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 クライアントと SSH 接続は、そのファイアウォールを通過する必要があります。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。

すべての Cisco DCNM ネイティブ HA ノードは、ファイアウォールの同じ側にある必要があります。内部 DCNM ネイティブ HA ポートは一覧表示されていません。ネイティブ HA ノード間でファイアウォールを設定することは推奨されていません。

Note DCNM で LAN デバイスを追加または検出すると、検出プロセスの一部として java が使用されます。ファイアウォールがプロセスをブロックすると、TCP 接続ポート 7 が検出プロセスとして使用されます。**cdp.discoverPingDisable** サーバ プロパティが **true** に設定されていることを確認します。**[Web UI]**、**[Administration]**、**[DCNM Server]**、**[Server Properties]** の順に選択して、サーバ プロパティを設定します。

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。

次の表に、Cisco DCNM Web クライアント、SSH クライアント、および Cisco DCNM サーバ間の通信に使用されるすべてのポートを示します。

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
22	TCP	SSH	クライアントから DCNM 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 サーバ	これは DCNM Web サーバに到達するために必要です。
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。

次の表に、Cisco DCNM サーバと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示します。

Note サービスは、ファイアウォールのいずれかの側でホストできます。

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+	DNS サーバから DCNM 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	DNS サーバから DCNM 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。
123	UDP	NTP	DCNM 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
5000	TCP	Docker レジストリ	DCNM サーバへの着信	DCNM コンピューティングノードからの要求をリッスンしている DCNM サーバ上の Docker レジストリ サービス。
5432	TCP	postgres	DCNM サーバから Postgres DB 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のみ必要です。

次の表に、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	DCNM サーバからデバイス：デバイス管理用。 デバイスから DCNM サーバ：SCP (POAP)。
67	UDP	DHCP	デバイスから DCNM サーバ	
69	TCP	TFTP	デバイスから DCNM サーバ	POAP に必須

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
161	TCP/UDP	SNMP	サーバから DCNM デバイス	TCP を使用するための server.properties 経由で設定されている DCNM は、UDP ポート 161 の代わりに TCP ポート 161 を使用します。
514	UDP	Syslog	デバイスから DCNM サーバ	
2162	UDP	SNMP_TRAP	デバイスから DCNM サーバ	
33000 ～ 33499	TCP	gRPC	デバイスから DCNM サーバ	LAN 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。