ASA CX モジュール

この章では、ASA で実行される ASA CX モジュールを設定する方法について説明します。

ASA CX モジュール

ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。

ASA CX モジュールがどのように ASA と連携するか

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

ご使用のデバイスをデモンストレーション用に、通常のインライン モードまたはモニタ専用モードのいずれかに設定できます。

- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。
- モニタ専用配置では、トラフィックのコピーがデバイスに送信されますが、ASA に戻されることはありません。モニタ専用モードでは、ネットワークに影響を与えることなくデバイスがトラフィックへの処理を行うことがわかります。モニタ専用のサービス ポリシーまたはトラフィック転送インターフェイスを使用してこのモードを設定できます。モニタ専用モードに関するガイドラインと制限事項については、「ASA CX のガイドライン」（P.18-6）を参照してください。

次の各セクションでは、これらのモードについて詳しく説明します。

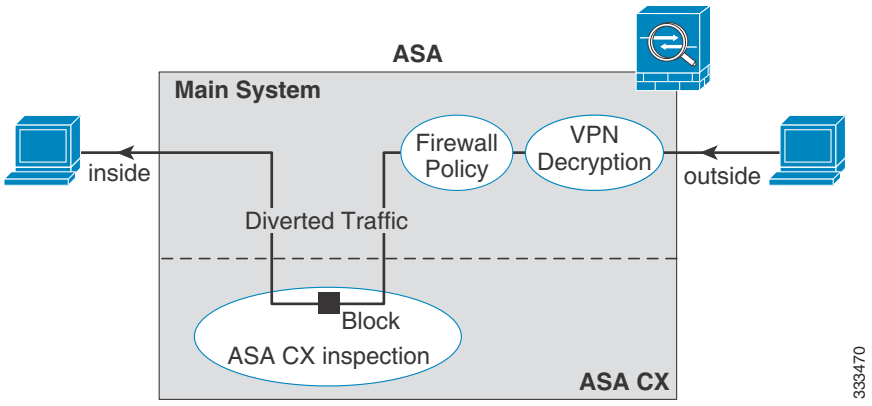
ASA CX の通常のインライン モード

通常のインライン モードでは、トラフィックは、ファイアウォール検査を通過してから ASA CX モジュールへ転送されます。ASA で ASA CX インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA CX モジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA CX モジュールに送信されます。
5. ASA CX モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA CX モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

次の図は、ASA CX モジュールを使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに対して許可されていないトラフィックを ASA CX モジュールが自動的にブロックします。それ以外のトラフィックは、ASA を通って転送されます。

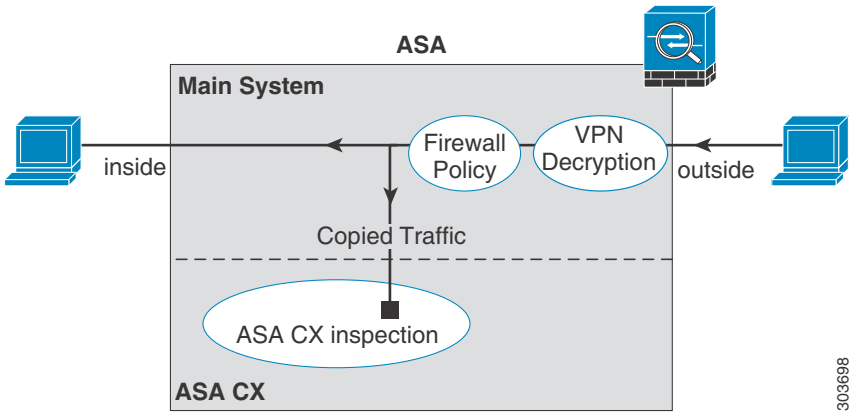
図 18-1　ASA での ASA CX モジュールのトラフィック フロー



モニタ専用モードでのサービス ポリシー

テストおよびデモンストレーション用に、ASA CX モジュールに読み取り専用トラフィックの重複ストリームを送信するように ASA を設定できるので、モジュールが ASA トラフィック フローに影響を与えることなく、どのようにトラフィックをインスペクションするかを確認できます。このモードでは、ASA CX モジュールが通常どおりトラフィックをインスペクションし、ポリシーを決定し、イベントを生成します。ただし、パケットが読み取り専用コピーであるため、モジュールのアクションは実際のトラフィックには影響しません。代わりに、モジュールはインスペクション後コピーをドロップします。次の図は、モニタ専用モードの ASA CX モジュールを示します。

