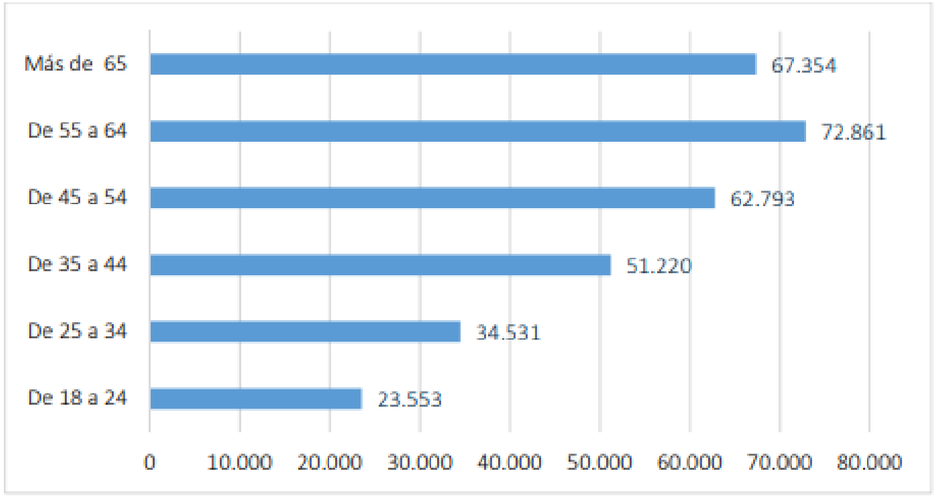
Tabla B.5: Costes totales

Costes de mano de obra

Horas	€/Hora	Total
405	12.27	**4.969,35€**

Tabla B.2: Costes de mano de obra

Salario medio segmentado por edad



Base: Total muestra (n=2040)

Fuente: Mapa socio-profesional del titulado en Ingeniería de Telecomunicación (Colegio Oficial de Ingenieros de Telecomunicación).