使用する前に

ここでは、Firepower Threat Defense の設定を開始する方法について説明します。

このガイドの対象読者

このガイドでは、Firepower Threat Defense デバイスに含まれている Firepower Device Manager の Web ベースのインターフェイスを使用して Firepower Threat Defense を設定する方法について説明します。

Firepower Device Manager を使うことで、小～中規模なネットワークで最も一般的に使用されるソフトウェアの基本機能の設定が行えます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合、統合 Firepower Device Manager の代わりに Firepower Management Center デバイスを使用します。

クラウドベースのアプリケーションである Cisco Defense Orchestrator を使用して、1 つまたは複数のデバイスを管理することもできます。クラウド管理の方法については、https://youtu.be/fsIfsHhnpQU でビデオを視聴し、Cisco Defense Orchestrator ポータル（http://www.cisco.com/go/cdo）を熟読してください。製品マニュアルは https://docs.defenseorchestrator.com/ で検索できます。Cisco Defense Orchestrator へのデバイスの接続の詳細については、クラウド管理の設定（Cisco Defense Orchestrator）を参照してください。

Firepower Device Manager は次のデバイスで使用できます。

表 *1 : Firepower Device Manager* がサポートされるモデル

デバイス モデル	Firepower Threat Defense の最小ソフトウェア バージョン
Firepower 1010、1120、1140	6.4
Firepower 1150	6.5
Firepower 2110、2120、2130、2140	6.2.1
Firepower 4110、4115、4120、4125、4140、4145、4150	6.5
Firepower 9300	6.5
Firepower Threat Defense Virtual VMware 用	6.2.2
Firepower Threat Defense Virtual カーネルベース仮想マシン（KVM）ハイパーバイザ用	6.2.3
Firepower Threat Defense Virtual Microsoft Azure クラウド用	6.5
ASA 5508-X、5516-X	6.1
ASA 5525-X、5545-X、5555-X	6.1
ASA 5515-X （注） ASA 5515-X のサポートは 6.4（許可される最後のバージョン）で終了します。このモデルにバージョン 6.5 以降をインストールすることはできません。	6.1
ISA 3000（Cisco 3000 シリーズ産業用セキュリティ アプライアンス）	6.2.3

Firepower Device Manager/FTD バージョン 6.5.0 の新機能

リリース：2019 年 9 月 26 日

次の表は、Firepower Device Manager を使用して設定した場合に、FTD 6.5.0 で使用可能な新機能を示しています。

機能	説明
Firepower 4100/9300 の FDM のサポート。	FDM を使用して Firepower 4100/9300 で Firepower Threat Defense を設定できるようになりました。ネイティブ インスタンスのみがサポートされています。コンテナ インスタンスはサポートされていません。

機能	説明
Microsoft Azure クラウド用 Firepower Threat Defense Virtual の FDM のサポート。	Firepower Device Manager を使用して Microsoft Azure クラウド用 Firepower Threat Defense Virtual で Firepower Threat Defense を設定できます。
Firepower 1150 のサポート。	Firepower 1150 用の FTD が導入されました。
Firepower 1010 ハードウェアスイッチのサポート、PoE+のサポート。	Firepower 1010 では、各イーサネット インターフェイスをスイッチポートまたは通常のファイアウォールインターフェイスとして設定できます。各スイッチポートを VLAN インターフェイスに割り当てます。Firepower 1010 は、Ethernet1/7 および Ethernet 1/8 での Power over Ethernet+（PoE+） もサポートしています。 デフォルト設定で、Ethernet1/1 が外部として設定され、Ethernet1/2 ～ 1/8 が内部 VLAN1 インターフェイスのスイッチポートとして設定されるようになりました。バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。
インターフェイスのスキャンと置き換え。	インターフェイス スキャンでは、シャーシで追加、削除、または復元されたインターフェイスが検出されます。設定で古いインターフェイスを新しいインターフェイスに置き換えることもできるため、インターフェイスの変更がシームレスに行えます。
インターフェイス表示の向上。	**[デバイス（Device）]**>**[インターフェイス（Interfaces）]** ページの構成が改められました。物理インターフェイス、ブリッジ グループ、Etherchannel、および VLAN 用のタブが別々に設けられました。任意の対象デバイス モデルについて、モデルに関連するタブのみが表示されます。たとえば、[VLAN] タブは Firepower 1010 モデルでのみ使用できます。また、各インターフェイスの設定と使用方法に関する詳細情報がリストに表示されます。