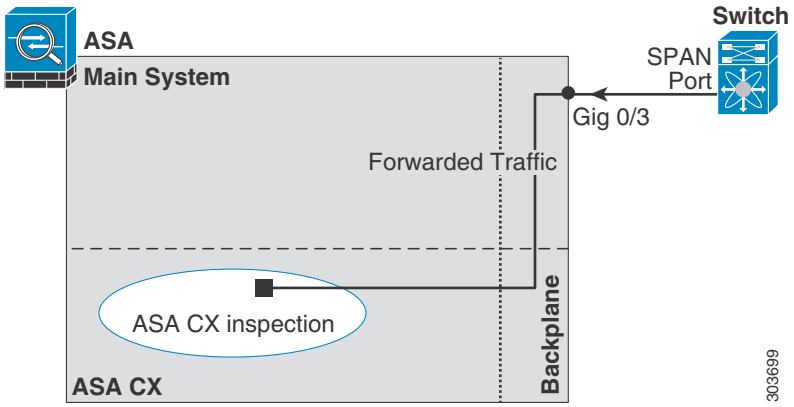
図 18-2　ASA CX モニタ専用モード



モニタ専用モードでのトラフィック転送インターフェイス

または、ASA インターフェイスを転送インターフェイスに設定し、ASA 処理を行わずに受信したすべてのトラフィックを直接 ASA CX モジュールに転送できます。テストおよびデモンストレーション用に、トラフィック転送では ASA 処理の余分な複雑性を取り除きます。トラフィック転送はモニタ専用モードでのみサポートされるので、ASA CX モジュールはインスペクション後トラフィックをドロップします。次の図は、トラフィック転送が設定されている ASA GigabitEthernet 0/3 インターフェイスを示します。このインターフェイスは、ASA CX モジュールがすべてのネットワーク トラフィックをインスペクションできるように、スイッチの SPAN ポートに接続されます。

図 18-3　ASA CX トラフィック転送



ASA CX の管理アクセス

ASA CX モジュールの管理には、初期設定（とその後のトラブルシューティング）およびポリシー管理の 2 つの異なるアクセスのレイヤがあります。

- 「初期設定」（P.18-4）
- 「ポリシー設定および管理」（P.18-5）

初期設定

初期設定を行うには、ASA CX モジュールの CLI を使用して **setup** コマンドを実行し、その他の任意の設定値を設定する必要があります。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA CX コンソール ポート：ASA CX コンソール ポートは、独立した外部コンソール ポートです。
  - ASA CX Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.8.8）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。ASA CX 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA CX ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。
  - ASA CX Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.1.2）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行します。ASA CX 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA CX モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。ASA CX IP アドレスの設定は、ASA CX オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA CX 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、Cisco Prime Security Manager（PRSM）を使用して ASA CX ポリシーを設定します。PRSM は ASA CX 設定インターフェイスの名前であり、それとは別に ASA CX デバイス、Cisco Prime Security Manager を設定する製品の名前でもあります。

その後、ASDM、ASA CLI、またはマルチ デバイス モードで PRISM を使用して、ASA CX モジュールにトラフィックを送信するために ASA ポリシーを設定します。

アクティブ認証用の認証プロキシ

アイデンティティ ポリシーを ASA CX に設定して、アクセス ポリシーで使用するユーザ アイデンティティ情報を収集できます。システムは、ユーザ アイデンティティをアクティブに（ユーザ名およびパスワードのクレデンシャルの入力を求めるプロンプトを表示する）またはパッシブに（AD エージェントまたは Cisco Context Directory Agent（CDA）が収集した情報を取得する）収集できます。

アクティブ認証を使用する場合は、認証プロキシとして動作するように ASA を設定する必要があります。ASA CX モジュールは認証要求を ASA インターフェイスの IP アドレス/プロキシ ポートにリダイレクトします。デフォルト ポートは 885 ですが、別のポートを設定することもできます。

アクティブ認証をイネーブルにするには、「ASA CX サービス ポリシーの作成」（P.18-18）で説明するように、トラフィックを ASA CX にリダイレクトするサービス ポリシーの一部として認証プロキシをイネーブルにします。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。
- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。

ASA CX モジュールのライセンス要件

ASA CX モジュールと PRSM には追加のライセンスが必要です。このライセンスは ASA との関連でインストールするのではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。詳細については、ASA CX のマニュアルを参照してください。

ASA CX の前提条件

PRSM を使用して ASA を設定するには、セキュアな通信を行うために ASA に証明書をインストールする必要があります。デフォルトでは、ASA は自己署名証明書を生成します。ただし、この証明書のパブリッシャが不明であるため、ブラウザに証明書の検証を求めるプロンプトが表示されます。これらのブラウザのプロンプトが表示されないようにするには、代わりに既知の認証局（CA）からの証明書をインストールします。CA からの証明書を要求する場合、証明書タイプがサーバ認証証明書とクライアント認証証明書の両方であることを確認します。詳細については、一般的な操作のコンフィギュレーション ガイドを参照してください。

ASA CX のガイドライン

コンテキスト モードのガイドライン

ASA CX 9.1(3) を始めに、複数のマルチ コンテキスト モードがサポートされます。

ただし、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。したがって、複数のコンテキストで同じ IP アドレスを使用できず、各コンテキストに独自のネットワークを含める必要があります。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。トラフィック転送インターフェイスは、トランスペアレント モードでのみサポートされます。

フェールオーバーのガイドライン

フェールオーバーを直接にはサポートしていません。ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX によるインスペクションを受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

ASA クラスタリングのガイドライン

クラスタリングはサポートされません。

IPv6 のガイドライン

- IPv6 をサポートします。
- （9.1(1) 以前）NAT 64 はサポートされません。9.1(2) 以降では、NAT 64 がサポートされます。

モデルのガイドライン

- ASA 5585-X および 5512-X ～ ASA 5555-X でのみサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。

