



Instituto Politécnico Nacional

ESCUELA SUPERIOR DE CÓMPUTO

CLASE 26 - VPC Y REGLAS DE FIREWALL

Sistemas Distribuidos
Ukranio Coronilla Contreras

Luciano Hernández Jonathan

7CM3

Abril 29, 2025

1 Ejercicio1

Tome un rango IPv4 de una de las subredes que aparecen en su lista y calcule el rango.

En este caso elegí la siguiente subred:

<input checked="" type="checkbox"/>	default	asia-east1	default	IPv4	10.140.0.0/20
-------------------------------------	-------------------------	------------	-------------------------	------	---------------

Figure 1: Subred VPC seleccionada

Datos de la dirección IP

- Dirección IP base: 10.140.0.0
- Máscara: /20

Resta de máscaras

$$\text{Bits disponibles} = 32 (\text{total}) - 20 (\text{máscara}) = 12 \text{ bits}$$

Cantidad de direcciones disponibles

$$2^{12} = 4096 \text{ direcciones}$$

Conversión a binario y llenado de bits

IP base (binario) = 00001010.10001100.00000000.00000000

Máscara /20 = 11111111.11111111.11110000.00000000

Bits de host = $\underbrace{0000}_{4 \text{ bits fijos}} \underbrace{00000000.00000000}_{12 \text{ bits variables}}$

Límites de la subred en binario

Primera dirección (red) = 00001010.10001100.00000000.00000000

Última dirección (broadcast) = 00001010.10001100.00001111.11111111

Conversión a decimal

Primera IP (10.140.0.0) = Red (no usable)

Primera usable = 10.140.0.1

Última usable = 10.140.15.254

Broadcast = 10.140.15.255 (no usable)

Rango de direcciones utilizables

10.140.0.1 – 10.140.15.254

2 Ejercicio 2

2.1 Creación de instancias.

Creamos las instancias en subredes diferentes usando el shell de google cloud como se muestra acontinuación.

```
IPV6_ACCESS_TYPE:  
INTERNAL_IPV6_PREFIX:  
EXTERNAL_IPV6_PREFIX:  
luher_jonathan@cloudshell:~ (molten-acumen-458316-r4)$ gcloud compute instances create instance-asia1 \  
--zone=asia-east1-a \  
--machine-type=f1-micro \  
--subnet=default \  
--image-family=debian-11 \  
--image-project=debian-cloud \  
--tags=test-fw-rule  
Created [https://www.googleapis.com/compute/v1/projects/molten-acumen-458316-r4/zones/asia-east1-a/instances/instance-asia1].  
NAME: instance-asia1  
ZONE: asia-east1-a  
MACHINE_TYPE: f1-micro  
PREEMPTIBLE:  
INTERNAL_IP: 10.140.0.2  
EXTERNAL_IP: 35.236.157.155  
STATUS: RUNNING
```

Figure 2: Instancia 1

```
luher_jonathan@cloudshell:~ (molten-acumen-458316-r4)$ gcloud compute instances create instance-asia2 --zone=asia-east2-b --machine-type=f1-micro --subnet=default  
--image-family=debian-11 --image-project=debian-cloud --tags=test-fw-rule  
Created [https://www.googleapis.com/compute/v1/projects/molten-acumen-458316-r4/zones/asia-east2-b/instances/instance-asia2].  
NAME: instance-asia2  
ZONE: asia-east2-b  
MACHINE_TYPE: f1-micro  
PREEMPTIBLE:  
INTERNAL_IP: 10.170.0.2
```

Figure 3: Instancia 2

2.2 Pruebas de las 6 reglas de firewall.

A continuación se explican las pruebas realizadas para comprobar cada una de las 6 reglas de firewall que tienen por default las instancias de la subred de VPC.

2.2.1 Regla de firewall para ICMP (ping)

En esta primera prueba se realiza ping a cada una de las instancias, y se tiene como respuesta el número de bytes desde la dirección IP de la instancia, indicándonos que el tráfico ICMP está permitido.

