

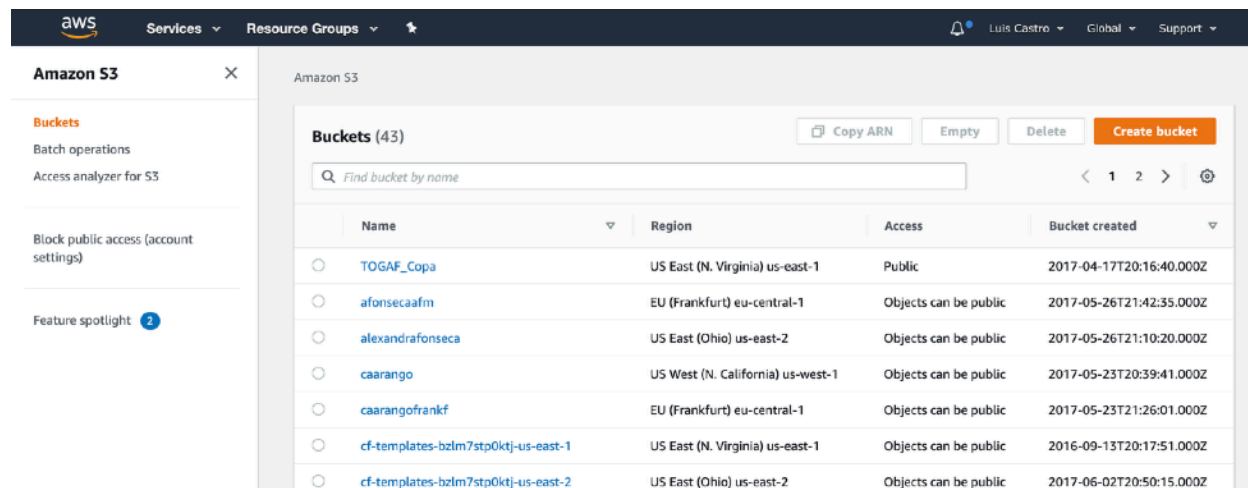
Paso 1

Acceder a la consola de AWS mediante el siguiente link:

<https://lcastrose.signin.aws.amazon.com/console>

Paso 2

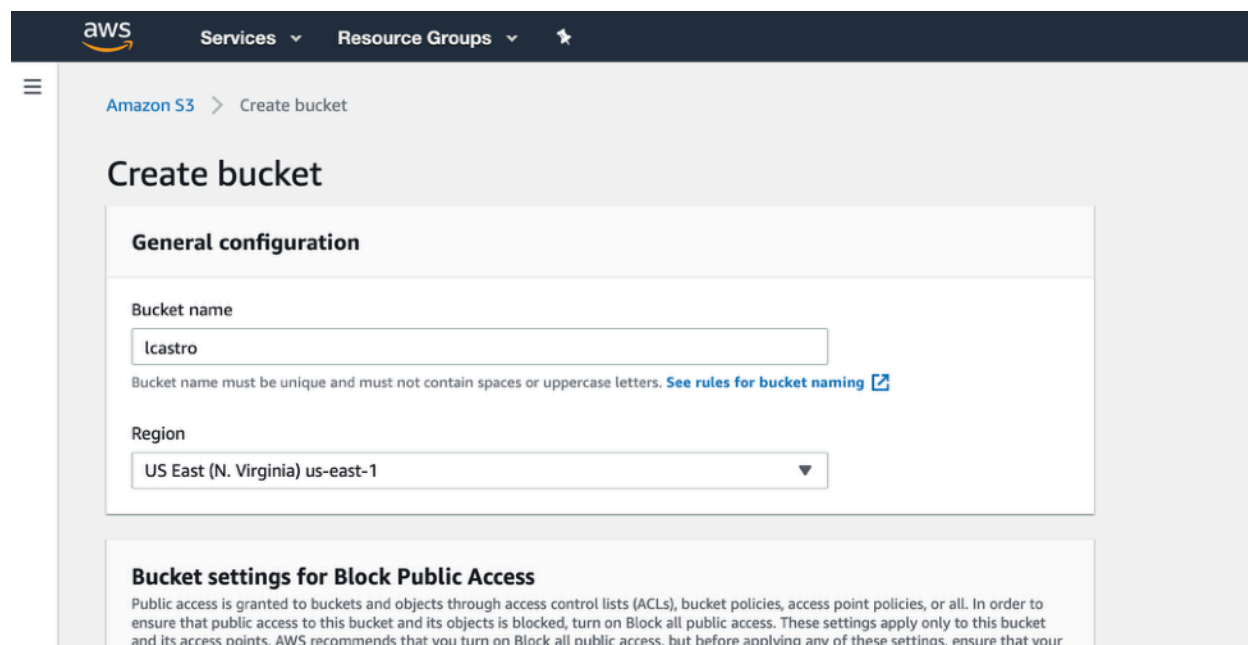
Acceder al servicio de S3



Name	Region	Access	Bucket created
TOGAF_Copa	US East (N. Virginia) us-east-1	Public	2017-04-17T20:16:40.000Z
afonsecaafm	EU (Frankfurt) eu-central-1	Objects can be public	2017-05-26T21:42:35.000Z
alexandrafonseca	US East (Ohio) us-east-2	Objects can be public	2017-05-26T21:10:20.000Z
caarango	US West (N. California) us-west-1	Objects can be public	2017-05-23T20:39:41.000Z
caarangofrank	EU (Frankfurt) eu-central-1	Objects can be public	2017-05-23T21:26:01.000Z
cf-templates-bzlm7stp0ktj-us-east-1	US East (N. Virginia) us-east-1	Objects can be public	2016-09-13T20:17:51.000Z
cf-templates-bzlm7stp0ktj-us-east-2	US East (Ohio) us-east-2	Objects can be public	2017-06-02T20:50:15.000Z

Paso 3

Cree un nuevo Bucket con el nombre de usuario en **Create Bucket**, seleccione la región que le corresponde y haga click en **Create Bucket**



Create bucket

General configuration

Bucket name: lcastro

Region: US East (N. Virginia) us-east-1

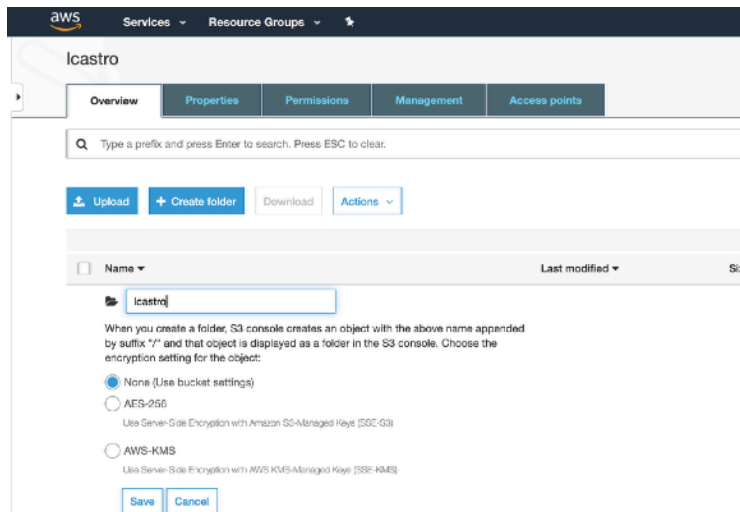
Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your