モニタ専用モードのガイドライン

モニタ専用モードは厳密にデモンストレーション用であり、モジュールの通常の動作モードではありません。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードで、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。
- 次の機能は、モニタ専用モードではサポートされません。
  - 拒否ポリシー
  - アクティブ認証
  - 復号ポリシー
- ASA CX は、モニタ専用モードでパケット バッファリングを実行せず、イベントはベストエフォート方式で生成されます。たとえば、長い URL がパケット境界にまたがっている一部のイベントは、バッファリングの欠如の影響を受ける可能性があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。

上記のほか、トラフィック転送インターフェイスには次のガイドラインがあります。

- ASA はトランスペアレント モードにする必要があります。
- 最大 4 つのインターフェイスを、トラフィック転送インターフェイスとして設定できます。その他の ASA インターフェイスは、通常どおり使用できます。
- トラフィック転送インターフェイスは、VLAN または BVI ではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられた VLAN を設定することはできません。
- トラフィック転送インターフェイスは、ASA トラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含む ASA 機能向けに設定できません。
- トラフィック転送インターフェイスとサービス ポリシーの両方を ASA CX トラフィック用に設定できません。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.18-6）を参照してください。
- ハードウェア モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA CX モジュールに、後で別のソフトウェアをインストールすることはできません。

ASA CX のデフォルト設定

次の表に、ASA CX モジュールのデフォルト設定を示します。

表 18-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	ASA 5585-X：Management 1/0 192.168.8.8/24 ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	ASA 5585-X：192.168.8.1/24 ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	Admin123

ASA CX モジュールの設定

ASA CX モジュールの設定プロセスでは、ASA CX セキュリティ ポリシーを ASA CX モジュール上で設定してから、トラフィックを ASA CX モジュールに送信するように ASA を設定します。ASA CX モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA CX 管理インターフェイスの接続」（P.18-9）。ケーブルで ASA CX 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。

ステップ 2　「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.18-12）。

ステップ 3　「(ASA 5585-X) ASA CX 管理 IP アドレスの変更」(P.18-14)（必要な場合）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「基本的な ASA CX 設定値の設定」(P.18-15)。この設定は ASA CX モジュールで行います。

ステップ 5　「ASA CX モジュールでのセキュリティ ポリシーの設定」(P.18-17)。

ステップ 6　（任意）「認証プロキシ ポートの設定」(P.18-17)。

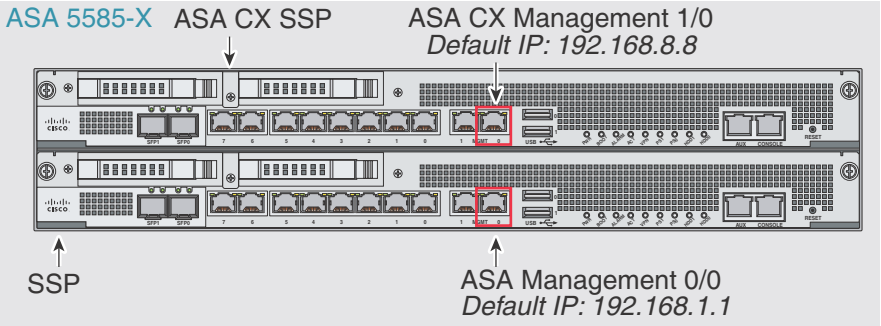
ステップ 7　「ASA CX モジュールへのトラフィックのリダイレクト」(P.18-17)。

ASA CX 管理インターフェイスの接続

ASA CX モジュールへの管理アクセスを提供する以外に、ASA CX 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

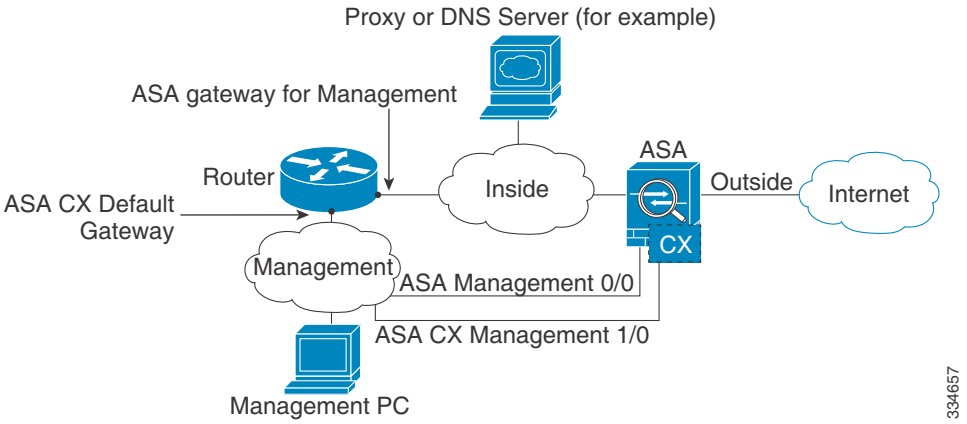
ASA 5585-X（ハードウェア モジュール）

ASA CX モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレス（192.168.8.8/24）を使用して ASA CX Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