The screenshot shows a Google Cloud Shell terminal window with the following output:

```
chinese55@chinese55-ThinkPad-T440:~$ ping -i[[200-35.236.157.155-  
ping: 35.236.157.155: Name or service not known  
chinese55@chinese55-ThinkPad-T440:~$ ping 35.236.157.155  
PING 35.236.157.155 (35.236.157.155) 56(84) bytes of data:  
64 bytes from 35.236.157.155: icmp_seq=1 ttl=57 time=226 ms  
64 bytes from 35.236.157.155: icmp_seq=2 ttl=57 time=249 ms  
64 bytes from 35.236.157.155: icmp_seq=3 ttl=57 time=275 ms  
64 bytes from 35.236.157.155: icmp_seq=4 ttl=57 time=192 ms  
64 bytes from 35.236.157.155: icmp_seq=5 ttl=57 time=218 ms  
64 bytes from 35.236.157.155: icmp_seq=6 ttl=57 time=344 ms  
64 bytes from 35.236.157.155: icmp_seq=7 ttl=57 time=176 ms  
64 bytes from 35.236.157.155: icmp_seq=8 ttl=57 time=287 ms  
64 bytes from 35.236.157.155: icmp_seq=9 ttl=57 time=176 ms  
64 bytes from 35.236.157.155: icmp_seq=10 ttl=57 time=232 ms  
64 bytes from 35.236.157.155: icmp_seq=11 ttl=57 time=256 ms  
64 bytes from 35.236.157.155: icmp_seq=12 ttl=57 time=177 ms  
64 bytes from 35.236.157.155: icmp_seq=13 ttl=57 time=303 ms  
64 bytes from 35.236.157.155: icmp_seq=14 ttl=57 time=176 ms  
64 bytes from 35.236.157.155: icmp_seq=15 ttl=57 time=356 ms  
64 bytes from 35.236.157.155: icmp_seq=16 ttl=57 time=271 ms  
64 bytes from 35.236.157.155: icmp_seq=17 ttl=57 time=192 ms  
64 bytes from 35.236.157.155: icmp_seq=18 ttl=57 time=216 ms  
64 bytes from 35.236.157.155: icmp_seq=19 ttl=57 time=240 ms  
64 bytes from 35.236.157.155: icmp_seq=20 ttl=57 time=264 ms  
^C  
(gcloud) The project property must be set to a valid project ID, [[PROJECT_ID]] is not a valid project ID.  
Set your project, run:  
gcloud config set project PROJECT_ID  
To unset it, run:  
gcloud config unset project  
luher_jonathan@cloudshell:~ (molten-acumen-458316-r4)$
```

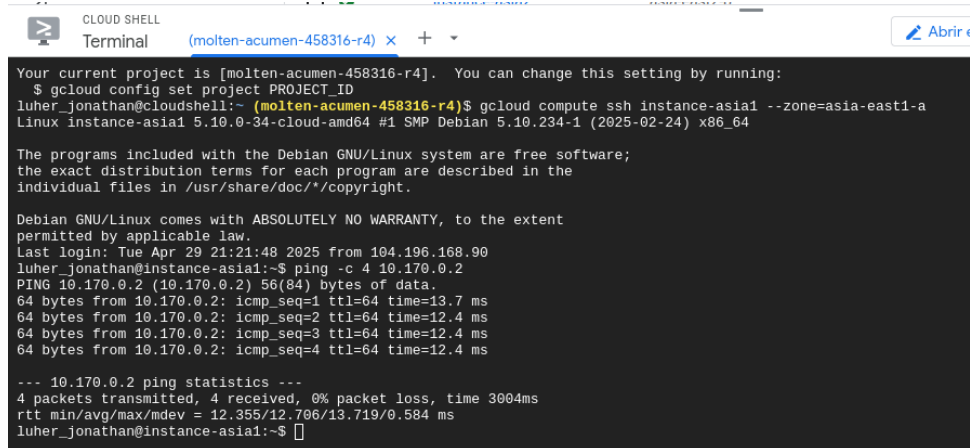
On the right, a side window displays the 'En uso por' (In use by) table for the firewall rules:

En uso por	IP interna	IP externa	Conectar
	10.140.0.2 (nic0)	35.236.157.155 (nic0)	SSH
	10.170.0.2 (nic0)	34.150.67.36 (nic0)	SSH

Figure 4: Trafico ICMP

2.2.2 Trafico Interno

Esta prueba valida que el tráfico entre instancias dentro de la misma red VPC esté permitido, asegurando que servicios internos puedan interactuar sin restricciones. Se verifica haciendo ping o conectándose via SSH entre las IPs internas de las instancias, lo que demuestra que la comunicación intranet funciona según lo configurado.



```
CLOUD SHELL
Terminal (molten-acumen-458316-r4) x + v
Your current project is [molten-acumen-458316-r4]. You can change this setting by running:
$ gcloud config set project PROJECT_ID
luher_jonathan@cloudshell:~ (molten-acumen-458316-r4)$ gcloud compute ssh instance-asial --zone=asia-east1-a
Linux instance-asial 5.10.0-34-cloud-amd64 #1 SMP Debian 5.10.234-1 (2025-02-24) x86_64

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

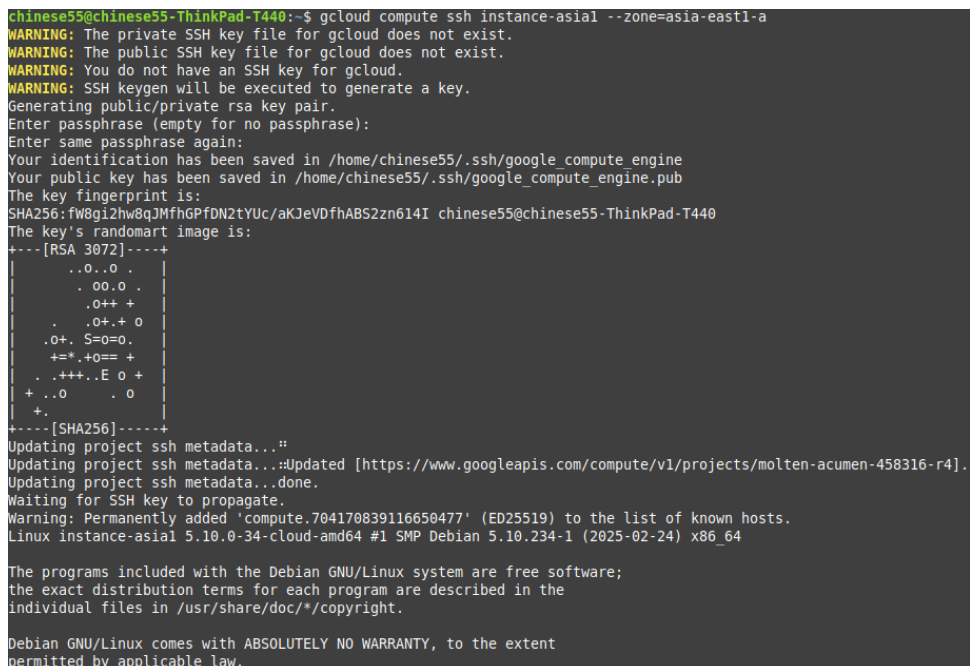
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr 29 21:21:48 2025 from 104.196.168.90
luher_jonathan@instance-asial:~$ ping -c 4 10.170.0.2
PING 10.170.0.2 (10.170.0.2) 56(84) bytes of data:
64 bytes from 10.170.0.2: icmp_seq=1 ttl=64 time=13.7 ms
64 bytes from 10.170.0.2: icmp_seq=2 ttl=64 time=12.4 ms
64 bytes from 10.170.0.2: icmp_seq=3 ttl=64 time=12.4 ms
64 bytes from 10.170.0.2: icmp_seq=4 ttl=64 time=12.4 ms

--- 10.170.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 12.355/12.706/13.719/0.584 ms
luher_jonathan@instance-asial:~$
```