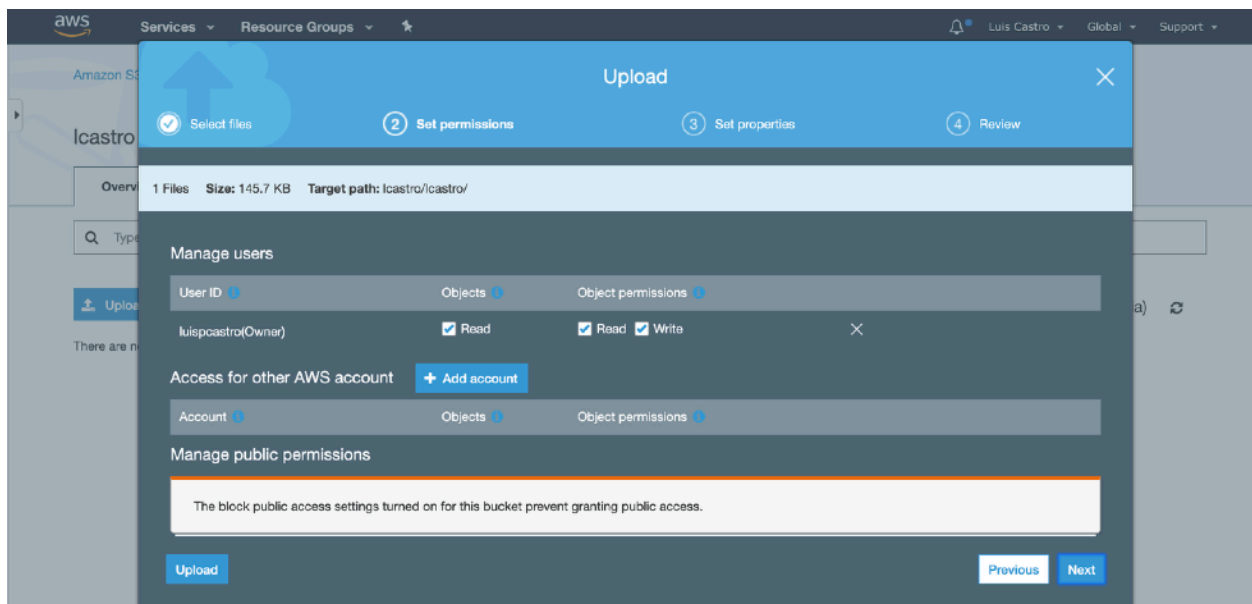
Paso 4

Dentro del Bucket creado cree un nuevo folder con el mismo nombre de usuario en **Create Folder** y haga **upload** del archivo enviado vía correo:

palo-alto-networks-product-summary-specsheet

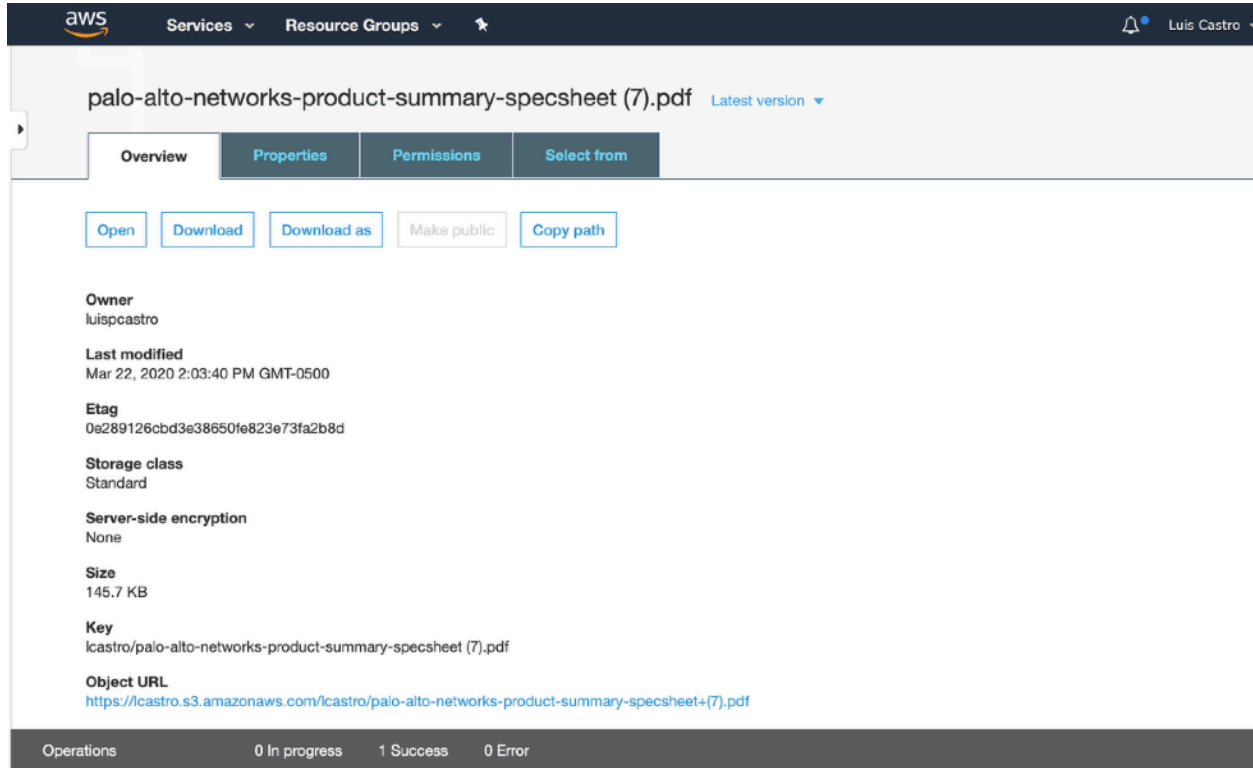


Hacer Click en Upload y aceptar los valores por Default



Paso 5

Verifique dentro de las propiedades del archivo cargado el link del archivo y haga click para abrir el link



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'aws' logo, 'Services', 'Resource Groups', and a user profile 'Luis Castro'. Below this, the file name 'palo-alto-networks-product-summary-specsheet (7).pdf' is displayed with a 'Latest version' dropdown. A tabbed interface shows 'Overview', 'Properties', 'Permissions', and 'Select from'. Under 'Overview', there are buttons: 'Open', 'Download', 'Download as', 'Make public', and 'Copy path'. The 'Properties' section lists the following details:

- Owner:** luispcastro
- Last modified:** Mar 22, 2020 2:03:40 PM GMT-0500
- Etag:** 0e289126cbd3e38650fe823e73fa2b8d
- Storage class:** Standard
- Server-side encryption:** None
- Size:** 145.7 KB
- Key:** lcastro/palo-alto-networks-product-summary-specsheet (7).pdf
- Object URL:** [https://lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+\(7\).pdf](https://lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+(7).pdf)

At the bottom, an 'Operations' bar shows '0 In progress', '1 Success', and '0 Error'.