機能	説明
ISA 3000 の新しいデフォルト設定。	ISA 3000 のデフォルト設定が次のように変更されました。 • すべてのインターフェイスが BVI1 のブリッジ グループ メンバーとなりました。BVI1 には名前が付いていないため、ルーティングには参加しません。 • GigabitEthernet1/1 および 1/3 は外部インターフェイスとなり、GigabitEthernet1/2 および 1/4 は内部インターフェイスとなります。 • 内部/外部ペアごとにハードウェア バイパスが有効になります（使用可能な場合）。 • すべてのトラフィックについて、内部から外部、および外部から内部が許可されます。 バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。
ASA 5515-X のサポート終了。最後にサポートされるリリースは FTD 6.4。	ASA 5515-X に FTD 6.5 をインストールすることはできません。ASA 5515-X 用に最後にサポートされるリリースは FTD 6.4 です。
Cisco ISA 3000 デバイスのアクセス制御ルールにおける Common Industrial Protocol（CIP）および Modbus アプリケーション フィルタリングのサポート。	Cisco ISA 3000 デバイスで Common Industrial Protocol（CIP）および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write というように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。 プリプロセッサを有効にするには、CLI セッション（SSH またはコンソール）でエキスパート モードに移行し、**sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}** コマンドを発行する必要があります。展開のたびに展開後にプリプロセッサがオフになるため、展開のたびにこのコマンドを発行する必要があります。

機能	説明
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp** および **igmp**（インターフェイス モード）コマンド、およびグローバル コマンド **ptp mode e2etransparent** と **ptp domain** を追加できるようになりました。また、FTD CLI に **show ptp** コマンドが追加されました。
EtherChannel（ポート チャネル）インターフェイス。	EtherChannel インターフェイス（ポート チャネルとも呼ばれます）を設定できます。 （注） FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス（Interfaces）] ページに表示されます。 **[デバイス（Device）] > [インターフェイス（Interfaces）]** ページが更新され、EtherChannel の作成ができるようになりました。
FDM からシステムを再起動およびシャットダウンする機能。	新しい [再起動/シャットダウン（Reboot/Shutdown）] システム設定ページからシステムを再起動またはシャットダウンできるようになりました。以前は、FDM の CLI コンソールを使用して、あるいは SSH またはコンソール セッションから、**reboot** および **shutdown** コマンドを発行する必要がありました。これらのコマンドを使用するには、管理者権限が必要です。
FDM CLI コンソールでの **failover** コマンドのサポート。	FDM CLI コンソールを使用して **failover** コマンドを発行できるようになりました。
スタティック ルート用のサービス レベル契約（SLA）モニタ。	スタティックルートとともに使用するためのサービスレベル契約（SLA）モニタオブジェクトを設定します。SLA モニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。SLA モニタオブジェクトを選択できるように、[オブジェクト（Object）] ページに [SLA モニタ（SLA Monitors）] を追加し、スタティック ルートを更新しました。

機能	説明
Smart CLI および FTD API でのルーティングの変更。	今回のリリースには、Smart CLI および FTD API でのルーティング設定に対していくつかの変更が追加されています。以前のリリースでは、BGP 用として単一の Smart CLI テンプレートがありました。今回は、BGP（ルーティング プロセス設定）用と BGP 一般設定（グローバル設定）用に別々のテンプレートが用意されました。 FTD API では、新しい BGP 一般設定のメソッドを除いて、すべてのメソッドのパスが変更され、パスに「/virtualrouter」が挿入されました。 • スタティック ルート メソッドのパスは、以前は /devices/default/routing/{parentId}/staticrouteentries でしたが、今後は /devices/default/routing/virtualrouters/default/staticrouteentries になります。 • BGP メソッドは、/devices/default/routing/bgpgeneralsettings と /devices/default/routing/virtualrouters/default/bgp の 2 つの新しいパスに分割されました。 • OSPF パスは /devices/default/routing/virtualrouters/default/ospf および /devices/default/routing/virtualrouters/default/ospfinterfacesettings になりました。 FTD API を使用してルーティング プロセスを設定している場合は、呼び出しを調べて必要に応じて修正してください。