Figure 5: Trafico interno

2.3 Acceso SSH (default-allow-ssh)

El propósito es confirmar que el protocolo SSH (puerto 22) está accesible para administración remota desde cualquier IP. La prueba consiste en intentar una conexión SSH desde una terminal externa usando gcloud o herramientas como OpenSSH, verificando que el acceso sea exitoso sin bloqueos del firewall. Como se muestra a continuación se logró un acceso exitoso desde mi terminal local en Linux.



```
chinese55@chinese55-ThinkPad-T440:~$ gcloud compute ssh instance-asial --zone=asia-east1-a
WARNING: The private SSH key file for gcloud does not exist.
WARNING: The public SSH key file for gcloud does not exist.
WARNING: You do not have an SSH key for gcloud.
WARNING: SSH keygen will be executed to generate a key.
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/chinese55/.ssh/google_compute_engine
Your public key has been saved in /home/chinese55/.ssh/google_compute_engine.pub
The key fingerprint is:
SHA256:fw8gi2hw8qJmFhGPfDN2tYUc/aKJeVdfhABS2zn614I chinese55@chinese55-ThinkPad-T440
The key's randomart image is:
+----[RSA 3072]-----+
| ..0..0 |
| .00..0 |
| .0++ + |
| .0+.+ 0 |
| .0+. S=0=0. |
| +=*+.0=+ + |
| .+++..E 0 + |
| + ..0 . 0 |
| +. |
+----[SHA256]-----+
Updating project ssh metadata...:
Updating project ssh metadata...:Updated [https://www.googleapis.com/compute/v1/projects/molten-acumen-458316-r4].
Updating project ssh metadata...done.
Waiting for SSH key to propagate.
Warning: Permanently added 'compute.704170839116650477' (ED25519) to the list of known hosts.
Linux instance-asial 5.10.0-34-cloud-amd64 #1 SMP Debian 5.10.234-1 (2025-02-24) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Figure 6: Acceso SSH

2.3.1 default-allow-rdp (RDP para Windows)

Diseñada para validar que el protocolo RDP (puerto 3389) esté habilitado para conexiones a instancias Windows. Aunque la prueba se ejecuta en instancias Linux (que no usan RDP), intentar una conexión revela si el firewall está aplicando correctamente la regla default-allow-rdp.

```
chinese55@instance-asia1:~$ nc -zv 35.236.157.155 3389
nc: connect to 35.236.157.155 port 3389 (tcp) failed: Connection refused
chinese55@instance-asia1:~$ nc -zv 35.236.157.155 22
Connection to 35.236.157.155 port [tcp/ssh] succeeded!
```

Figure 7: Caption

Con lo anterior se concluye lo siguiente:

- La regla default-allow-rdp está habilitada (el tráfico llega a la instancia).
- No hay servicio RDP ejecutándose (por eso el "rechazo").
- Si se hubiera obtenido Connection timed out, significaría que el firewall está bloqueando el puerto.

2.3.2 default-deny-ingress (Bloqueo externo)

Esta prueba demuestra que el firewall bloquea todo tráfico entrante no explícitamente permitido por otras reglas. La configuración default-deny-ingress actúa como última barrera de seguridad. Para verificarlo, se intenta acceder a puertos no autorizados (ej: 80 para HTTP) usando herramientas como netcat (nc), esperando un timeout o rechazo activo como respuesta. EN este caso se realizo un escaneo con nmap al puerto 80.

```
chinese55@chinese55-ThinkPad-T440:~$ nmap -Pn -p 80 34.150.67.36
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-29 23:54 CST
Nmap scan report for 36.67.150.34.bc.googleusercontent.com (34.150.67.36)
Host is up.