Paso 6

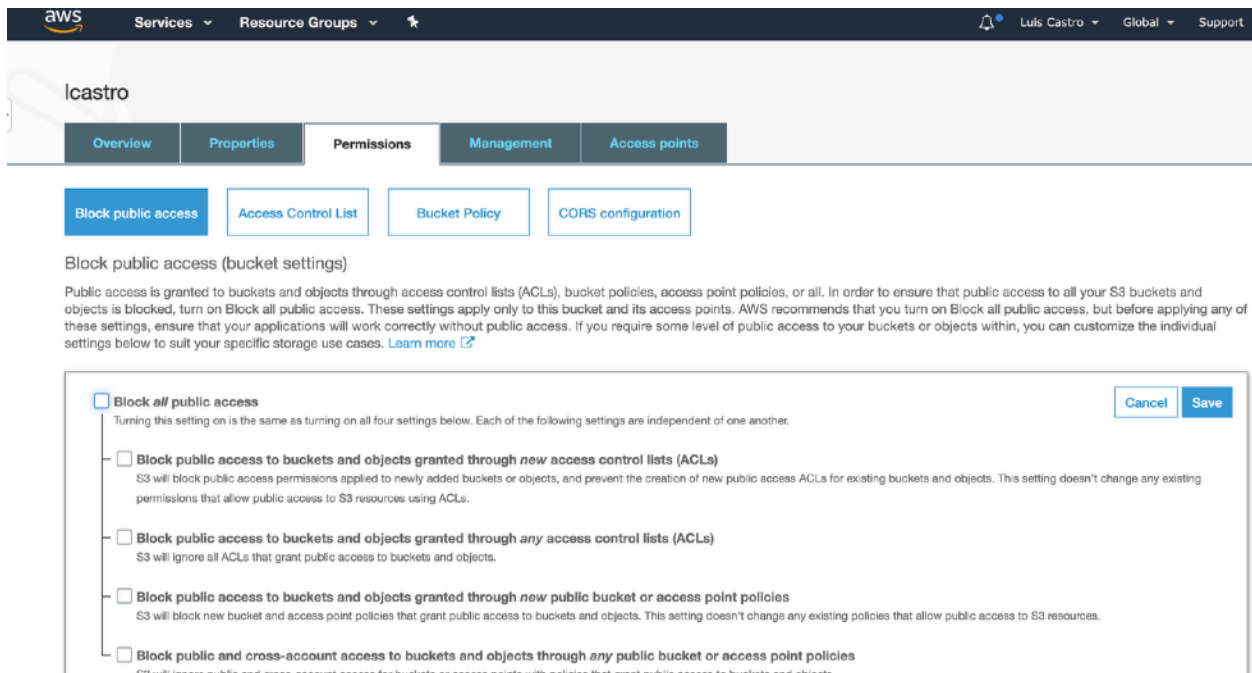
Hacer click en el **Object URL** y validar resultado