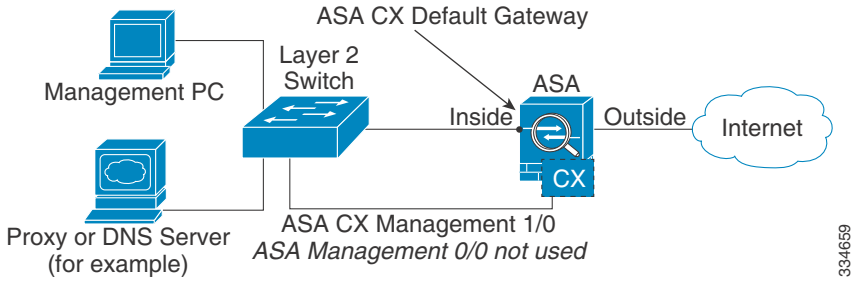
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA CX Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



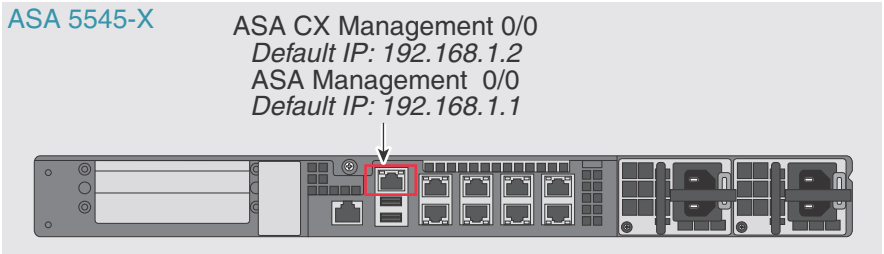
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA CX モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA CX Management 1/0 アドレスを設定できます。



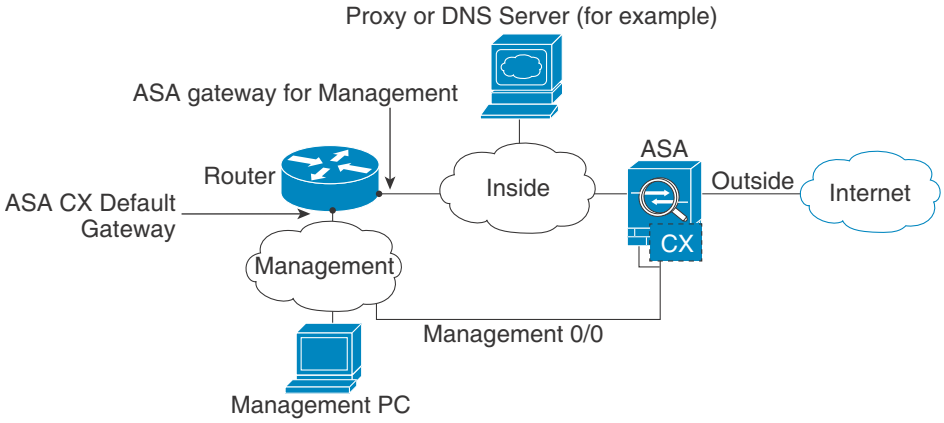
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行し、ASA CX 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定を行うには、SSH で ASA CX のデフォルト IP アドレス（192.168.1.2/24）に接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA CX にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



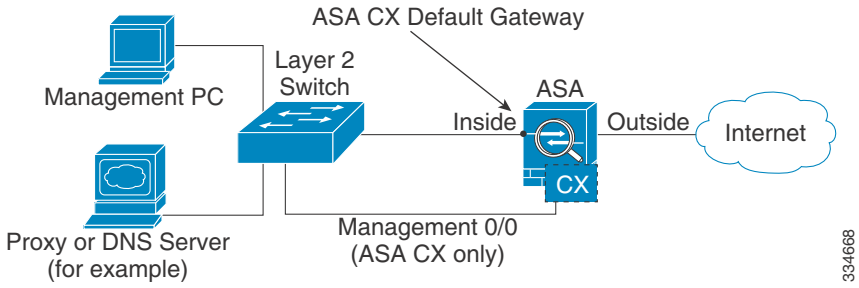
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA CX の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA 設定の名前を Management 0/0 インターフェイスから削除する場合、そのインターフェイスの ASA CX IP アドレスを引き続き設定できます。ASA CX モジュールは基本的には ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上にあるように ASA CX 管理アドレスを設定 できます。



（注）　Management 0/0 に対して ASA が設定した名前を削除する必要があります。これが ASA で設定されている場合、ASA CX アドレスは、ASA と同じネットワーク上に存在する必要があり、これによって、その他の ASA インターフェイス上ですでに設定されたネットワークはすべて除外されます。名前が設定されていない場合、ASA CX は、任意のネットワーク上（たとえば、ASA 内部ネットワーク）に存在することができます。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

ASA CX モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに使用できます。既存の ASA に ASA CX を追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA CX ブート ソフトウェアをインストールし、SSD を分割する必要があります。物理的に SSD を取り付けるには、『ASA Hardware Guide』を参照してください。

最初に ASA CX モジュールをアンインストールする必要がある点を除いて、モジュールのイメージの再作成はこれと同じ手順です。システムのイメージの再作成は、SSD を交換する場合に行います。

