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 Datacenter is separated by a firewall, i.e., DCNM is configured behind a firewall. The Cisco DCNM Web Client, Cisco DCNM SAN Client, and Cisco Device Manager connectivity will pass-through that firewall. A firewall can be placed between the DCNM Server and DCNM-managed devices also.

Beginning with Cisco DCNM Release 11.0(1), DCNM SAN Client initiates communication with DCNM SAN Server on HTTPS port 443. However, both DCNM SAN Client and Device Manager communicate with the devices directly also. Device Manager can be invoked through DCNM SAN Server UI and it runs within the context of the DCNM SAN Server. The Device Manager communication with devices remains same, as if it was running independently.

DCNM SNMP proxy services on DCNM SAN Server use a configurable TCP port (9198 by default) for SNMP communications between the DCNM SAN Client or Device Manager, and DCNM Server.

Performance Manager uses TCP, by default, for data collections.

The UDP SNMP_TRAP local ports are between 1163-1170, for both Cisco DCNM-SAN and Device Manager. DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses.

You can select the UDP port that the Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the `DeviceManager.bat` file in the `C:\Program Files\Cisco Systems\MDS9000\bin` directory:

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.

Note On the windows VM, run the **netstat -nab** command, to view the ports that are used by the `javaw.exe` process.

- On a LINUX desktop, uncomment the following in the `DeviceManager.sh` file in the `$HOME/.cisco_mds9000/bin` directory:

  ```
  # JVMARGS=$JVMARGS -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.

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

The eth0 (Mgmt) interface is used for DCNM Web Client, DCNM SAN Client, Device Manager, and Fabric discovery. Below table is applicable for eth0 (Mgmt).

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

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	SSH to DCNM SAN Server	SSH access to external world is optional.
443	TCP	HTTPS	Client to DCNM SAN Server	Cisco DCNM Web Client, Cisco DCNM SAN Client to the Cisco DCNM Server
1099	TCP	Java RMI	Client to DCNM SAN Server	Cisco DCNM SAN Client to Server
1163 to 1170	UDP	SNMP_TRAP	Device to SAN Client and Device Manager	Cisco DCNM SAN Client and Cisco Device Manager use same range of ports.
2443	TCP	HTTPS	Client to DCNM Server	Required during installation, to reach the server. DCNM closes this port after installation completes. Required only for DCNM SAN OVA/ISO during installation, to reach the server. DCNM SAN server closes this port after installation completes.
3528	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP

Port Number	Protocol	Service Name	Direction of Communication	Remarks
3529	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP SSL

Port Number	Protocol	Service Name	Direction of Communication	Remarks
9198	UDP/TCP	SNMP	SAN Client, Device Manager to DCNM SAN Server. Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed with the `client -Dsnmp.localport` option. Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed in `server.properties` file. DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.	Cisco DCNM SNMP proxy services use the TCP port (9198 by default) for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
61616	TCP	Messaging	DCNM SAN Client to DCNM SAN Server	

The eth0 (Mgmt) interface is used for DCNM Web Client, DCNM SAN Client, Device Manager, and Fabric discovery. Below table is applicable for eth0 (Mgmt).

The following table lists all the ports that are used for communication between the Cisco DCNM Server and other services which can be hosted on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
49	TCP/UDP	TACACS+	Cisco DCNM SAN Server to ACS Server	ACS Server can be on either side of the firewall.
53	TCP/UDP	DNS	Cisco DCNM SAN Server to DNS Server	DNS Server can be on either side of the firewall.
123	UDP	NTP	Cisco DCNM SAN Server to NTP Server	NTP Server can be on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
1521	TCP	Oracle	DCNM SAN Server to the Oracle database Server	This is necessary if the Oracle server is installed external to the DCNM host machine. Oracle server may be configured to listen on a different port and in that case that port in question must be taken into account. **Note** You can choose the Oracle server port during DCNM SAN installation and must not be modified later, after installation.
5432	TCP	Postgres	Cisco DCNM SAN Server to Postgres Server	The default installation of DCNM does not need this port. This is necessary if Postgres is installed externally to the DCNM host machine.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
9198	UDP\TCP	SNMP	DCNM SAN Client, Device Manager to DCNM SAN Server	

Port Number	Protocol	Service Name	Direction of Communication	Remarks
				Cisco DCNM SNMP proxy services use the TCP port (9198 by default) on DCNM SAN Server for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server. Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed with the client -Dsnmp.localportoption. Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed in the server.properties file. DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach the managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM

Port Number	Protocol	Service Name	Direction of Communication	Remarks
				SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.

The eth1 (Enhanced fabric mgmt out-of-band) interface is used for Trap, Event, Alarm, Syslog, SCP, SFTP, TFTP, Config Archive, ISSU, SAN Insights. Below table is applicable for eth1 (Enhanced fabric mgmt out-of-band).

The following table lists all the ports that are used for communication between Cisco DCNM Server and Managed devices.

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

Port Number	Protocol	Service Name	Direction of Communication	Remarks
5989	TCP	SMI-S Agent	Both direction	Server to Device. This is where the Storage device listens. An application to DCNM Server – When DCNM Server is acting as storage proxy. Server to the Storage device port number is depended upon where the storage device is listening on. It could be 5989, 5888, or other ports.
33000	TCP	gRPC	Device to DCNM SAN Server	SAN 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.