

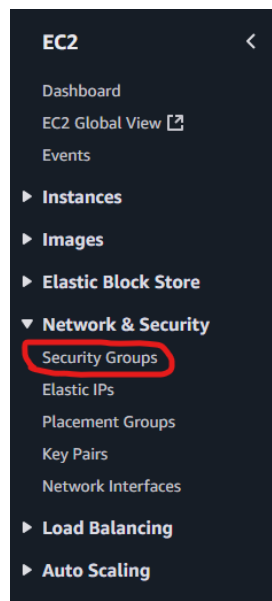
AWS Security Groups – BucStop

What is an AWS Security Group?

An AWS Security Group is a virtual firewall that can be applied to EC2 instances to control the traffic that is able to flow into and out of the EC2 instance. Traffic is controlled using two sets of rules: Inbound Rules which control the traffic that is able to flow into the EC2 instance and Outbound Rules which control the traffic that is able to flow out of the EC2 instance. Different EC2 instances should have Security Groups designed specifically for the needs of the instance (like a Production Instance Security Group that only allows access from the IPv4 addresses associated with the ETSU Wi-Fi network and a Development Instance Security Group that allows access from IPv4 addresses outside of the ETSU network).

How to access AWS Security Groups

AWS Security Groups can be accessed through the EC2 service on the AWS Console. From the EC2 service, you can find Security Groups under the Network and Security section as shown below:



From the Security Groups page, you can create, manage, and delete any security groups that you have.

Security Groups (3) Info								
Find security groups by attribute or tag								
<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
<input type="checkbox"/>	-	sg-08892312f83a51e51	BucStop Security Group	vpc-005cd6541e94f8be6	Allows access to BucStop EC2 from any ...	676206917188	9 Permission entries	1 Permission entry
<input type="checkbox"/>	-	sg-0b6d6f61e6d2891e69	BucStop On-Campus Security Group	vpc-005cd6541e94f8be6	Allow students connected to ETSU WiFi ...	676206917188	16 Permission entries	2 Permission entries
<input type="checkbox"/>	-	sg-092c6d2d58c61a079	default	vpc-005cd6541e94f8be6	default VPC security group	676206917188	1 Permission entry	1 Permission entry

Creating a Security Group

When creating a security group, you need to provide a name, description, associated VPC (Virtual Private Cloud), the inbound rules, the outbound rules, and any tags (optional). For each of these, you can find more information by clicking the blue “Info” button beside the name to be provided additional information and links to manual pages that go into further detail.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

This security group has no inbound rules.

[Add rule](#)

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom	
			Q	
			0.0.0.0/0	

[Add rule](#)

[Delete](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Create security group](#)

Inbound Rules

Inbound Rules govern the types of traffic that is allowed to contact the EC2 instance. There are multiple different options that can be specified for an inbound rule from the type of traffic, protocol, port range, source, and description.

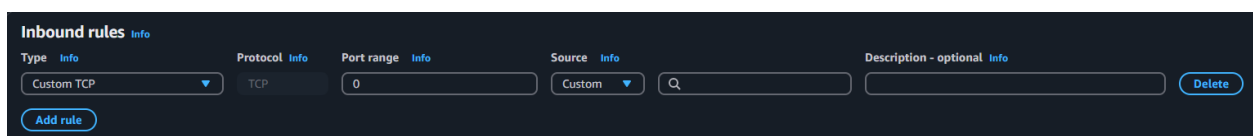
The Type determines what kind of traffic is allowed to connect to the EC2 instance whether it is a custom TCP, custom UDP, custom ICMP, SSH, HTTP, HTTPS, etc.

The Protocol is the associated type of protocol for the type specified (TCP for a custom TCP, UDP for a custom UDP, TCP for SSH, etc.).

The Port Range is the specific ports that will be allowed access (22 for SSH, 80 for HTTP, 443 for HTTPS, etc.) This section is very important for the project as the containers run on their own ports (8080 for the WebApp, 8081 for the API Gateway, 8082 for Snake, 8083 for Pong, 8084 for Tetris) and will need to be explicitly allowed with an inbound rule.

The Source is the IPv4 or IPv6 address that is being allowed to connect to the instance. This section is also very important for the project as the end goal of the project is that only those connected to the ETSU Wi-Fi networks should be allowed access (216.145.70.0/23 and 151.141.0.0/16 are the associated IPv4 addresses).

Lastly, the Description is an optional text field that can be used to write additional information about the rule.