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>48AC54C167AD02FF</RequestId>
  <HostId>
    FEOznPKeneF7lGTgymX3B14Wcq7G2A356xovVzG5u8ztqRGBxS2A5Xi jOiT6at+2exp925neK+U=
  </HostId>
</Error>
```

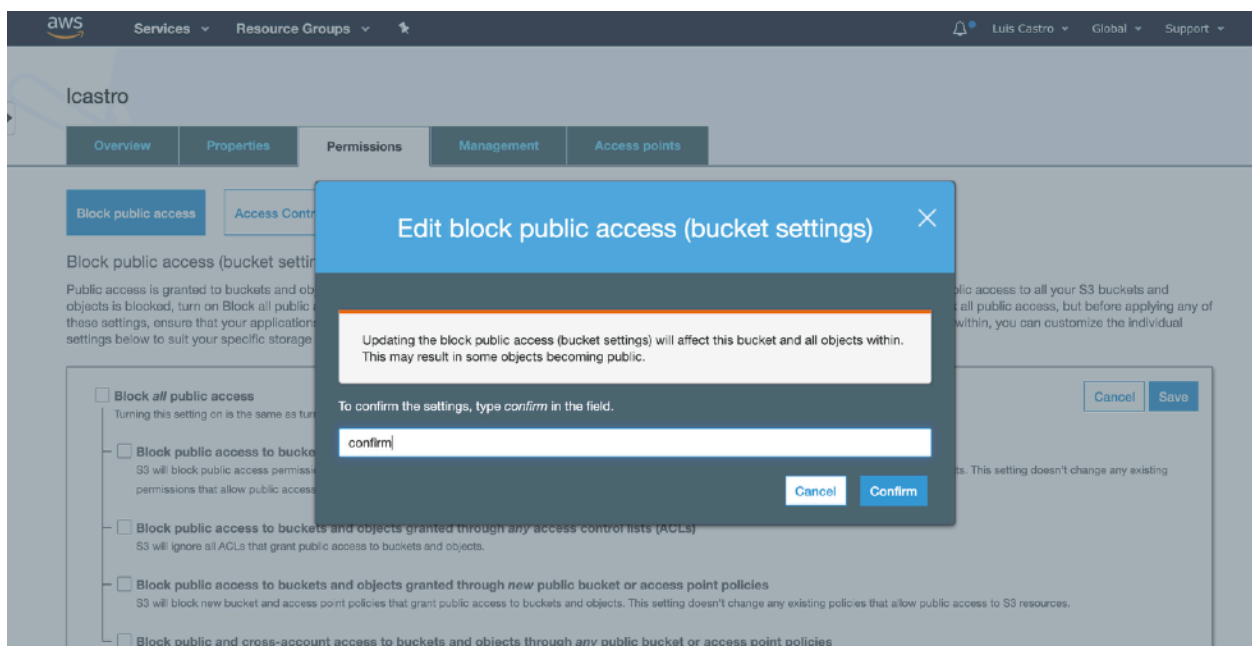
Paso 7

Darle acceso Publico al Bucket, para esto se debe de ir directamente al Bucket, seguidamente hacer click en **Permissions** y hacer click en **Edit** sobre **Block Public Access** y deseleccionar **Block All public access**, y dar **Save**



The screenshot shows the AWS Management Console interface for an S3 bucket. The 'Permissions' tab is active, and the 'Block public access' section is expanded. The 'Block all public access' checkbox is unchecked. Below it, four sub-settings are listed, each with an unchecked checkbox: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. The 'Access Control List' tab is selected in the top navigation bar.

Escribir *confirm* para que los cambios se apliquen



The screenshot shows the same AWS Management Console interface as before, but with a modal dialog box open. The dialog box is titled 'Edit block public access (bucket settings)' and contains a warning message: 'Updating the block public access (bucket settings) will affect this bucket and all objects within. This may result in some objects becoming public.' Below the warning, it says 'To confirm the settings, type confirm in the field.' and there is an input field with the text 'confirm' entered. There are 'Cancel' and 'Confirm' buttons at the bottom of the dialog box.

Paso 8

Ir al folder creado y hacer click en **Permissions** y escoja **Public Access>Everyone>Access to the Object>Read Object** y valide nuevamente el acceso al link

