# 使用する前に



## 適切な移行プロセスの選択

Cisco Defense Orchestrator（CDO）を使用して適応型セキュリティアプライアンス（ASA）の設定を FDM による管理 デバイスに移行するには、2 つの方法があります。

- CDO ソリューション：ASA 設定を FDM による管理 デバイスに移行し、FTD デバイスを CDO および Firepower Device Manager で管理する場合は、CDO でクラウドベースのプロセスを使用して ASA 設定を移行します。
- オンプレミスソリューション（Firepower Device Manager）：ASA 設定を FDM による管理 デバイスに移行する場合は、CDO でクラウドベースのプロセスを使用して ASA 設定を移行します。その後、Firepower Device Manager を使用して構成を管理できます。

このガイドは、読者が CDO 操作の基本を理解していることを前提としています。詳細については、『CDO Data Sheet』を参照してください。

## Cisco Defense Orchestrator の移行プロセスについて

CDO は、適応型セキュリティアプライアンス（ASA）を FDM による管理 デバイスに移行するのに役立ちます。CDO には、ASA の実行構成を FDM テンプレートに移行するための [ASA からFDMに移行（ASA to FDM Migration）] ウィザードが用意されています。

（注） [ツールとサービス（Tools & Services）] で [ASAからFDMに移行（ASA to FDM Migration）] オプションを表示するには、show-fdm および enable-asa-to-ftd-migration 機能フラグを有効にする必要があります。 [ツールとサービス（Tools & Services）] で利用できない場合は、TAC に連絡して、[ASAからFDMに移行（ASA to FDM Migration）] オプションをアクティブにします。

[ASAからFDMに移行（ASA to FDM Migration）] ウィザードを使用して、ASA の実行設定の次の要素を FDM テンプレートに移行できます。

- インターフェイス
- ルート
- アクセス制御ルール（ACL）
- ネットワークアドレス変換（NAT）ルール
- ネットワークオブジェクトとネットワーク グループ オブジェクト

（注） CDOは、予約済みキーワードを含むオブジェクト名をサポートしていません。オブジェクト名を、「ftdmig」というサフィックスを追加して変更してください。

- サービスオブジェクトとサービス グループ オブジェクト
- サイト間 VPN

CDO は、参照されたオブジェクトのみを移行します。アクセス制御リスト内で、定義されているがアクセスグループに参照されていないオブジェクトは移行されません。CDO が特定の要素の移行に失敗する一般的な理由には、次の 1 つ以上が当てはまる場合があります。

- ICMP コードのない ICMP アクセスリスト
- TCP/UDP アクセスリストにアクセスグループが設定されていない
- IP アクセスリストがサイト間 VPN プロファイルにマップされていない
- アクセスリストを参照するネットワークオブジェクトまたはグループのいずれかが移行されていない
- インターフェイスがシャットダウンとして参照される

（注） 構成内の参照されていないオブジェクトまたはオブジェクトグループも削除され、移行中に未使用としてマークされます。移行されていない要素の詳細については、「移行レポート」を参照してください。

ASA実行構成のこれらの要素をFDMテンプレートに移行したら、そのFDMテンプレートを、CDOによって管理される新しいFDMによる管理 デバイスに適用できます。FDMによる管理デバイスはテンプレートで定義された構成を採用するため、FDMによる管理はASAの実行構成のいくつかの側面を使用して構成されるようになりました。

ASA実行コンフィギュレーションの他の要素は、このプロセスを使用して移行されません。これらの他の要素は、FDMテンプレートでは空の値で表されます。テンプレートがFDMによる管理デバイスに適用されると、移行された値が新しいデバイスに適用され、空の値は無視されます。新しいデバイスの他のデフォルト値は、すべて保持されます。移行されなかったASA実行コンフィギュレーションのその他の要素は、移行プロセス以外でFDMによる管理 デバイスで再作成する必要があります。