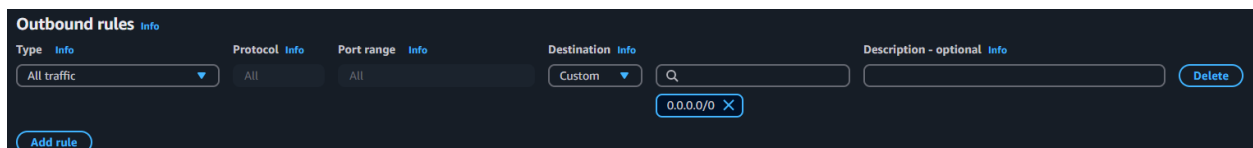


The screenshot shows the 'Inbound rules' configuration page in the AWS Management Console. It features a dark-themed interface with a header 'Inbound rules' and an 'Info' link. Below the header, there are five main sections: 'Type' (set to 'Custom TCP'), 'Protocol' (set to 'TCP'), 'Port range' (set to '0'), 'Source' (set to 'Custom' with a search icon), and 'Description - optional'. Each section has an 'Info' link. At the bottom left is an 'Add rule' button, and at the bottom right is a 'Delete' button.

Outbound Rules

Outbound Rules govern the types of traffic that is allowed out of the EC2 instance. There are multiple different options that can be specified for an outbound rule from the type of traffic, protocol, port range, destination, and description. The type, protocol, port range, and description are the exact same as those mentioned in the Inbound Rules section.

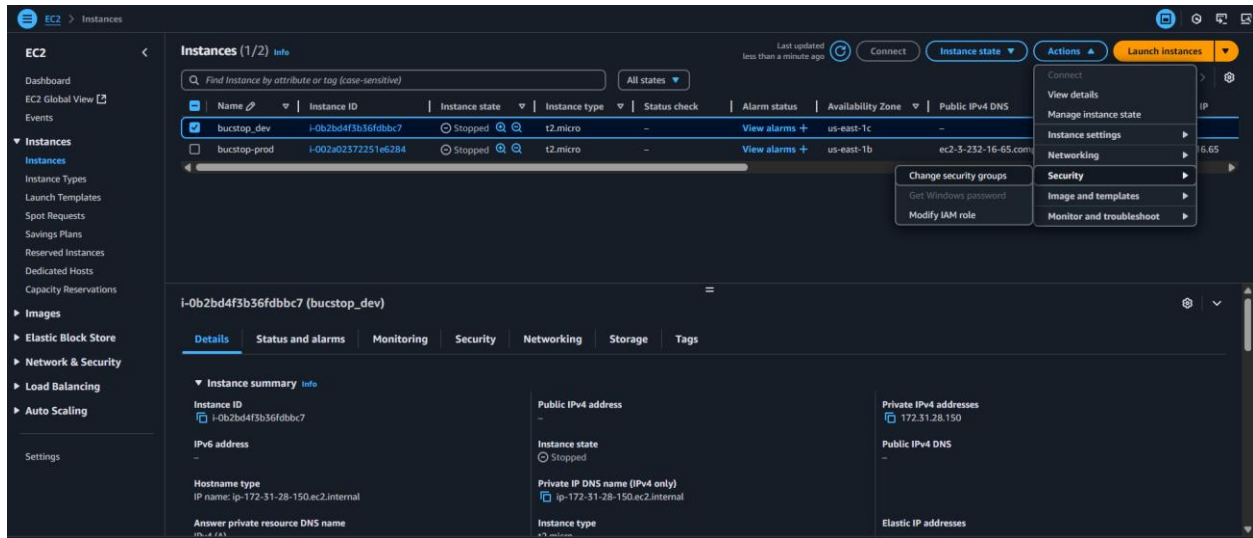
The Destination is the IPv4 or IPv6 addresses that are allowed to be contacted by the EC2 instance. This section is very important for the project as the end goal of the project is that only those connected to the ETSU Wi-Fi networks should be able to be accessed by the EC2 instance (216.145.70.0/23 and 151.141.0.0/16 are the associated IPv4 addresses).



