ファイアウォール背後での Cisco DCNM の実行

この章では、ファイアウォールの背後で Cisco DCNM を実行する方法について説明します。

ファイアウォール背後での Cisco DCNM の実行

通常、企業(外部)およびデータセンターはファイアウォールによって分離されます。つまり、DCNM はファイアウォールの背後に設定されます。Cisco DCNM Web クライアント、 Cisco DCNM SAN クライアント、Cisco デバイス マネージャ接続はファイアウォールを通過します。また、ファイアウォールは、DCNM サーバと DCNM 管理対象デバイスの間に配置できます。

Cisco DCNM リリース 11.0(1) 以降では、DCNM SAN クライアントは、HTTPS ポート 443 で DCNM SAN サーバとの通信を開始します。ただし、DCNM SAN クライアントとデバイス マネージャは両方ともデバイスと直接通信します。デバイス マネージャは DCNM SAN サーバ UI を使用して起動でき、DCNM SAN サーバのコンテキスト内で動作します。デバイス マネージャとデバイスとの通信は、個別に実行されている場合と同様に変わりません。

DCNM SNMP サーバの DCNM SNMP プロキシ サービスは、DCNM SAN クライアントまたはデバイス マネージャ、DCNM サーバの間の SNMP 通信に設定可能な TCP ポート (デフォルトは 9198) を使用します。

Performance Managerは、データ収集にデフォルトでTCPを使用します。

UDP SNMP_TRAP ローカル ポートは、Cisco DCNM-SAN およびデバイス マネージャの両方で 1163 ～ 1170 の間です。Cisco DCNM-SAN Client および Device Manager は、使用可能な最初の UDP ポートを使用して、SNMP 応答を送受信します。

次のステートメントのコメント解除によって、デバイス マネージャが SNMP 応答に使用する UDP ポートを選択できます。

ファイアウォール背後での Cisco DCNM の実行

- Windows デスクトップでは、C:\Program Files\Cisco Systems\MDS9000\bin ディレクトリの DeviceManager.bat ファイル内の次のステートメントをアンコメントします。

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

[localport] が空いているローカル ポートの値の場合。

Note Windows VM で **netstat -nab** コマンドを実行して、javaw.exe プロセスで使用されているポートを表示します。

- LINUX デスクトップでは、$HOME/.cisco_mds9000/bin ディレクトリの DeviceManager.sh ファイル内の次のステートメントをアンコメントします。

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

[localport] が空いているローカル ポートの値の場合。

入力トラフィックがクライアントから入力される場合のスタンダードポートは、ローカルファイアウォールを無効にするまで変更できません。

eth0（Mgmt）インターフェイスは、DCNM Web クライアント、DCNM SAN クライアント、デバイス マネージャ、およびファブリック ディスカバリに使用されます。以下の表は、eth0（Mgmt）に適用されます。

次の表に、DCNM Web クライアント、DCNM SAN クライアント、デバイス マネージャ、SSH クライアント、およびDCNM サーバ間の通信に使用されるすべてのポートの一覧を示します。

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
22	TCP	SSH	SSH から DCNM SAN サーバ	外部への SSH アクセスはオプションです。
443	TCP	HTTPS	クライアントから DCNM SAN サーバ	Cisco DCNM Web クライアント、Cisco DCNM SAN クライアントから Cisco DCNM サーバ
1099	TCP	Java RMI	クライアントから DCNM SAN サーバ	Cisco DCNM SAN クライアントからサーバ

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
1163 ~ 1170	UDP	SNMP_TRAP	デバイスから SAN クライアントおよびデバイス マネージャ	Cisco DCNM SAN クライアントと Cisco デバイス マネージャは、同じ範囲のポートを使用します。
2443	TCP	HTTPS	クライアントから DCNM サーバ	サーバに到達するために、インストール中に必要です。インストール完了後、DCNM はポートを閉じます。 サーバに到達するために、インストール中に DCNM SAN OVA/ISO にのみ必要です。DCNM SAN サーバは、インストールが完了した後このポートを閉じます。
3528	[TCP]	JBOSS	クライアントから DCNM SAN サーバ	Wildfly JBOSS CORBA-IIOP
3529	[TCP]	JBOSS	クライアントから DCNM SAN サーバ	Wildfly JBOSS CORBA-IIOP SSL

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
9198	UDP/TCP	SNMP		Cisco DCNM SNMP プロキシサービスは、Cisco DCNM SAN クライアントまたは Cisco デバイスマネージャと Cisco DCNM サーバ間の SNMP 通信に TCP ポート (デフォルトでは 9198) を使用します。