（注）　ASA 5585-X ハードウェア モジュールの場合、ASA CX モジュールからイメージをインストールまたはアップグレードする必要があります。詳細は、ASA CX モジュールのマニュアルを参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドは IPS ソフトウェア モジュールをシャットダウンしてアンインストールし、ASA をリロードします。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**noservice-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/アンインストール コマンドを使用して古いイメージを削除します。たとえば、**sw-module module cxsc uninstall** などです。
- Cisco.com（http://software.cisco.com/download/type.html?mdfid=284325223&flowid=34503）から、ASA CX のブート イメージおよびシステム ソフトウェア パッケージの両方を取得します。

手順

ステップ 1　ブート イメージをデバイスにダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：まず、ブート イメージをワークステーションにダウンロードするか、FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に、ASDM で [Tools] > [File Management] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。
- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 2　ASA CX 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA CX システム ソフトウェアをダウンロードします。

ステップ 3　次のコマンドを入力して、ASA disk0 で ASA CX モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

（注）　「ERROR: Another service (ips) is running, only one service is allowed to run at any time」のようなメッセージが表示される場合、別のソフトウェア モジュールがすでに設定されていることを意味します。このソフトウェア モジュールをシャットダウンして削除し、上の前提条件セクションの説明に従って新しいモジュールをインストールする必要があります。

例：

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 4　次のコマンドを入力して、ASA CX ブート イメージをロードします。

```
hostname# sw-module module cxsc recover boot
```

ステップ 5　ASA CX モジュールが起動するまで約 5 分待ってから、現在実行中の ASA CX ブート イメージへのコンソール セッションを開きます。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc.Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。しばらく待ってから再試行してください。

ステップ 6　SSD を分割します。

```
asacx-boot> partition
....
Partition Successfully Completed
```

ステップ 7　「基本的な ASA CX 設定値の設定」（P.18-15）に従って、**setup** コマンドを使用して基本的なネットワーク設定を実行し（ASA CX CLI を終了しないでください）、この手順に戻ってソフトウェア イメージをインストールします。

ステップ 8　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用してください。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

インストールの終了時にシステムが再起動して、コンソール セッションが閉じられます。アプリケーション コンポーネントのインストールと ASA CX サービスの起動には 10 分以上かかります（**show module cxsc** の出力には、すべてのプロセスが Up と表示されます）。

次のコマンドは asacx-sys-9.3.1.1-112.pkg システム ソフトウェアをインストールします。

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:                 Cisco ASA CX 9.3.1.1-112 System Install
        Requires reboot:             Yes

Do you want to continue with upgrade?[n]: Y
Warning: Please do not interrupt the process or turn off the system.Doing so might leave
system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade.Press Enter to reboot the system.
```

（ASA 5585-X）ASA CX 管理 IP アドレスの変更

デフォルトの管理 IP アドレス（192.168.8.8）を使用できない場合は、管理 IP アドレスを ASA から設定できます。管理 IP アドレスを設定した後は、初期設定を実行するために SSH を使用して ASA CX モジュールにアクセスできます。

（注）　ソフトウェア モジュールの場合、ASA CX CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA CX 管理 IP アドレスを設定できます。「基本的な ASA CX 設定値の設定」（P.18-15）を参照してください。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- CLI で、次のコマンドを使用して ASA CX の管理 IP アドレス、マスク、およびゲートウェイを設定します。

  session 1 do setup host ip *ip_address*/*mask*,*gateway_ip*

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。

- （シングルコンテキスト モードのみ）ASDM で、[Wizards] > [Startup Wizard] を選択して、ウィザードの [ASA CX Basic Configuration] まで進めます。ここで IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。デフォルトが適していない場合は、他の認証プロキシのポートを設定することもできます。

基本的な ASA CX 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA CX モジュール上で設定する必要があります。ASA CX CLI は、これらの設定を行う唯一の方法です。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA CX 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのコンソール セッションを開きます。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  ```
  hostname# session cxsc console
  ```

ステップ 2　ユーザ名 **admin** およびパスワード **Admin123** を使用してログインします。この手順の中で、パスワードを変更します。

ステップ 3　次のコマンドを入力します。

```
asacx> setup
```

例：

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

セットアップ ウィザードでは入力が求められます。次の例は、ウィザードでの一般的な順序を示しています。プロンプトで **N** ではなく **Y** を入力した場合は、追加の設定を行うことができます。次に、IPv4 および IPv6 両方のスタティック アドレスの設定例を示します。IPv6 ステートレス自動設定を設定するには、スタティック IPv6 アドレスを設定するかどうかを尋ねるプロンプトで **N** と応答します。

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
```

```
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server?(y/n) [N]: N
Do you want to configure Local Domain Name?(y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains?(y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

ステップ 4　最後のプロンプトが完了すると、設定のサマリーが示されます。サマリーに目を通して値が正しいことを確認し、変更した設定を適用するには **Y** を入力します。変更をキャンセルするには **N** を入力します。

例：

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

（注）　ホスト名を変更した場合は、ログアウトして再びログインするまでプロンプトに新しい名前は表示されません。

ステップ 5　NTP を使用しない場合は、時刻を設定します。デフォルトのタイム ゾーンは UTC タイム ゾーンです。現在の設定を表示するには、**show time** コマンドを使用します。時間設定を変更するには、次のコマンドを使用できます。

```
asacx> config timezone
asacx> config time
```