# 移行プロセスのライセンス

FDMによる管理 デバイス移行プロセスはCDOの一部であり、CDOライセンス以外の特定のライセンスは必要ありません。

# 注意事項と制約事項

（注） CDOでサポートされていない設定は、移行中に**サポート対象外**として削除され、**移行レポート**で報告されます。

| 機能名 | 移行できるもの | 移行に関する制限 |
|---|---|---|
| ファイアウォールモード | ルーテッドファイアウォール モード | トランスペアレントモードの設定は移行できません。 |

| 機能名 | 移行できるもの | 移行に関する制限 |
| --- | --- | --- |
| インターフェイス設定 | • 物理インターフェイス<br>• サブインターフェイス | • FDMによる管理デバイスには、移行するASA インターフェイスの設定と同等以上の物理インターフェイスが必要です。<br>• サブインターフェイス（サブインターフェイス ID は移行時の VLAN ID と同じ番号に常に設定されます）<br>• 次のインターフェイス設定はFDMによる管理 デバイスに移行されません。<br>  • ASA インターフェイスのセカンダリ VLAN<br>  • Redundant Interface<br>  • □ブリッジ グループ インターフェイス<br>  • 仮想トンネル インターフェイス |

| 機能名 | 移行できるもの | 移行に関する制限 |
|---|---|---|
| EtherChanel | 物理インターフェイスで設定された EtherChannel。<br><br>EtherChanel にマッピングされたメンバーインターフェイスは、移行中も保持されます。 | • 設定を移行する前に、CDO を使用して FDM による管理 デバイスに同等の数の EtherChannel を作成する必要があります。「FDM 管理対象デバイスの EtherChannel インターフェイスの追加」を参照してください。<br><br>• Firepower 1000 または 2100 シリーズのハードウェアデバイス（1010、1120、1140、1150、2110、2120、2130、2140）の設定にのみ移行できます。<br><br>• EtherChannel 設定を、ASA 8.4+ からソフトウェアバージョン 6.5+ で動作する FDM による管理 デバイスに移行できます。<br><br>• 移行前に FDM による管理 デバイスで作成されている EtherChannel は、移行される EtherChannel と同じタイプである必要があります。<br><br>CDO が移行するのは、EtherChannel から EtherChannel へ、および物理インターフェイスから物理インターフェイスへのみです。<br><br>• FDM テンプレートで EtherChannel にマッピングされたメンバーインターフェイスを、移行ウィザードのインターフェイス マッピング ステップでユーザーが使用することはできません。ただし、それらは保持され、割り当てられた EtherChannel に移行されます。 |
| ルーティング | スタティック ルート | • 同じネットワークを宛先とする静的ルートが複数ある場合、最小のメトリック値を持つ 1 つのルートのみが移行され、その他のルートはドロップされます。<br><br>• 次のルート機能は FDM による管理 デバイスに移行されません。<br><br>  • トンネルルート<br><br>  • Null 0 インターフェイスルート<br><br>  • SLA トラックを持つ静的ルート |

| 機能名 | 移行できるもの | 移行に関する制限 |
| --- | --- | --- |
| アクセス制御ルール（ACL） | • 有効化されたアクセス制御ルール<br>• 送信元オブジェクトと宛先オブジェクト<br>• CDO は、FDM による管理デバイスの許可、信頼、ブロックなどのアクションをサポートしています。移行時に、移行元の ASA の設定における許可アクションと拒否アクションが処理され、CDO で FDM による管理 デバイスに関してサポートされているアクションにマッピングされます。<br>• CDOは、ポリシー、インターフェイス、またはアクセスグループ（IP プロトコルを持たない）に付加された ACL の移行をサポートしています。<br>• 非暗号化 L3 トンネル プロトコルを使用した ACE | 次の ACL 機能は FDM による管理 デバイスに移行されません。<br>• CDO と Firepower Device manager は、IPv4 と IPv6 の混在プロトコルを使用した ACL をサポートしていません。<br>• 重大度情報のロギング<br>• 非アクティブのルールまたは無効化されたルール<br>• TCP、UDP、または ICMP 以外のプロトコルを持つサービスオブジェクトまたはサービスグループを使用した ACE<br>• TCP または UDP 以外のサービスオブジェクトを使用した ACE<br>• インラインオブジェクトを使用した ACE の TCP または UDP 以外のプロトコル<br>• 時間範囲を使用した ACE<br>• アクセスグループを使用してマッピングされていないアクセスリスト |