The screenshot shows the AWS IAM console interface. The 'Permissions' tab is active, and the 'Select from' button is highlighted. A modal window titled 'Everyone' is open, displaying a warning: 'This object will have public access. Everyone will have access to one or all of the following: read this object, read and write permissions.' Below the warning, there are checkboxes for 'Access to the object' (checked), 'Read object', 'Access to this object's ACL', 'Read object permissions', and 'Write object permissions'. The 'Read object' checkbox is checked, and the 'Save' button is visible at the bottom right of the modal.

Validar el URL: <bucket-name>.S3.amazonaws.com/<folder-name>/File Name

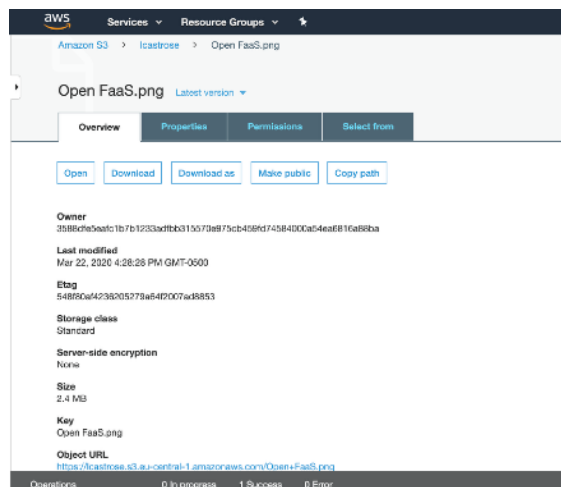
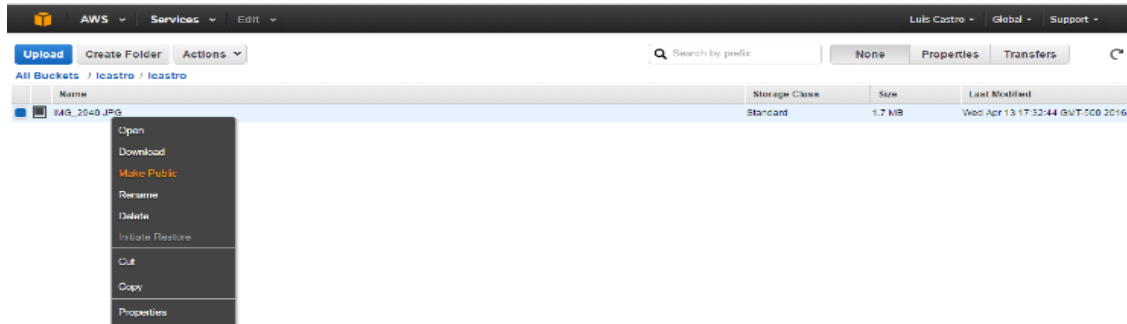
lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+(7).pdf

Palo Alto Networks Platform Specifications and Features Summary						
Table 1: Firewall Performance and Capabilities						
Performance and Capabilities	PA-7000	PA-7000P	PA-8200	PA-8200P	PA-8200	PA-8200P
Firewall throughput (App-ID, appsec)	700 Gbps	950 Gbps	56 Gbps	56 Gbps	40 Gbps	30 Gbps
Threat Prevention throughput (appsec)	350 Gbps	525 Gbps	31.5 Gbps	31.5 Gbps	21 Gbps	15 Gbps
IPsec VPN throughput	280 Gbps	373 Gbps	27 Gbps	27 Gbps	18 Gbps	13 Gbps
New sessions per second	4,900,000	6,525,000	350,000	350,000	254,000	190,000
Maximum sessions	320,000,000	425,000,000	64,000,000	64,000,000	45,000,000	34,000,000
Virtual systems (base/max)	35/325	45/325	35/325	35/325	25/225	18/180
Hardware Specifications	PA-7000	PA-7000P	PA-8200	PA-8200P	PA-8200	PA-8200P
Interfaces supported NPC option 14	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)	10/100/1000 (up to 12), SFP/SFP+ (up to 8), QSFP+ (up to 4), QSFP28 (up to 4)
Management I/O	SFP/SFP+ (2), SFP/SFP+ HA (2), HSC1 HA2/HA3 (2), RS45 serial console (1), Micro USB serial console (1)	SFP/SFP+ (2), SFP/SFP+ HA (2), HSC1 HA2/HA3 (2), RS45 serial console (1), Micro USB serial console (1)	10/100/1000 (2), 10/100/1000 out-of-band management (1), RS45 console (1)	10/100/1000 (2), 10/100/1000 out-of-band management (1), RS45 console (1)	10/100/1000 (2), 10/100/1000 out-of-band management (1), RS45 console (1)	10/100/1000 (2), 10/100/1000 out-of-band management (1), RS45 console (1)