ステップ 6　次のコマンドを入力して、admin のパスワードを変更します。

```
asacx> config passwd
```

例：

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

ステップ 7　**exit** コマンドを入力してログアウトします。

ASA CX モジュールでのセキュリティ ポリシーの設定

ASA CX モジュールでセキュリティ ポリシーを設定するには PRSM を使用します。セキュリティ ポリシーは、モジュールが提供するサービスを制御します。ASA CX CLI、ASA CLI、または ASDM を使用してポリシーを設定できません。

PRSM は ASA CX 設定インターフェイスの名前であり、それとは別に ASA CX デバイス、Cisco Prime Security Manager を設定する製品の名前でもあります。設定インターフェイスへのアクセス方法とその使用方法は同じです。PRSM を使用して ASA CX/PRSM セキュリティ ポリシーを設定する方法の詳細については、ASA CX ユーザ ガイドまたはオンライン ヘルプを参照してください。

PRSM を開くには、Web ブラウザを使用して次の URL を開きます。

https://*management_address*

management_address は ASA CX 管理インターフェイスまたは PRSM サーバの DNS 名または IP アドレスです。たとえば、https://asacx.example.com などです。

認証プロキシ ポートの設定

ASA CX ポリシーでアクティブ認証を使用する場合、ASA は、認証プロキシのポートとしてポート 885 を使用します。885 が許可されない場合は別のポートを設定できますが、デフォルト以外のポートは 1024 より大きい必要があります。認証プロキシの詳細については、「アクティブ認証用の認証プロキシ」（P.18-5）を参照してください。

マルチコンテキスト モードでは、各セキュリティ コンテキスト内のポートを変更します。

認証プロキシ ポートを変更するには、次のコマンドを入力します。

```
cxsc auth-proxy port port
```

たとえば、**cxsc auth-proxy port 5000** などです。

ASA CX モジュールへのトラフィックのリダイレクト

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトできます。デモンストレーション用にのみ、元のトラフィックが影響を受けることなく、ASA CX モジュールへのトラフィックのコピーを転送するサービス ポリシーに対するモニタ専用モードもイネーブルにできます。

デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。

- 「ASA CX サービス ポリシーの作成」（P.18-18）
- 「トラフィック転送インターフェイスの設定（モニタ専用モード）」（P.18-20）

ASA CX サービス ポリシーの作成

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトします。

（注）　ASA CX は双方向にリダイレクトを行います。したがって、1 つのインターフェイスにサービス ポリシーを設定し、そのインターフェイス上のホストとリダイレクションが設定されていないインターフェイス上のホストが接続されている場合、それらのホスト間の ASA CX ではないインターフェイスから発信されるトラフィックを含めたすべてのトラフィックは ASA CX モジュールに送信されます。ただし、認証プロキシは入力トラフィックのみに適用されるため、ASA は、サービス ポリシーが適用されているインターフェイス上の認証プロキシに対してのみ処理を行います。

はじめる前に

- この手順を使用して ASA で認証プロキシをイネーブルにする場合は、必ず ASA CX モジュールで認証用のディレクトリ レルムも設定してください。詳細については、ASA CX ユーザ ガイドを参照してください。
- （ASA CX と交換した）IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA CX サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。
- PRSM をマルチ デバイス モードで使用するときは、以下で説明するようにトラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

手順

ステップ 1　モジュールに送信するトラフィックを L3/L4 指定するためのクラス マップを作成します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map cx_class
hostname(config-cmap)# match access-list cx_traffic
```

モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。

```
policy-map name
```

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　この手順の最初に作成したクラス マップを指定します。

class *name*

例：

```
hostname(config-pmap)# class cx_class
```

ステップ 4　ASA CX モジュールにトラフィックを送信します。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

それぞれの説明は次のとおりです。

- **fail-close** キーワードを指定すると、ASA CX モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。
- **fail-open** キーワードを指定すると、モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。
- **auth-proxy** キーワードを任意で指定すると、アクティブ認証に必要な認証プロキシがイネーブルになります。
- デモンストレーション用にのみ、**monitor-only** を指定して、トラフィックの読み取り専用のコピーを ASA CX モジュールに送信します。すべてのクラスとポリシーは、モニタ専用モード、または通常のインライン モードのいずれか設定する必要があります。同じ ASA で両方のモードを混在させることはできません。

例：

```
hostname(config-pmap-c)# cxsc fail-close auth-proxy
```

ステップ 5　ASA CX トラフィックに複数のクラス マップを作成した場合、ポリシーに別のクラスを指定して **cxsc** リダイレクト アクションを適用できます。

ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.1-5）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。

ステップ 6　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

トラフィック転送インターフェイスの設定（モニタ専用モード）

デモンストレーション用にのみ、すべてのトラフィックが ASA CX モジュールに直接転送されるトラフィック転送インターフェイスを設定できます。正常な ASA CX の動作については、「ASA CX サービス ポリシーの作成」（P.18-18）を参照してください。

詳細については、「モニタ専用モードでのトラフィック転送インターフェイス」（P.18-4）を参照してください。トラフィック転送インターフェイスに固有のガイドラインと制限については「ASA CX のガイドライン」（P.18-6）も参照してください。

はじめる前に

- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1　トラフィック転送に使用する物理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *physical_interface*

例：