PORT      STATE      SERVICE
80/tcp    filtered  http

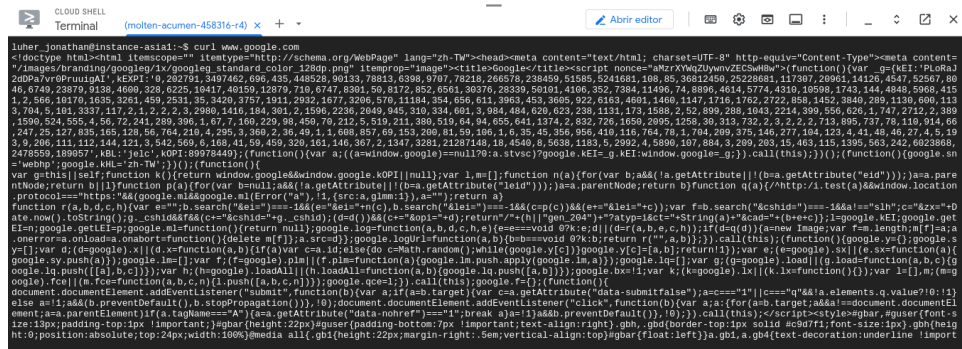
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
chinese55@chinese55-ThinkPad-T440:~$ ^C
```

Figure 8: Bloqueo externo

El resultado filtered en Nmap indica que el firewall de Google Cloud está bloqueando activamente el tráfico al puerto 80 (HTTP), lo que confirma que la regla default-deny-ingress funciona correctamente. Esto significa que, aunque la instancia está activa (Host is up), cualquier intento de conexión externa a puertos no permitidos (como el 80) es descartado silenciosamente por el firewall. El estado filtered diferencia este bloqueo de un puerto simplemente cerrado (closed), donde el tráfico sí llega a la instancia pero no hay servicio escuchando.

2.3.3 Restricción de tráfico saliente (default-deny-egress)

Confirma que las instancias no pueden iniciar conexiones salientes no autorizadas. La regla default-deny-egress complementa la seguridad impidiendo exfiltración de datos o conexiones maliciosas. La prueba consiste en intentar acceder a recursos externos (ej: google.com) desde la instancia via curl o ping, verificando que falle debido a la política de bloqueo predeterminada.



