Running Cisco DCNM Behind a Firewall

This chapter provides information about running Cisco DCNM behind a firewall.

Running Cisco DCNM Behind a Firewall

Generally, an Enterprise (external world) and Data center is separated by a firewall, i.e., DCNM is configured behind a firewall. The Cisco DCNM Web Client and SSH connectivity must pass-through that firewall. Also, a firewall can be placed between the DCNM Server and DCNM-managed devices.

All Cisco DCNM Native HA nodes must be on the same side of the firewall. The internal DCNM Native HA ports are not listed, as it is not recommended to configure a firewall in between the Native HA nodes.

Note When you add or discover LAN devices in DCNM, java is used as a part of the discovery process. If firewall blocks the process then it uses TCP connection port 7 as a discovery process. Ensure that the **cdp.discoverPingDisable** server property is set to **true**. Choose **Web UI > Administration > DCNM Server > Server Properties** to set the server property.

Any standard port where the Ingress traffic enters from clients cannot be modified unless you disable the local firewall.

The following table lists all ports that are used for communication between Cisco DCNM Web Client, SSH Client, and Cisco DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Client to DCNM Server	SSH access to external world is optional.
443	TCP	HTTPS	Client to DCNM Server	This is needed to reach DCNM Web Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
2443	TCP	HTTPS	Client to DCNM Server	Required during installation, to reach the server. DCNM closes this port after installation completes.

The following table lists all ports that are used for communication between Cisco DCNM Server and other services.

Note The services can be hosted on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
49	TCP/UDP	TACACS+	DCNM Server to DNS Server	ACS Server can be either side of the firewall.
53	TCP/UDP	DNS	DCNM Server to DNS Server	DNS Server can be either side of the firewall.
123	UDP	NTP	DCNM Server to NTP Server	NTP Server can be either side of the firewall.
5000	TCP	Docker Registry	Incoming to DCNM Server	Docker Registry Service on DCNM Server listening to requests from DCNM compute nodes.
5432	TCP	Postgres	DCNM Server to Postgres DB Server	Default installation of DCNM does not need this port. This is needed only when Postgres is installed external to the DCNM host machine.

The following table lists all ports that are used for communication between DCNM Server and managed devices:

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Both Direction	DCNM Server to Device – To manage devices. Device to DCNM Server – SCP (POAP).
67	UDP	DHCP	Device to DCNM Server	
69	TCP	TFTP	Device to DCNM Server	Required for POAP
161	TCP/UDP	SNMP	Server to DCNM Device	DCNM configured via `server.properties` to use TCP uses TCP port 161, instead of UDP port 161.
514	UDP	Syslog	Device to DCNM Server	
2162	UDP	SNMP_TRAP	Device to DCNM Server	
33000-33499	TCP	gRPC	Device to DCNM Server	LAN Telemetry Streaming

Configuring Custom Firewalls

Note This is applicable for DCNM OVA/ISO deployments only.

Cisco DCNM Server deploys a set of IPTables rules, known as DCNM Local Firewall. These rules open TCP/UDP ports that are required for Cisco DCNM operations. You can't manipulate the built-in Local Firewall without accessing the OS interface, through SSH, and change the rules. Don't change the Firewall rules, as it may become vulnerable to attacks, or impact the normal functioning of DCNM.

To cater to a given deployment or a network, Cisco DCNM allows you to configure your own firewall rules, from Release 11.3(1), using CLIs.

Note These rules can be broad or granular, and supersedes the built-in Local Firewall rules. Therefore, configure these rules carefully, during a maintenance period.

You don't need to stop or restart DCNM server or applications to configure custom firewalls.

Caution IPTable prioritizes the rules in the order that they are configured. Therefore, more granular rules must be installed in the beginning. To ensure that the order of the rules is as required, you can create all rules in a text editor, and then execute the CLIs in the desired order. If rules need to be adjusted, you can flush all rules and configure the rules in the desired order.

You can perform the following operations on the Custom Firewalls.

Note Run all the commands on the Cisco DCNM server using SSH.

Custom Firewall CLI

View the custom firewall CLI chain help and examples using the **appmgr user-firewall** command.

```
dcnm# appmgr user-firewall
dcnm# appmgr user-firewall – h
```

Configure Rules for Custom Firewall

Configure the custom firewall rules using the **appmgr user-firewall {add | del}** command.

```
appmgr user-firewall {add|del} proto {tcp|udp} port {<port><port range n1:n2>}
[{in|out} <interface name>] [srcip <ip-address> [/<mask>]] [dstip <ip-address> [/<mask>]]
action {permit|deny}
```

Note The custom firewall rules supersede the local Firewall rules. Therefore, be cautious and ensure that the functionalities aren't broken.

Example: Sample Custom Firewall Rules

- `dcnm# appmgr user-firewall add proto tcp port 7777 action deny`

  This rule drops all TCP port 7777 traffic on all interfaces.

- `dcnm# appmgr user-firewall add proto tcp port 443 in eth1 action deny`

  This rule drops all TCP port 443 incoming traffic on interface eth1.

- `dcnm# appmgr user-firewall add proto tcp port 7000:7050 srcip 1.2.3.4 action deny`

  This rule drops TCP port range 10000-10099 traffic coming from IP address 1.2.3.4.

Preserving Custom Firewall Rules

Preserve the custom firewall rules across reboots, using the **appmgr user-firewall commit** command.

Note Each time you modify the rules, you must execute this command to preserve the rules across reboots.

Installing Custom Firewall Rules on Native HA Standby Node

In a Cisco DCNM Native HA setup, when you execute the **appmgr user-firewall commit** on the Active node, the rules are synchronized to the Standby node automatically. However, the new rules are operational only after a system reboot.

To apply the rules immediately, install the custom firewall rules on Standby node using the **appmgr user-firewall user-policy-install** command.

Deleting Custom Firewalls

Delete all the custom firewalls using the **appmgr user-firewall flush-all** command.

To delete the custom firewalls permanently, use the **appmgr user-firewall commit** command.