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
			SAN クライアント、デバイス マネージャから DCNM SAN サーバ SNMP プロキシが使用可能な場合は、Cisco DCNM SAN クライアントが空いているローカル ポート（UDP）または 9198（TCP）をランダムに選択します。ポートは、`client -Dsnmp.localport` を使用して変更できます。 SNMP プロキシが使用可能な場合は、Cisco デバイス マネージャが空いているローカル ポート（UDP）または 9198（TCP）をランダムに選択します。ポートは、`server.properties` ファイルで変更できます。 DCNM SNMP プロキシは、SAN クライアントまたはデバイス マネージャが管理対象デバイスに直接到達できず、管理対象デバイスから DCNM SAN サー	

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
			バに送信される SNMP 応答を SAN クライアントおよびデバイス マネージャにリレーできる場合に使用されます。DCNM SAN クライアントとデバイス マネージャは、SNMP 応答を取得するために DCNM SAN サーバ ポート 9198 (または任意のポートが設定されている) に到達する必要があります。	
61616	[TCP]	メッセージ	DCNM SAN クライアントから DCNM SAN サーバ	

eth0（Mgmt）インターフェイスは、DCNM Web クライアント、DCNM SAN クライアント、デバイス マネージャ、およびファブリック ディスカバリに使用されます。以下の表は、eth0 (Mgmt) に適用されます。

次の表に、Cisco DCNM サーバと、ファイアウォールのどちらかでホスト可能なその他のサービス間の通信に使用されるすべてのポートを一覧表示します。

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
49	TCP/UDP	TACACS+	Cisco DCNM SAN サーバから ACS サーバ	ACS サーバは、ファイアウォールのいずれかの側になります。
53	TCP/UDP	DNS	Cisco DCNM SAN サーバから DNS サーバ	DNS サーバは、ファイアウォールのいずれかの側になります。

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
123	UDP	NTP	Cisco DCNM SAN サーバから NTP サーバ	NTP サーバは、ファイアウォールのいずれかの側になります。

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
1521	TCP	Oracle	DCNM SAN サーバから Oracle データベース サーバ	これは、Oracle サーバが DCNM ホスト マシンの外部にインストールされている場合に必要です。Oracle サーバは、別のポートでリッスンするように設定されている場合があります。その場合は、対象のポートを考慮する必要があります。 **Note** DCNM SAN のインストール時に Oracle サーバ ポートを選択できます。インストール後や後で変更することはできません。

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
5432	TCP	postgres	Postgres サーバへの Cisco DCNM SAN サーバ	DCNM のデフォルト インストールでは、このポートは必要ありません。 これは、Postgres が DCNM ホスト マシンの外部にインストールされている場合に必要です。

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
9198	UDP/TCP	SNMP	DCNM SAN クライアント、デバイス マネージャから DCNM SAN サーバ	

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
				Cisco DCNM SNMP プロキシサービスは、Cisco DCNM SAN クライアントまたは Cisco デバイスマネージャと Cisco DCNM サーバ間の SNMP 通信のため、DCNM SAN サーバで TCP ポート (デフォルトでは 9198) を使用します。 SNMP プロキシに到達するために、Cisco DCNM SAN クライアントが空いているローカルポート（UDP）または 9198（TCP）をランダムに選択します。ポートは、client -Dsnmp.localportoption を使用して変更できます。 SNMP プロキシに到達するために、Cisco デバイス マネージャが空いているローカルポート（UDP）または 9198（TCP）をランダムに選択します。ポートは、server.properties ファイルで変更できます。 DCNM SNMP プ

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
				ロキシは、SAN クライアントまたはデバイス マネージャが管理対象デバイスに直接到達できず、管理対象デバイスから DCNM SAN サーバに送信される SNMP 応答を SAN クライアントおよびデバイス マネージャにリレーできる場合に使用されます。DCNM SAN クライアントとデバイス マネージャは、SNMP応答を取得するために DCNM SAN サーバ ポート 9198 (または任意のポートが設定されている) に到達する必要があります。

eth1（拡張ファブリック管理アウトオブバンド）インターフェイスは、トラップ、イベント、アラーム、Syslog、SCP、SFTP、TFTP、構成アーカイブ、ISSU、SAN Insights に使用されます。以下の表は、eth1（拡張ファブリック管理アウトオブバンド）に適用されます。

次の表に、Cisco DCNM サーバと管理対象デバイス間の通信に使用されるすべてのポートの一覧を示します。

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
22	TCP	SSH	両方向	サーバからデバイス：デバイス管理用。 デバイスからサーバ：SCP (POAP)