| 機能名 | 移行できるもの | 移行に関する制限 |
| --- | --- | --- |
| ネットワークアドレス変換（NAT）ルール | • ネットワークオブジェクト（自動）および Twice（手動）NAT または PAT<br>• スタティック NAT<br>• ダイナミック NAT または PAT<br>• アイデンティティ NAT<br>• 送信元ポート（サービス）変換 | 次の NAT ルール機能は FDM による管理 デバイスに移行されません。<br>• PAT プール<br>• 単一方向（Unidirectional）<br>• 非アクティブ<br>• Twice NAT の場合、宛先ポート（サービス）変換のための**宛先**サービスオブジェクトの使用（送信元と宛先の両方を持つサービスオブジェクトを含む）<br>• 宛先ポート変換<br>• NAT46、NAT64<br>（注） CDO は、0.0.0.0/32 のネットワークオブジェクトをサポートしていません。 |
| サービスオブジェクトとサービス グループ オブジェクト | サービスオブジェクトとネストされたグループ<br>CDO がサポートしているサービスオブジェクトで使用されるプロトコルのリストについては、「CDO 上の対応 IP プロトコル」を参照してください。 | • プロトコル、BCC-RCC-MON、および BBN-RCC-MON はサポートされていません。<br>• 「より小さい（less than）」、「より大きい（greater than）」、「等しくない（not equal to）」などの演算子はサポートされていません。<br>• オブジェクトグループのネスト |
| ネットワークオブジェクトとネットワーク グループ オブジェクト | ネットワークオブジェクトとネットワーク グループ オブジェクト | 次のネットワークオブジェクトまたはネットワークグループはサポートされていません。<br>• 不連続マスクベース<br>• IPv4 アドレスで最初のオクテットが「0」の IP アドレス |

| 機能名 | 移行できるもの | 移行に関する制限 |
|---|---|---|
| ICMP タイプ | ICMP タイプ | 次の ICMP タイプはサポートされていません。<br>• 無効な ICMP タイプまたはコードを持つ ICMP ベースのサービス オブジェクト エントリ<br>• ICMPv4 または ICMPv6 タイプのコードのないサービスタイプまたは ICMP タイプ オブジェクト<br>• 未割り当ての ICMP タイプ（IANA に従う）または無効な ICMP タイプ |
| その他のサポートされていないオブジェクト | - | 次の各種オブジェクトはサポートされていません。<br>• SGT ベースのネットワーク オブジェクト グループ<br>• ユーザーベースのネットワーク オブジェクト グループ |
| サイト間 VPN | • IKEv1 と IKEv2 の両方のフェーズ 1 およびフェーズ 2 プロポーザル<br>• IKEv1 と IKEv2 の両方の 完全転送秘密（PFS）<br>• ネストされたオブジェクトグループを使用したクリプトアクセスリスト<br>• 複数のピア IP を使用したクリプトマップ<br>• 暗号マップでトンネルに使用される IKEv1 と IKEv2 の両方 | 次のサイト間 VPN 機能はサポートしていません。<br>• vpn-filter<br>• vpn-idle-timeout<br>• isakmp keepalive threshold 10 retry 10<br>• crypto map vpnmap 200 set security-association lifetime seconds 360<br>• set security-association lifetime kilobytes unlimited<br>• set security-association lifetime seconds 3600<br>• 証明書認証<br>• ダイナミック クリプト マップ<br>• ルートベースの VPN（仮想トンネルインターフェイス） |