```
luser_jonathan@instance-aa1ai:~$ curl www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="zh-TW"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="
/images/branding/google/1x/google_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="a2rYwQ2UywnvZECsWdW">(function(){var g={kEI:"PL0rA2
209PwVwBrungAt_kE0P1_0_202784_301462_606_435_448528_30133_78833_6388_9707_70210_206578_238459_51585_554184_186_85_30812450_2522864_117307_20601_4122_4047_52557_80
46_6749_23870_9138_4660_328_6225_19417_40159_12879_710_6747_8301_50_8172_852_0561_30376_28339_50101_4106_352_7384_11496_74_8896_4614_5774_4310_10598_1743_144_4848_5968_415
1_2_566_10170_1035_3261_459_2531_35_3420_3757_1911_2932_1077_3206_576_11184_354_056_611_3963_453_3605_922_6183_4601_1466_1147_1716_1762_2722_858_1452_3840_209_1130_600_113
3_704_5_103_3537_117_2_1_2_2_3_2980_1410_104_301_2_1596_2230_2049_945_310_334_601_3_904_484_020_023_230_1131_171_1088_2_52_899_208_1043_2214_309_356_020_1_747_2712_2_389
1590_524_555_4_55_72_241_289_396_1_67_7_160_220_98_450_70_212_5_519_211_380_519_64_84_655_641_1374_2_832_726_1650_2095_1258_30_313_732_2_3_2_2_2_713_895_737_78_110_914_66
247_25_127_835_105_120_86_764_216_4_295_3_368_2_36_49_1_1_688_857_69_153_260_81_59_180_1_6_35_45_356_956_410_116_764_76_1_704_289_375_146_277_184_123_4_41_48_46_27_4_5_19
3_9_206_111_112_140_121_3_542_369_6_159_41_59_459_320_161_146_307_2_1347_3281_21297148_18_4540_8_5038_1153_5_2392_4_8890_107_884_3_209_283_45_463_115_1399_583_242_6023868
2478559_189957_kBL_jeic_kOP1:89978449})(function(){var a;((a=window.google)==null?a:stvc)?google.kEI=g.kEI:window.google=g;}).call(this));(function(){google.sm
="webp";google.kEL="zh-TW";})();(function(){
var g=this;self=function k(){return window.google&&window.google.kOP1[null];var l,l=[];function n(a){for(var b;a&&(l=a.getAttribute)||!(b=a.getAttribute("eid"))){a=a.pare
ntNode;return b}}function p(a){for(var b=null;a&&(l=a.getAttribute)||!(b=a.getAttribute("leid"))){a=a.parentNode;return b}}function q(a){/http://.test(a&&window.location
.protocol=="https"&&google.mI&&google.mI(Error("a"),l,{src:a,glmm:l}),a="");return a}
function r(a,b,d,c,h){var s="";b.search("kai=")===-1&&(s="kai="+n(C).b.search("kai=")===-1&&(c=c(c))&&(s+=kai+"c"));var f=b.search("kcsid=")===-1&&a="slh";c="kzx"+D
ate.now().toString();g._csid&&f&&(c+="&csid="+g._csid);(d=d())&&(c+="&op="+d);return"/"+(h||"gen_204")+"?atyp=ia&t="+String(a)+"&cad="+b+c;});l=google.kEI;google.get
EI=google.getEI?p;google.mI=function(){return null};google.log=function(a,b,d,c,h,e){e=e===void 0?k:e;d||(d=r(a,b,e,c,h));if(d=d(d)){a=new Image;var f=a.length;mf[a]=a;a
.onerror=a.onload=a.onabort=function(){delete mf[f];a.src=d};google.log.l=function(a,b){(cb=void 0?k:b;return r(" "+a,b));}).call(this);(function(){google.yz(f);google.s
y=[];var d;(d=google).x||(d.x=function(a,b){if(a)var c=a.id;else{do c=Math.random();while(google.y(c))}google.y[c]=[a,b];return l});var e;(e=google).sx||(e.sx=function(a){
google.sy.push(a)});google.l=[];var f;(f=google).pl||(f.pl=function(a){google.la.push.apply(google.la,a)});google.lq=[];var g;(g=google).load||(g.load=function(a,b,c){g
oogle.la.push([a,b,c]);});var h;(h=google).loadAll||(h.loadAll=function(a,b){google.lq.push([a,b]);});google.bce||(var k;(k=google).bce||(k.bce=function(D){var l=[];(mg
oogle).fce||(m.fce=function(a,b,c,n){l.push([a,b,c,n]);});google.qce=l;}).call(this);google.f={};function(){
document.documentElement.addEventListener("submit",function(b){var a;r(a=b.target){var c=a.getAttribute("data-submitfalse");a=====1?l=====0&&a.elements.q.value?0:1;
size a=i&&a(b.preventDefault(),b.stopPropagation());});document.documentElement.addEventListener("click",function(b){var a;a={for(a=b.target;a&&a=document.documentElement;
a=a.parentElement){if(a.tagName==="A"){a=a.getAttribute("data-nohref")==="1"?break:aA=1ja&&b.preventDefault();});}).call(this);</script><style>#qbar,#user{font-s
ize:15px;padding-top:1px!important;#qbar{height:22px;#user{padding-bottom:7px!important;text-align:right;gdn,gdb{border-top:1px solid #c0c0c1;font-size:10px;gdn{heig
ht:8px;position:absolute;top:22px;width:100%;media all{gdb{height:22px;margin-right:5px;vertical-align:top;#qbar{float:left}}a.gbi,a.gbt{text-decoration:underline!important
```

Figure 9: Tráfico de salida.

Al recibir una respuesta inmediata al realizar un curl a www.google.com nos indica que el tráfico de salida esta funcionando correctamente.