Size	19U, 19" standard rack	4U, 19" standard rack or 1U, 19" standard rack with optional PAN-ABSTRACT MC	3U, 19" standard rack	3U, 19" standard rack	3U, 19" standard rack	3U, 19" standard rack
Power supply	2500 W AC (2400 W / 2300 W) (4 expandable to 8)	2500 W AC (2400 W / 2300 W) (4)	1200 W AC or DC (12 fully redundant) (2)	1200 W AC or DC (12 fully redundant) (2)	1200 W AC or DC (12 fully redundant) (2)	1200 W AC or DC (12 fully redundant) (2)
Redundant power supply	Yes	Yes	Yes	Yes	Yes	Yes
Disk drives	24.0 GB SED system drive, RAID (2)	24.0 GB SED system drive, RAID (2)	System: 360 GB SSD, RAID (1) Log: 8 TB HDD, RAID (2)	System: 360 GB SSD, RAID (1) Log: 8 TB HDD, RAID (2)	System: 360 GB SSD, RAID (1) Log: 8 TB HDD, RAID (2)	System: 360 GB SSD, RAID (1) Log: 8 TB HDD, RAID (2)
Hot-swappable fans	Yes	Yes	Yes	Yes	Yes	Yes
Performance and Capabilities	PA-2260		PA-2260P		PA-2260	
Firewall throughput (App-ID, appsec)	10 Gbps		6.5 Gbps		5 Gbps	
Threat Prevention throughput (appsec)	4.4 Gbps		3 Gbps		2.4 Gbps	
IPsec VPN throughput	4.8 Gbps		3.2 Gbps		2.7 Gbps	
New sessions per second	118,000		84,000		57,000	
Maximum sessions	3,900,000		2,700,000		1,900,000	

Paso 11

Acceder al servicio de CloudFront

Cree un nuevo Bucket en la región de Frankfurt con el nombre de usuario seguido del nombre de la región (todo pegado y en minúscula) y suba la fotografía enviada por correo, modifique los permisos, hágala Pública e ingrese al link de la imagen y copie el link

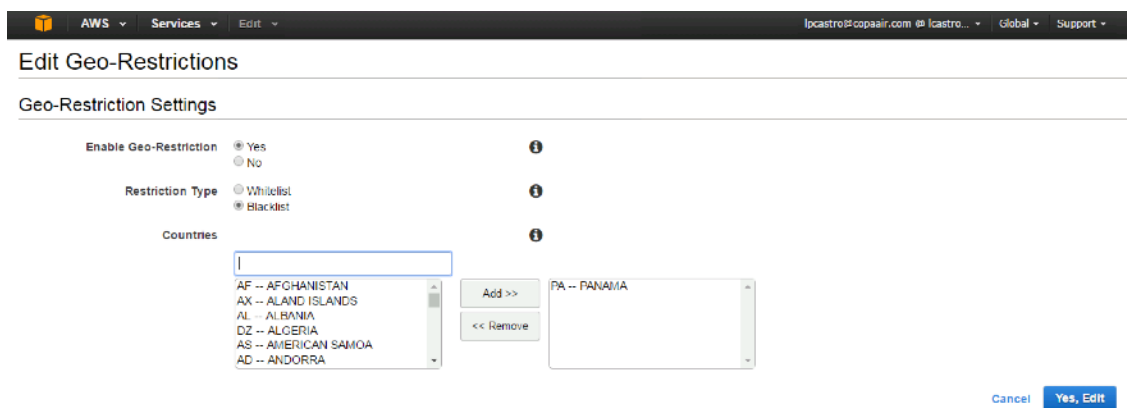
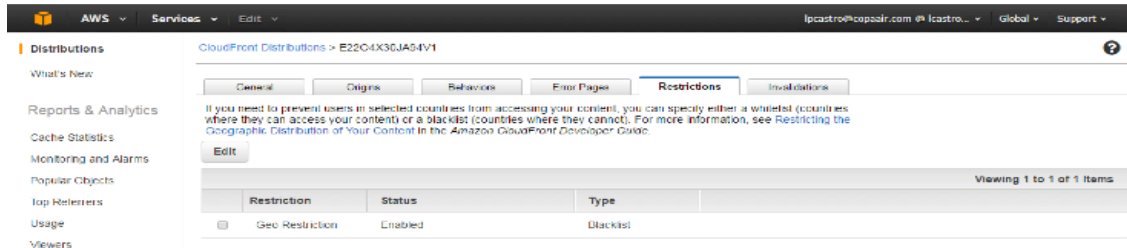


Ejemplo:

<https://lcastrore.s3.eu-central-1.amazonaws.com/Open+FaaS.png>

Paso 14

Modifique la distribución para restringir el acceso por Geo-Localización y active la **Restriction Type - Blacklist** y agregue su Pais (Ej: Panamá) y marque **Yes, Edit**.



Paso 15

Valide después que la distribución se encuentre completada que el acceso es restringido