```
hostname(config)# interface gigabitethernet 0/5
```

ステップ 2　インターフェイスに設定された名前を削除します。このインターフェイスがいずれかの ASA 設定で使用されると、その設定は削除されます。指定したインターフェイス上でトラフィック転送を設定できません。

no nameif

ステップ 3　トラフィック転送をイネーブルにします。

traffic-forward cxsc monitor-only

ステップ 4　インターフェイスをイネーブルにします。

no shutdown

追加のインターフェイスについて、この手順を繰り返します。

例

次の例は、GigabitEthernet 0/5 のトラフィック転送インターフェイスを作成します。

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward cxsc monitor-only
  no shutdown
```

ASA CX モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **admin** のデフォルトのパスワードは **Admin123** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュール パスワードをデフォルトにリセットするには、次のいずれかの方法を使用します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- （CLI）ハードウェア モジュール（ASA 5585-X）

  hw-module module 1 password-reset

- （CLI）ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）

  sw-module module cxsc password-reset

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 {**reload** | **reset**}

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc {**reload** | **reset**}

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

（注） ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 shutdown

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc shutdown

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

手順

ステップ 1　ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

```
hostname# sw-module module cxsc uninstall

Module cxsc will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module cxsc?[confirm]
```

ステップ 2　ASA をリロードします。新しいモジュールをインストールする前に、ASA をリロードする必要があります。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション

ASA CX CLI を使用して、基本的なネットワーク設定を構成し、モジュールのトラブルシューティングを行います。

ASA から ASA CX ソフトウェア モジュール CLI にアクセスするには、ASA からセッション接続できます。モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。**admin** ユーザ名とパスワード（デフォルトは **Admin123**）を入力します。

- Telnet セッション：

  ```
  session cxsc
  ```

  CX ASA CLI で、終了して ASA CLI に戻るには、**exit** コマンドを使用するか **Ctrl+Shift+6、x** を押します。

- コンソール セッション：

  ```
  session cxsc console
  ```

  コンソール セッションからログアウトする唯一の方法は、**Ctrl+Shift+6、x** を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注）　**session cxsc console** コマンドは、**Ctrl+Shift+6、x** がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6、x** は、ASA CX コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で ASA CX を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、ASA CX コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、コンソール コマンドの代わりに **session cxsc** コマンドを使用します。

ASA CX モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA CX 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA CX の syslog メッセージは、メッセージ番号 429001 から始まります。

- 「モジュール ステータスの表示」（P.18-24）
- 「モジュールの統計情報の表示」（P.18-24）
- 「モジュール接続のモニタリング」（P.18-25）

モジュール ステータスの表示

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

- **show module** [**1** | **cxsc**] [**details**]

  モジュールのステータスを表示します。ASA CX モジュールに固有のステータスを確認するには、1（ハードウェア モジュールの場合）または cxsc（ソフトウェア モジュールの場合）キーワードを指定します。モジュールを管理するデバイスのアドレスなどの追加情報を取得するには、details キーワードを指定します。

- **show module cxsc recover**

  モジュールのインストール時に使用されたブート イメージの場所を表示します。

次に、ASA CX SSP がインストールされている ASA での **show module** コマンドの出力例を示します。

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
  1 ASA 5585-X CX Security Services Processor-10 ASA5585-SSP-CX10   JAF1510BLSA

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.7(6)78
  1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     0.6.1

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 ASA CX Security Module         Up               0.6.1

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

モジュールの統計情報の表示

cxsc コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、**show service-policy cxsc** コマンドを使用します。カウンタをクリアするには、**clear service-policy** を使用します。

次に示す **show service-policy** コマンドの出力例では、認証プロキシがディセーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に示す **show service-policy** コマンドの出力例では、認証プロキシがイネーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。この場合は、proxied カウンタもインクリメントされます。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

モジュール接続のモニタリング

ASA CX モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain cxsc**

  トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。

- **show asp table classify domain cxsc-auth-proxy**

  ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。次に、コマンドの出力例を示します。ここでは、宛先「port=2000」は **cxsc auth-proxy port 2000** コマンドによって設定された認証プロキシのポートであり、宛先「ip/id=192.168.0.100」は ASA インターフェイスの IP アドレスである 1 つのルールを示します。

  ```
  hostname# show asp table classify domain cxsc-auth-proxy
  Input Table
  in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
      hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
      src ip/id=0.0.0.0, mask=0.0.0.0, port=0
      dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
      input_ifc=inside, output_ifc=identity
  ```

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについては、以下で説明します。

- **show asp event dp-cp cxsc-msg**

  この出力には、dp-cp キューにある ASA CX モジュール メッセージの数が表示されます。ASA CX モジュールからの VPN クエリーのみが dp-cp に送信されます。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドは、ASA CX モジュールに関連する次のドロップ理由を含めることができます。

フレーム ドロップ：

- cxsc-bad-tlv-received：これが発生するのは、ASA が CXSC から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standby Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- cxsc-request：CXSC 上のポリシーが理由で、フレームをドロップするよう CXSC から要求されました。このポリシーによって、CXSC はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。

