Skip to content

Enterprise

Search or jump to…

-

  In this repository All GitHub Enterprise ↵
  Jump to ↵

- No suggested jump to results

-

  In this repository All GitHub Enterprise ↵
  Jump to ↵
-

  In this repository All GitHub Enterprise ↵
  Jump to ↵
- Octocat Spinner Icon

- Pull requests
- Issues
- Explore

-
- ▶ +
- ▶ @pounder

Sign out

- ▶ Watch
  2
- ★ Unstar 1
  ★ Star 1
- ▶ Fork
  0

DXC-Tucson/Container-scan-poc Private

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings
Permalink

Branch: develop

Find file Copy path
Container-scan-poc/Docs/Technical Reference/**4.networking.md**
942b9b2 10 minutes ago
@pounder pounder update route tables and NSGs
▶ **1** contributor
Raw Blame History

✏

🗑

379 lines (256 sloc) 24.3 KB

Networking

Contents

Network Topology

=================

Network Topology

VPC Topology

============

(Top)

Guidance: DevOps tools are segregated into a Network Operations Centre (NOC) VPC with all containers deployed into a dedicated Kubernetes VPC as recommended in the Amazon EKS "Getting Started" guide. Both VPCs are within the same AWS region and joined via a peering link.

VPC Peering

Peering Route Tables

============

(Top)

Guidance: VPC Peering Links provide a secure private connection between discrete cloud networks.

Routes TBD

NOC VPC

NOC Route Tables

============

(Top)

Guidance: Route tables should be applied to network subnets. They are required to ensure correct traffic routing and require explicitly described inbound and outbound rules.

Private Subnet Route Table

Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	NAT Gateway
192.168.0.0/16	Peering Link

Public Subnet Route Table

Destination	Target
172.16.0.0/20	Local
0.0.0.0/0	Internet Gateway

NOC ACL Definitions

===============

(Top)

Guidance: Access Control Lists (ACL) should be applied to network subnets. They are stateless and require explicitly described inbound and outbound rules.

ACL Rules for the NOC Public Subnet

Inbound

Rule	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	0.0.0.0/0	TCP	443	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	DXC Global WAN	TCP	22	ALLOW	Allows inbound SSH traffic over the Internet gateway.
130	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from hosts on the Internet that are responding to requests originating in the subnet.
*	0.0.0.0/0	all	all	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows outbound HTTP traffic from the subnet to the Internet.

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
110	0.0.0.0/0	TCP	443	ALLOW	Allows outbound HTTPS traffic from the subnet to the Internet.
120	172.16.10.0/24	TCP	8080	ALLOW	Allows outbound HTTP traffic from the public subnet to the private subnet
130	172.16.10.0/24	TCP	8443	ALLOW	Allows outbound HTTPS traffic from the public subnet to the private subnet
140	0.0.0.0/0	TCP	32768-65535	ALLOW	Allows outbound responses to clients on the Internet
150	172.16.10.0/24	TCP	22	ALLOW	Allows outbound SSH access to instances in your private subnet
*	0.0.0.0/0	all	all	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

ACL Rules for the NOC Private Subnet

Inbound

Rule	Source IP	Protocol	Port	Allow/Deny	Comments
100	172.16.0.0/24	TCP	80	ALLOW	Allows servers in the public subnet access to HTTP web interfaces in the private subnet.
110	172.16.0.0/24	TCP	443	ALOW	Allows servers in the public subnet access to HTTPS web interfaces in the private subnet.
120	172.16.0.0/24	TCP	8080	ALLOW	Allows servers in the public subnet access to the private subnet.
130	172.16.0.0/24	TCP	8443	ALLOW	Allows servers in the public subnet access to the private subnet.
140	172.16.0.0/0	TCP	22	ALLOW	Allows inbound SSH traffic from an SSH bastion in the public subnet
150	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from the NAT device in the public subnet for requests originating in the private subnet.
160	192.168.0.0/16	TCP	1024-65535	ALLOW	Allows inbound return traffic from the Kubernetes VPC.
*	0.0.0.0/0	all	all	DENY	Denies all IPv4 inbound traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows outbound HTTP traffic from the subnet to the Internet.
110	0.0.0.0/0	TCP	443	ALLOW	Allows outbound HTTPS traffic from the subnet to the Internet.
120	172.16.0.0/24	TCP	32768-65535	ALLOW	Allows outbound responses to the public subnet
130	192.168.0.0/16	TCP	22	ALLOW	Allows outbound SSH traffic to the Kubernetes VPC.
140	192.168.0.0/16	TCP	443	ALLOW	Allows outbound HTTPS traffic to the Kubernetes VPC.