機能	説明
新しいURLカテゴリおよびレピュテーション データベース。	システムは、Cisco Talos とは別の URL データベースを使用します。新しいデータベースでは、URL のカテゴリにいくつかの違いがあります。アップグレードすると、もう存在していないカテゴリがアクセス制御や SSL 復号ルールで使用されている場合、システムはそのカテゴリを適切な新しいカテゴリに置き換えます。変更を有効にするには、アップグレード後に設定を展開します。カテゴリの変更についての詳細は、[保留中の変更（Pending Changes）] ダイアログに表示されます。引き続き希望する結果が得られることを確認するため、URL フィルタリングポリシーを調べる必要がある場合があります。 アクセス制御ポリシーと SSL 復号ポリシーの [URL] タブ、および **[デバイス（Device）] > [システム設定（System Settings）] > [URLフィルタリング設定（URL Filtering Preferences）]** ページに URL ルックアップ機能を追加しました。この機能を使用すると、特定の URL に割り当てられているカテゴリを確認できます。同意しない場合は、カテゴリの異議を送信するリンクもあります。このどちらの機能も、URL に関する詳細情報を提供する外部 Web サイトを使用します。
セキュリティ インテリジェンスでは、ホスト名ではなく IP アドレスを使用する URL 要求に対して IP アドレスの評価を使用する。	HTTP/HTTPS 要求の宛先が、ホスト名ではなく IP アドレスを使用する URL である場合は、ネットワーク アドレス リストにある IP アドレスの評価が検索されます。ネットワークおよびURL リストでIPアドレスを重複させる必要はありません。これにより、エンド ユーザがプロキシを使用してセキュリティ インテリジェンスの評価のブロックを回避することが困難になります。
接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントを Cisco Cloud に送信するためのサポート。	Cisco Cloud サーバにイベントを送信できます。このサーバから、各種のシスコ クラウドサービスがイベントにアクセスできます。イベント送信後に、Cisco Threat Response などのクラウド アプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。このサービスを有効にすると、デバイスから、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントがシスコのクラウドに送信されます。 **[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** にある Cisco Threat Response の項目を「Cisco Cloud にイベントを送信（Send Events to the Cisco Cloud）」に変更しました。

機能	説明
シスコ クラウドサービスのリージョンサポート。	スマートライセンスへの登録時に、シスコ クラウドサービスリージョンの選択が求められるようになりました。このリージョンは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Cloud を通過するすべてのクラウド機能で使用されます。登録済みデバイスを以前のリリースからアップグレードすると、自動的に US リージョンに割り当てられます。リージョンを変更する必要がある場合は、スマートライセンスを登録解除して、改めて再登録して新しいリージョンを選択する必要があります。 [スマートライセンス（Smart License）] ページと初期デバイス セットアップ ウィザードで、ライセンス登録プロセスにステップを追加しました。また、**[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページでもリージョンを確認できます。
FTD REST API バージョン 4（v4）。	ソフトウェア バージョン 6.5 用の FTD REST API のバージョン番号が 4 になりました。API の URL の v1/v2/v3 を v4 に置き換える必要があります。v4 の API には、ソフトウェア バージョン 6.5 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソース モデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[API エクスプローラ（API Explorer）] を選択します。

機能	説明
FTD アクセス制御ルールで送信元および宛先の一致基準として使用できる TrustSec セキュリティ グループの API サポート。	FTD API を使用して、送信元または宛先のトラフィックの一致基準に TrustSec セキュリティ グループを使用したアクセス コントロール ポリシー ルールを設定できます。ISE からセキュリティ グループ タグ（SGT）のリストがダウンロードされます。SXP の更新がないかリッスンし、スタティック SGT から IP アドレスへのマッピングを取得するように、システムを設定できます。 GET /object/securitygrouptag メソッドを使用して、ダウンロードしたタグのリストを表示でき、SGTDynamicObject リソースを使用して 1 つ以上のタグを表す動的オブジェクトを作成できます。この動的オブジェクトをアクセス制御ルールで使用して、送信元または宛先のセキュリティ グループに基づくトラフィックの一致基準を定義できます。 セキュリティ グループに関連する ISE オブジェクトまたはアクセス制御ルールに変更を加えると、FDM でそれらのオブジェクトを編集しても変更が保持されます。ただし、FDM でルールを編集する場合、アクセス ルールのセキュリティ グループの基準を表示することはできません。API を使用してセキュリティグループに基づくアクセス ルールを設定する場合は、その後 FDM を使用してアクセス コントロール ポリシーのルールを編集する際に注意が必要です。 AccessRule（sourceDynamicObjects および destinationDynamicObjects 属性）、IdentityServicesEngine（subscribeToSessionDirectoryTopic および subscribeToSxpTopic 属性）、SecurityGroupTag、SGTDynamicObject の各 FTD API リソースを追加または変更しました。 イベント ビューアに、送信元と宛先のセキュリティ グループ タグと名前を列として追加しました。