- cxsc-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。
- cxsc-fail：既存のフローに対する CXSC コンフィギュレーションが削除されており、CXSC で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- cxsc-malformed-packet：CXSC からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。

フロードロップ：

- cxsc-request：フローを終了させることを CXSC が要求しました。アクション ビット 0 が設定されます。
- reset-by-cxsc：フローの終了とリセットを CXSC が要求しました。アクション ビット 1 が設定されます。
- cxsc-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

認証プロキシでの問題のトラブルシューティング

認証プロキシ機能を使用するときに問題が発生した場合は、次の手順に従って設定および接続のトラブルシューティングを行います。

（注） 2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

手順

ステップ 1　コンフィギュレーションを確認します。

- ASA で、**show asp table classify domain cxsc-auth-proxy** コマンドの出力を調べて、ルールがインストールされていて正しいことを確認します。
- PRSM で、ディレクトリのレルムが作成されていて正しいクレデンシャルが指定されていることを確認するとともに、接続をテストして、認証サーバに到達可能であることを確認します。また、認証用のポリシー オブジェクトが設定されていることを確認します。

ステップ 2　**show service-policy cxsc** コマンドの出力を見て、プロキシされたパケットがあるかどうかを調べます。

ステップ 3　バックプレーンに対してパケット キャプチャを実行します（**capture** *name* **interface asa_dataplane**）。そしてトラフィックが正しく設定されたポートにリダイレクトされているかどうかを確認します。**show running-config cxsc** コマンドまたは **show asp table classify domain cxsc-auth-proxy** コマンドを使用して設定されたポートを確認できます。

例

ポート 2000 が一貫して使用されていることの確認

1. 認証プロキシのポートを確認します。

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 認証プロキシ ルールを確認します。

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. パケット キャプチャでは、リダイレクト要求が宛先ポート 2000 に送られる必要があります。

ASA CX モジュールの設定例

次の例では、すべての HTTP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合はすべての HTTP トラフィックがブロックされます。

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
hostname(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list my-cx-acl
hostname(config)# class-map my-cx-class2
hostname(config-cmap)# match access-list my-cx-acl2
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap)# class my-cx-class2
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy interface outside
```

ASA CX モジュールの履歴

機能名	プラットフォームリリース	説明
ASA CX SSP-10 および -20 用の ASA 5585-X（SSP-10 および -20 搭載）サポート	ASA 8.4(4.1) ASA CX 9.0(1)	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module**、**show service-policy** の各コマンドが導入または変更されました。
ASA CX SSP 用 ASA 5512-X ～ ASA 5555-X サポート	ASA 9.1(1) ASA CX 9.1(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA CX SSP ソフトウェア モジュールのサポートが導入されました。 **session cxsc**、**show module cxsc**、**sw-module cxsc** の各コマンドが変更されました。

機能名	プラットフォームリリース	説明
デモンストレーション用モニタ専用モード	ASA 9.1(2) ASA CX 9.1(2)	デモンストレーション目的でのみ、サービス ポリシー用のモニタリング専用モードをイネーブルにすることができ、元のトラフィックに影響を与えずに、トラフィックのコピーを ASA CX モジュールに転送することができます。 デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。 **cxsc {fail-close | fail-open} monitor-only**、**traffic-forward cxsc monitor-only** の各コマンドが変更または導入されました。
ASA CX モジュールに対する NAT 64 のサポート	ASA 9.1(2) ASA CX 9.1(2)	ASA CX モジュールとともに NAT 64 を使用できるようになりました。 変更されたコマンドはありません。
ASA CX SSP-40 および -60 用の ASA 5585-X（SSP-40 および -60 搭載）サポート	ASA 9.1(3) ASA CX 9.2(1)	ASA CX SSP-40 および -60 モジュールは、SSP-40 および -60 搭載の ASA 5585-X と一致するレベルで使用できます。 変更されたコマンドはありません。
ASA CX モジュールのマルチ コンテキスト モードのサポート	ASA 9.1(3) ASA CX 9.2(1)	ASA でコンテキストごとに ASA CX サービス ポリシーを設定できます。 **（注）** コンテキストごとに ASA サービス ポリシーを設定できますが、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。 変更されたコマンドはありません。

機能名	プラットフォームリリース	説明
ASA CX バックプレーンでキャプチャされたパケットのフィルタリング	ASA 9.1(3) ASA CX 9.2(1)	**match** または **access-list** キーワードを **capture interface asa_dataplane** コマンドと共に使用して、ASA CX バックプレーンでキャプチャされたパケットをフィルタリングできます。 ASA CX モジュールに固有の制御トラフィックは、access-list または match フィルタリングの影響を受けません。ASA はすべての制御トラフィックをキャプチャします。 マルチ コンテキスト モードでは、コンテキストごとにパケット キャプチャを設定します。マルチ コンテキスト モードのすべての制御トラフィックが送信されるのはシステム実行スペースだけであることに注意してください。access-list または match を使用して制御トラフィックのフィルタリングを行うことができないため、これらのオプションはシステム実行スペースでは使用できません。 **capture interface asa_dataplane** コマンドが変更されました。