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
*	0.0.0.0/0	all	all	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

NOC Network Security Groups

======================

(Top)

Guidance: Network Security Groups (NSG) should be applied to host instances in AWS. They are stateful and, therefore, only need to describe specific services.

Bastion Host Security Group

Inbound

Source	Protocol	Port Range	Comments
DXC Global WAN	TCP	22	Allow inbound SSH from Internet.

Outbound

Destination	Protocol	Port Range	Comments
0.0.0.0/0	All	All	Allow outbound access to the anywhere

Proxy Host Security Group

Inbound

Source	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow inbound HTTP from Internet.
Orchestrator Hosts(s)	TCP	22	Allow inbound SSH from Orchestrator.
0.0.0.0/0	TCP	443	Allow inbound HTTPS from Internet.

Outbound

Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
Orchestrator Hosts(s)	TCP	8080	Allow outbound HTTP access to the Orchestrator
Orchestrator Hosts(s)	TCP	8443	Allow outbound HTTPS access to the Orchestrator
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet

Orchestrator Host Security Group

Inbound

Source	Protocol	Port Range	Comments
Proxy Host(s)	TCP	8080	Allow inbound HTTP from Proxy.
Bastion Host	TCP	22	Allow inbound SSH from Bastion.
Proxy Host(s)	TCP	8443	Allow inbound HTTPS from Proxy.

Outbound

Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet
Kubectl Host(s)	TCP	22	Allow outbound SSH to Kubectl hosts.
Proxy Host(s)	TCP	22	Allow outbound SSH to Proxy hosts.

Kubectl Host Security Group

Inbound

Source	Protocol	Port Range	Comments
Orchestrator Hosts(s)	TCP	22	Allow inbound SSH from Bastion.

Outbound

Destination	Protocol	Port Range	Comments
192.168.0.0/16	TCP	22	Allow outbound SSH access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to anywhere

(Top)

Kubernetes VPC

Kubernetes Route Tables

============

(Top)

Guidance: Route tables should be applied to network subnets. They are required to ensure correct traffic routing and require explicitly described inbound and outbound rules.

Kubernetes Private Subnet Route Table

Destination	Target
192.168.0.0/16	Local
0.0.0.0/0	NAT Gateway
172.16.0.0/16	Peering Link

Kubernetes Public Subnet Route Table

Destination	Target
192.168.0.0/16	Local
0.0.0.0/0	Internet Gateway
172.16.0.0/16	Peering Link

Kubernetes ACL Definitions

===============

([Top](#))

Guidance: Access Control Lists (ACL) should be applied to network subnets. They are stateless and require explicitly described inbound and outbound rules.

ACL Rules for the Kubernetes Public Subnet

Inbound

Rule	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	0.0.0.0/0	TCP	443	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
130	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from hosts on the Internet that are responding to requests originating in the subnet.
140	172.16.10.0/24	TCP	22	ALLOW	Allows inbound SSH traffic from hosts in the NOC VPC private subnet
*	0.0.0.0/0	all	all	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows outbound HTTP traffic from the subnet to the Internet.
110	0.0.0.0/0	TCP	443	ALLOW	Allows outbound HTTPS traffic from the subnet to the Internet.
120	0.0.0.0/0	TCP	32768-65535	ALLOW	Allows outbound responses to clients on the Internet
130	172.16.10.0/24	TCP	1024-65535	ALLOW	Allows inbound return traffic from hosts in the NOC VPC private subnet
*	0.0.0.0/0	all	all	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

