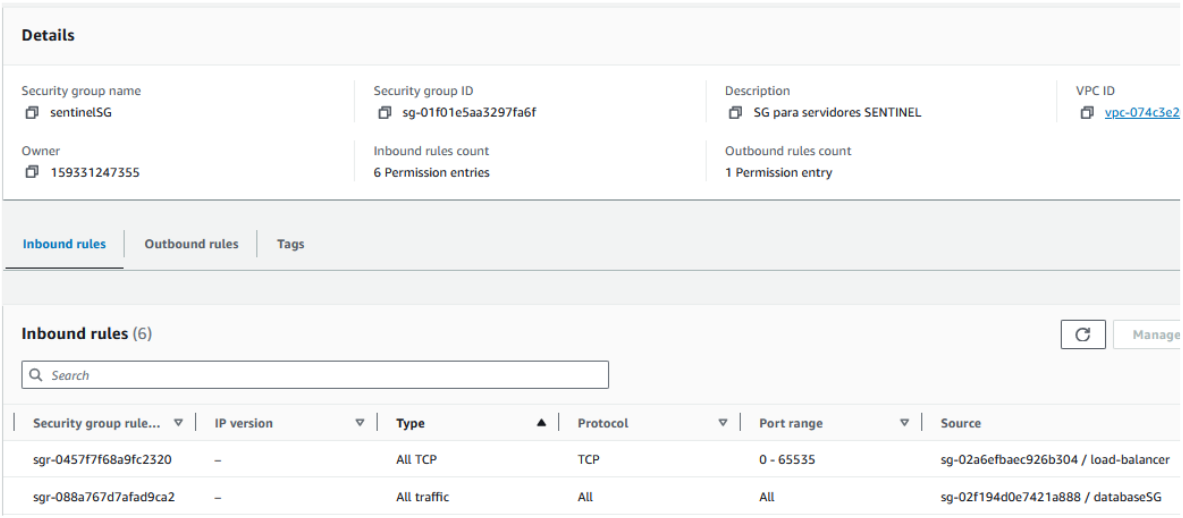
NETSEC-001 - Define security best practices for Virtual Private Cloud (Amazon VPC) and other network security considerations

Based on the methodology and design of the solution, security groups are defined in such a way as to allow traffic only to and from where it belongs.

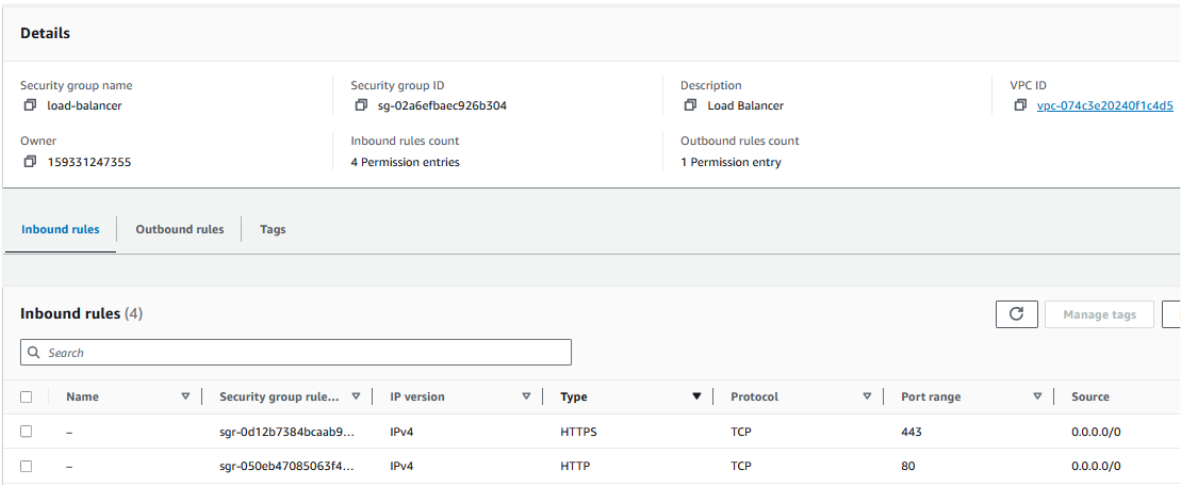
Considerations:

The entire implemented environment required a Landing Zone. Here we defined the VPC to be used and the security groups that would allow us to define access and restrictions for incoming and outgoing traffic. For more details, please review the networking documentation.

App Servers only accept traffic coming from the load balancer or from a database server



Load balancers accept https traffic from end customers



Databases only accept traffic coming from internal servers

Security group name
databaseSG

Security group ID
sg-02f194d0e7421a888

Description
SG para servidores Base de datos

VPC ID
vpc-074c3e20240f1c4d5

Owner
159331247355

Inbound rules count
7 Permission entries

Outbound rules count
1 Permission entry

Inbound rules | Outbound rules | Tags

Inbound rules (7)

Manage tags | Edit inbound rules

Search

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
–	sgr-0f8dde43b397f7379	IPv4	SMB	TCP	445	10.0.0.0/16
–	sgr-0ae1a4276ad90a3ce	–	RDP	TCP	3389	sg-0ab88db72795ee6c7 / accesoSG
–	sgr-0e1155fa663aea0df	–	MSSQL	TCP	1433	sg-008888daf595863d9 / elistSG
–	sgr-0b2af733a2682687e	–	MSSQL	TCP	1433	sg-01f01e5aa3297fa6f / sentinelSG
–	sgr-0c00d820add083f0c	–	MSSQL	TCP	1433	sg-0ab88db72795ee6c7 / accesoSG

All servers managed have SSM management enabled.

Systems Manager > Fleet Manager > Managed nodes

Fleet Manager Info

Managed Nodes (12)