注意事項と制約事項の詳細については、「ASA 構成の注意事項と制約事項」および「FDM による管理 デバイスに関する注意事項と制約事項」を参照してください。

# CDO 上の対応 IP プロトコル

CDO がサービスオブジェクトでサポートする IP プロトコルは、次のとおりです。

| サービスオブジェクトの IP プロトコル | | | |
|---|---|---|---|
| 1 = ICMP | 34 = THREEPC | 73 = CPHB | 106 = QNX |
| 2 = IGMP | 35 = IDPR | 74 = WSN | 107 = AN |
| 3 = GGP | 36 = XTP | 75 = PVP | 108 = IPCOMP |
| 5 = ST2 | 37 = DDP | 76 = BRSATMON | 109 = SNP |
| 6 = TCP | 38 = IDPRCMTP | 78 = WBMON | 110 = COMPAQPEER |
| 7 = CBT | 39 = TPPLUSPLUS | 77 = SUNND | 111 = IPXINIP |
| 8 = EGP | 40 = IL | 79 = WBEXPAK | 112 = VRRP |
| 9 = IGP | 42 = SDRP | 80 = ISOIP | 113 = PGM |
| 10 = BBNRCCMON | 45 = IDRP | 81 = VMTP | 115 = L2TP |
| 11 = NVP2 | 46 = RSVP | 82 = SECUREVMTP | 116 = DDX |
| 12 = PUP | 48 = MHRP | 83 = VINES | 117 = IATP |
| 13 = ARGUS | 49 = BNA | 84 = TTP | 118 = ST |
| 14 = EMCON | 50 = ESP | 85 = NSFNETIGP | 119 = SRP |
| 15 = XNET | 51 = AH | 86 = DGP | 120 = UTI |
| 16 = CHAOS | 52 = INLSP | 87 = TCF | 121 = SMP |
| 17 = UDP | 53 = SWIPE | 88 = EIGRP | 122 = SM |
| 18 = MUX | 54 = NARP | 89 = OSPFIGP | 123 = PTP |
| 19 = DCNMEAS | 55 = MOBILE | 90 = SPRITERPC | 124 = ISIS |
| 20 = HMP | 56 = TLSP | 91 = LARP | 125 = FIRE |
| 21 = PRM | 57 = SKIP | 92 = MTP | 126 = CRTP |
| 22 = XNSIDP | 58 = IPv6-ICMP | 93 = AX25 | 127 = CRUDP |
| 23 = TRUNK1 | 59 = IPv6NONXT | 94 = IPIP | 128 = SSCOPMCE |
| 24 = TRUNK2 | 62 = CFTP | 95 = MICP | 129 = IPLT |
| 25 = LEAF1 | 64 = SATEXPAK | 96 = SCCSP | 130 = SPS |
| 26 = LEAF2 | 65 = KRYPTOLAN | 97 = ETHERIP | 131 = PIPE |
| 27 = RDP | 66 = RVD | 98 = ENCAP | 132 = SCTP |
| 28 = IRTP | 67 = IPPC | 100 = GMTP | 133 = FC |
| 29 = ISOTP4 | 69 = SATMON | 101 = IFMPP | 254 = DIVERT |
| 30 = NETBLT | 70 = VISA | 102 = PNNI | |
| 31 = MFENSP | 71 = IPCV | 103 = PIM | |
| 32 = MERITINP | 72 = CPNX | 104 = ARIS | |
| 33 = SEP | | 105 = SCPS | |

# ベストプラクティス

CDO を使用して ASA 設定を FDM テンプレートに移行する場合は、次のベストプラクティスに従ってください。

- モデルデバイスの移行で **show run** コマンドを使用して、ASA デバイスから実行構成を取得していることを確認します。
- スキップされた設定、サポートされていない設定、および部分的にサポートされている設定について、移行レポートを確認します。
- 移行後、FDM による管理 デバイスに展開する前に、移行されたルールとオブジェクトを FDM テンプレートで確認します。
- ASA ポリシーを FDM テンプレートに移行する前に最適化します。
- 移行した ASA 設定は、既存の設定がない FDM による管理 デバイスに展開することをお勧めします。

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。