ACL Rules for the Kubernetes Private Subnet A

Inbound

Rule	Source IP	Protocol	Port	Allow/Deny	Comments

Rule	Source IP	Protocol	Port	Allow/Deny	Comments
100	172.16.10.0/24	TCP	22	ALLOW	Allows inbound SSH traffic from hosts in the NOC VPC private subnet
110	172.16.10.0/24	TCP	443	ALLOW	Allows inbound HTTPS traffic from hosts in the NOC VPC private subnet
120	192.168.20.0/24	ALL	ALL	ALLOW	Allows inbound all traffic from second availability zone for requests originating in the private subnet.
130	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from the NAT device in the public subnet for requests originating in the private subnet.
*	0.0.0.0/0	all	all	DENY	Denies all IPv4 inbound traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows outbound HTTP traffic from the subnet to the Internet.
110	0.0.0.0/0	TCP	443	ALLOW	Allows outbound HTTPS traffic from the subnet to the Internet.
120	192.168.0.0/24	TCP	32768-65535	ALLOW	Allows outbound responses to the public subnet
130	192.168.20.0/24	ALL	ALL	ALLOW	Allows outbound all traffic to second availability zone private subnet.
100	172.16.10.0/24	TCP	1024-65535	ALLOW	Allows outbound return traffic to hosts in the NOC VPC private subnet
*	0.0.0.0/0	all	all	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

ACL Rules for the Kubernetes Private Subnet B

Inbound

Rule	Source IP	Protocol	Port	Allow/Deny	Comments
100	172.16.10.0/24	TCP	22	ALLOW	Allows inbound SSH traffic from hosts in the NOC VPC private subnet
110	172.16.10.0/24	TCP	443	ALLOW	Allows inbound HTTPS traffic from hosts in the NOC VPC private subnet
120	192.168.10.0/24	ALL	ALL	ALLOW	Allows inbound all traffic from first availability zone for requests originating in the private subnet.
130	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from the NAT device in the public subnet for requests originating in the private subnet.
*	0.0.0.0/0	all	all	DENY	Denies all IPv4 inbound traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments

Rule	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	ALLOW	Allows outbound HTTP traffic from the subnet to the Internet.
110	0.0.0.0/0	TCP	443	ALLOW	Allows outbound HTTPS traffic from the subnet to the Internet.
120	192.168.0.0/24	TCP	32768-65535	ALLOW	Allows outbound responses to the public subnet
130	192.168.10.0/24	ALL	ALL	ALLOW	Allows outbound all traffic to first availability zone private subnet.
100	172.16.10.0/24	TCP	1024-65535	ALLOW	Allows outbound return traffic to hosts in the NOC VPC private subnet
*	0.0.0.0/0	all	all	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Kubernetes Network Security Groups

=======================

(Top)

Guidance: Network Security Groups (NSG) should be applied to host instances in AWS. They are stateful and, therefore, only need to describe specific services.

Control Plane Security Group

Inbound

Source	Protocol	Port Range	Comments
172.16.0.10/24	TCP	443	Allow inbound HTTPS from NOC VPC private subnet.
Worker Nodes	ALL	ALL	Allow inbound all traffic from worker nodes.

Outbound

Destination	Protocol	Port Range	Comments
Worker Nodes	TCP	1025-65535	Allow outbound access to the worker nodes
Worker Nodes	TCP	443	Allow outbound access to the anywhere ?? needed

Worker Nodes Security Group

Inbound

Source	Protocol	Port Range	Comments
172.16.0.10/24	TCP	22	Allow inbound SSH from NOC VPC private subnet.
Control Plane	TCP	443	Allow inbound HTTPS from Control Plane.
Worker Nodes	ALL	ALL	Allow inbound all traffic from worker nodes.
Control Plane	TCP	1025-65535	Allow inbound ephemeral ports from Control Plane.

Outbound

Destination	Protocol	Port Range	Comments
Control Plane	TCP	443	Allow outbound HTTPS access to the Control Plane
0.0.0.0/0	ALL	ALL	Allow outbound access to the anywhere

(Top)

▶

⚠ ✕ You can’t perform that action at this time.
Press h to open a hovercard with more details.