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, ICMP echo packets are sent as part of the discovery process. If you have a firewall that blocks ICMP messages, the discovery process fails. You can skip sending the ICMP echo packets by setting the **cdp.discoverPingDisable** server property to **true**. For more information about how to set a server property, Cisco DCNM Web UI **Administration > DCNM Server > Server Properties**.

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.

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).

Port Number	Protocol	Service Name	Direction of Communication	Remarks
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

Running Cisco DCNM Behind a Firewall