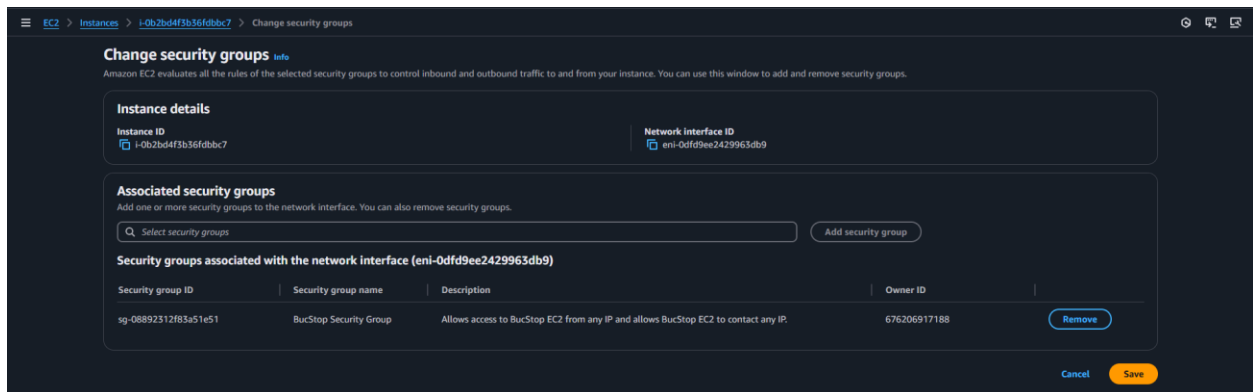
The screenshot shows the 'Outbound rules' configuration page in the AWS Management Console. It features a dark-themed interface with a header 'Outbound rules' and an 'Info' link. Below the header, there are five main sections: 'Type' (set to 'All traffic'), 'Protocol' (set to 'All'), 'Port range' (set to 'All'), 'Destination' (set to 'Custom' with a search icon), and 'Description - optional'. Each section has an 'Info' link. At the bottom left is an 'Add rule' button, and at the bottom right is a 'Delete' button. The 'Destination' field shows a search icon and a button to add a new destination.

Attaching a Security Group to an EC2 Instance

To attach a security group to an EC2 instance, navigate to the instances page of the EC2 service. From here, select the EC2 instance that you want to apply the Security Group to, select the “Actions” drop down menu on the right, select the “Security” section, and select “Change Security Groups”.



From here, you can view the currently attached security groups and add and remove security groups that are attached to the EC2 Instance.



Another way of viewing the currently attached security groups along with their inbound and outbound rules is through the Security Tab on the specific instance’s EC2 page.

DetailsStatus and alarmsMonitoringSecurityNetworkingStorageTags

▼ Security details

IAM Role

No roles attached to instance profile: ec2-cloudwatchserver-role

Owner ID

676206917188

Security groups

sg-08892312f83a51e51 (BucStop Security Group)

► Inbound rules

► Outbound rules

Team Cooked’s Security Groups

Development Security Group:

sg-08892312f83a51e51 - BucStop Security GroupActions ▼

Details

Security group name

BucStop Security Group

Owner

676206917188

Security group ID

sg-08892312f83a51e51

Inbound rules count

9 Permission entries

Description

Allows access to BucStop EC2 from any IP and allows BucStop EC2 to contact any IP.

Outbound rules count

1 Permission entry

VPC ID

vpc-005cd6541e94f8be6

Inbound rulesOutbound rulesSharing - newVPC associations - newTags

Inbound rules (9)

Q Search

Manage tagsEdit inbound rules

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sg-01a9dd3726d14f87a	IPv4	SSH	TCP	22	0.0.0.0/0	Allows connecting to BucStop EC2 via SSH (if key pairs are setup).
<input type="checkbox"/>	-	sg-02e37122614e13c8d	IPv4	HTTPS	TCP	443	0.0.0.0/0	Allows connecting to BucStop EC2 via HTTPS.
<input type="checkbox"/>	-	sg-02aa3123e5a22a863	IPv4	HTTP	TCP	80	0.0.0.0/0	Allows connecting to BucStop EC2 via HTTP.
<input type="checkbox"/>	-	sg-060f6c61c3c71593a	IPv4	Custom TCP	TCP	8080	0.0.0.0/0	-
<input type="checkbox"/>	-	sg-07afc01401685de9b	IPv4	Custom TCP	TCP	8081	0.0.0.0/0	-
<input type="checkbox"/>	-	sg-0932f0c3dca638329	IPv4	Custom TCP	TCP	8082	0.0.0.0/0	-
<input type="checkbox"/>	-	sg-0c69206f6d0cc3c6d	IPv4	Custom TCP	TCP	8083	0.0.0.0/0	-
<input type="checkbox"/>	-	sg-0dee9f7748238f9dd	IPv4	Custom TCP	TCP	8084	0.0.0.0/0	-
<input type="checkbox"/>	-	sg-0d58a358df407cf00	IPv4	Custom TCP	TCP	8085	0.0.0.0/0	-

Outbound rules (1)

Q Search

Manage tagsEdit outbound rules

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Destination	Description
<input type="checkbox"/>	-	sg-04b27e9f710462d86	IPv4	All traffic	All	All	0.0.0.0/0	Allows BucStop to access any IP.