ファイアウォール背後での Cisco DCNM の実行

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
67	UDP	DHCP	デバイスから DCNM SAN サーバ	
69	TCP	TFTP	デバイスから DCNM SAN サーバ	POAP に必須
161	TCP/UDP	SNMP	DCNM SAN サーバからデバイス	UDP ポート 161 の代わりに、ポート 161 で TCP を使用するために server.properties 経由で設定されている Cisco DCNM
514	UDP	Syslog	デバイスから DCNM SAN サーバ	
2162	UDP	SNMP_TRAP	デバイスから DCNM SAN サーバ	

ポート番号	プロトコル	Service Name	コミュニケーション方向	備考
5989	TCP	SMI-S エージェント	両方向	サーバからデバイスへ。これは、ストレージデ バイスがリッスンする場所です。 アプリケーションから DCNM サーバ：DCNM サーバがストレージ プロキシとして動作している場合。 サーバからのストレージ デバイス ポート番号は、ストレージ デバイスがリッスンしている場所によって異なります。5989、5888、またはその他のポートである可能性があります。
33000	TCP	gRPC	デバイスから DCNM SAN サーバ	SAN テレメトリ ストリーミング

カスタム ファイアウォールの設定

（注） これは、DCNM OVA/ISO 展開にのみ適用されます。

Cisco DCNM サーバは、DCNM ローカル ファイアウォールと呼ばれる IPTables ルールのセットを展開します。これらのルールは、Cisco DCNM 操作に必要な TCP/UDP ポートを開きます。OS インターフェイスにアクセスし、SSH を経由して、ルールを変更することなく内蔵ローカル ファイアウォールを操作することはできません。攻撃に対して脆弱になったり、DCNM の通常の機能に影響を及ぼす可能性があるため、ファイアウォール ルールを変更しないで下さい。

指定の展開またはネットワークに対応するため、Cisco DCNM では CLI を使用してリリース 11.3(1) から独自のファイアウォール ルールを設定できます。

（注） これらのルールは幅広いか粒度が細かく、内蔵ローカル ファイアウォール ルールを優先します。したがって、メンテナンス期間はこれらのルールを慎重に設定します。

カスタム ファイアウォールを設定するために、 DCNM サーバまたはアプリケーションを停止または再起動する必要はありません。

注意 IPTable は、設定している順番でルールに優先順位を付けます。従って、最初により粒度の細かいルールをインストールする必要があります。ルールの順番が要求通りにするため、テキスト エディタにすべてのルール作成し、希望の順番で CLI を実行することができます。ルールを調整する必要がある場合、すべてのルールを取り消し、希望の順番でルールを設定できます。

カスタム ファイアウォールで次の操作を実行できます。

（注） SSH を使用して Cisco DCNM サーバですべてのコマンドを実行します。

カスタム ファイアウォール CLI

appmgr user-firewall コマンドを使用して、カスタム ファイアウォール CLI チェーン ヘルプと例を表示します。

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

カスタム ファイアウォールのルールを設定する

appmgr user-firewall {add | del} コマンドを使用して、カスタム ファイアウォール ルールを設定します。

```
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}
```

（注） カスタム ファイアウォール ルールは、ローカル ファイアウォール ルールを優先します。従って、機能が破損していないか注意して確認します。

例：例のカスタム ファイアウォール ルール

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

このルールは、すべてのインターフェイスですべての TCP ポート 7777 トラフィックをドロップします。

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

  このルールは、インターフェイス eth1 ですべての TCP ポート 443 着信トラフィックをドロップします。

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

  このルールは、IP アドレス 1.2.3.4. から発信されている TCP ポート範囲 10000 ～ 10099 t トラフィックをドロップします。

カスタム ファイアウォール ルールの保持

appmgr user-firewall commit コマンドを使用して、再起動時にカスタム ファイアウォール ルールを保持します。

（注） ルールを変更するたびにこのコマンドを実行して、再起動時にルールを保持する必要があります。

ネイティブ HA スタンバイ ノードでカスタム ファイアウォール ルールをインストールする

Cisco DCNM ネイティブ HA セットアップでは、アクティブ ノードで **appmgr user-firewall commit** を実行するとき、ルールがスタンバイ ノードに自動的に同期されます。ただし、新しいルールはシステム再起動後にのみ動作します。

ルールをすぐに適用するには、**appmgr user-firewall user-policy-install** コマンドを使用してスタンバイ ノードでカスタム ファイアウォール ルールをインストールします。

カスタム ファイアウォールの削除

appmgr user-firewall flush-all コマンドを使用して、すべてのカスタム ファイアウォールを削除します。

カスタム ファイアウォールを永久に削除するには、**appmgr user-firewall commit** コマンドを使用します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。