

## 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

**Details**

Security group name  
sentinelSG

Security group ID  
sg-01f01e5aa3297fa6f

Description  
SG para servidores SENTINEL

VPC ID  
vpc-074c3e2

Owner  
159331247355

Inbound rules count  
6 Permission entries

Outbound rules count  
1 Permission entry

Inbound rules

Outbound rules

Tags

**Inbound rules (6)**

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-0457f7f68a9fc2320	-	All TCP	TCP	0 - 65535	sg-02a6efbaec926b304 / load-balancer
sgr-088a767d7afad9ca2	-	All traffic	All	All	sg-02f194d0e7421a888 / databaseSG

Load balancers accept https traffic from end customers

**Details**

Security group name  
load-balancer

Security group ID  
sg-02a6efbaec926b304

Description  
Load Balancer

VPC ID  
vpc-074c3e20240f1c4d5

Owner  
159331247355

Inbound rules count  
4 Permission entries

Outbound rules count  
1 Permission entry

Inbound rules

Outbound rules

Tags

**Inbound rules (4)**

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0d12b7384bcaab9...	IPv4	HTTPS	TCP	443	0.0.0.0/0
-	sgr-050eb47085063f4...	IPv4	HTTP	TCP	80	0.0.0.0/0

Databases only accept traffic coming from internal servers



Security group name  
databaseSG

Owner  
159331247355

Security group ID  
sg-02f194d0e7421a888

Inbound rules count  
7 Permission entries

Description  
SG para servidores Base de datos

Outbound rules count  
1 Permission entry

VPC ID  
vpc-074c3e20240f1c4d5

Inbound rules | Outbound rules | Tags

Inbound rules (7)

Search

Manage tags | Edit inbound rules

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sg-0f8dde43b397f7379	IPv4	SMB	TCP	445	10.0.0.0/16
<input type="checkbox"/>	-	sg-0ae1a4276ad90a3ce	-	RDP	TCP	3389	sg-0ab88db72795ee6c7 / accesoSG
<input type="checkbox"/>	-	sg-0e1155fa663aea0df	-	MSSQL	TCP	1433	sg-00888daf595863d9 / elistSG
<input type="checkbox"/>	-	sg-0b2af733a2682687e	-	MSSQL	TCP	1433	sg-01f01e5aa3297fa6f / sentinelSG
<input type="checkbox"/>	-	sg-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)