This Security Group was used for development purposes. It could have been made more secure by limiting access even further to individual IPv4 addresses of the Development Team, but we found this unnecessary. The Rules could also be condensed into a Port Range instead of explicitly allowing the Ports individually.

Production Security Group (Currently Broken):

Details

Security group name
 BucStop On-Campus Security Group

Security group ID
 sg-0b6df61e6d2891e69

Description
 Allow students connected to ETSU WiFi to connect to BucStop and BucStop to connect to them.

VPC ID
 vpc-005cd6541e94f8be6

Owner
 676206917188

Inbound rules count
16 Permission entries

Outbound rules count
2 Permission entries

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (16)

Manage tags

Edit inbound rules

☐

Name

Security group rule ID

IP version

Type

Protocol

Port range

Source

Description

<input type="checkbox"/>	-	sg-05e0d3c308c8d417d	IPv4	SSH	TCP	22	216.145.70.0/23	Allows connecting to BucStop EC2 via SSH (if key pairs are setup).
<input type="checkbox"/>	-	sg-0618b78f2e623edd8	IPv4	SSH	TCP	22	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-0829095298fccf47e	IPv4	HTTPS	TCP	443	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-03e00328423adcf8a	IPv4	HTTPS	TCP	443	216.145.70.0/23	Allows connecting to BucStop EC2 via HTTPS.
<input type="checkbox"/>	-	sg-002445e0badfb1e19	IPv4	HTTP	TCP	80	216.145.70.0/23	Allows connecting to BucStop EC2 via HTTP.
<input type="checkbox"/>	-	sg-072b843f9449c7171	IPv4	HTTP	TCP	80	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-0c0a133cf02295cf	IPv4	Custom TCP	TCP	8080	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-005b78063c6065287	IPv4	Custom TCP	TCP	8080	216.145.70.0/23	-
<input type="checkbox"/>	-	sg-0c3d25e9b73adac3c	IPv4	Custom TCP	TCP	8081	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-0191b094be8abb06b	IPv4	Custom TCP	TCP	8081	216.145.70.0/23	-
<input type="checkbox"/>	-	sg-0112ed0268bd8e3dc	IPv4	Custom TCP	TCP	8082	216.145.70.0/23	-
<input type="checkbox"/>	-	sg-0ca0cc235d0dbb962	IPv4	Custom TCP	TCP	8082	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-0dc868e69a01a3a81	IPv4	Custom TCP	TCP	8083	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-010b26817d3cc561b	IPv4	Custom TCP	TCP	8083	216.145.70.0/23	-
<input type="checkbox"/>	-	sg-0ed6acae21e5cf8e0	IPv4	Custom TCP	TCP	8084	151.141.0.0/16	-
<input type="checkbox"/>	-	sg-04f490ef77d5eb51d	IPv4	Custom TCP	TCP	8084	216.145.70.0/23	-

Outbound rules (2)

Manage tags

Edit outbound rules

☐

Name

Security group rule ID

IP version

Type

Protocol

Port range

Destination

Description

<input type="checkbox"/>	-	sg-0bf3f3735fb467758	IPv4	All traffic	All	All	216.145.70.0/23	Allows BucStop to access any ETSU IP.
<input type="checkbox"/>	-	sg-09a0b57c4f10ab55e	IPv4	All traffic	All	All	151.141.0.0/16	Allows BucStop to access any ETSU IP.

This Security Group was designed to be used for our production EC2 instance and set up to only allow traffic to and from IPv4 addresses associated with the ETSU Wi-Fi network. It does not currently work though, and we do not know why (although a current idea is that the outbound rules are breaking it). Any future teams that pick this solution up and work with AWS should devote time to fixing this in-class as the ability to test changes that are made is dependent on being on-campus and connected to the ETSU Wi-Fi network. Like the previous Security Group, the Rules could also be condensed into a Port Range instead of explicitly allowing the Ports individually.

Other Resources

Security Groups Overview (with Links to Further Topics)

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html?icmpid=docs_ec2_console#creating-security-group

Creating a Security Group

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/creating-security-group.html>

Inbound and Outbound Rules (with Sample Scenarios)

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html?icmpid=docs_ec2_console