機能	説明
FTD API を使用した設定のインポート/エクスポート。	FTD API を使用して、デバイス設定のエクスポートや設定ファイルのインポートが行えます。設定ファイルを編集して、インターフェイスに割り当てられている IP アドレスなどの値を変更できます。こうしたインポート/エクスポートを使用して新しいデバイス用のテンプレートを作成できます。そのため、ベースラインの構成をすばやく適用し、新しいデバイスをより迅速にオンラインにすることができます。デバイスのイメージを再作成した後、インポート/エクスポートを使用して設定を復元することもできます。または、単に一連のネットワーク オブジェクトや他の項目をデバイスのグループに配布する目的で使用することもできます。 ConfigurationImportExport のリソースとメソッド (/action/configexport、/jobs/configexports、/action/downloadconfig、/action/uploadconfig、/action/configs、/action/configimport、/jobs/configimports) を追加しました。
カスタム ファイル ポリシーの作成と選択。	FTD API を使用してカスタム ファイル ポリシーを作成し、FDM を使用してアクセス制御ルールでそれらのポリシーを選択することができます。 filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections の各 FTD API FileAndMalwarePolicies リソースを追加しました。 また、「Block Office Document and PDF Upload, Block Malware Others」と「Block Office Documents Upload, Block Malware Others」の 2 つの定義済みポリシーを削除しました。これらのポリシーを使用している場合は、ユーザが編集できるようにアップグレード中にユーザ定義のポリシーに変換されます。
FTD API を使用したセキュリティ インテリジェンス DNS ポリシーの設定。	FTD API を使用してセキュリティ インテリジェンス DNS ポリシーを設定できます。このポリシーは FDM には表示されません。 domainnamefeeds、domainnamegroups、domainnamefeedcategories、securityintelligencednspolicies の各 SecurityIntelligence リソースを追加しました。

機能	説明
Duo LDAP を使用したリモートアクセス VPN 二要素認証。	リモートアクセス VPN 接続プロファイルの 2 番目の認証ソースとして Duo LDAP を設定し、Duo パスコード、プッシュ通知、または通話を使用して二要素認証を実現できます。FTD API を使用して Duo LDAP ID ソース オブジェクトを作成する必要がありますが、FDM を使用してそのオブジェクトを RA VPN 接続プロファイルの認証ソースとして選択することができます。 duoldapidentitysources のリソースとメソッドを FTD API に追加しました。
FTD リモート アクセス VPN 接続の認可に使用する LDAP 属性マップの API サポート。	カスタムの LDAP 属性マップを使用して、リモート アクセス VPN の LDAP 認証を強化することができます。LDAP 属性マップにより、顧客固有の LDAP 属性名および値がシスコの属性名および値と同等になります。これらのマッピングを使用して、LDAP 属性値に基づいてユーザにグループ ポリシーを割り当てることができます。これらのマップは FTD API を使用してのみ設定できます。FDM を使用して設定することはできません。ただし、API を使用してこれらのオプションを設定すれば、後で FDM で Active Directory のアイデンティティ ソースを編集することで設定を保存できます。 LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping、RadiusIdentitySource の各 FTD API オブジェクト モデルを追加または変更しました。

機能	説明
FTD サイト間 VPN 接続におけるリバース ルート インジェクションとセキュリティ アソシエーション（SA）のライフタイムの API サポート。	FTD API を使用して、サイト間 VPN 接続のリバース ルート インジェクションを有効にすることができます。逆ルート注入（RRI）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。デフォルトでは、スタティック RRI が有効になっており、接続の設定時にルートが追加されます。ダイナミック RRI は無効になっています。ダイナミック RRI では、セキュリティ アソシエーション（SA）が確立されたときにのみルートが挿入され、その後 SA が切断されたときにルートが削除されます。ダイナミック RRI は IKEv2 接続でのみサポートされています。 また、接続のセキュリティ アソシエーション（SA）のライフタイムを秒単位または送信キロバイト単位で設定することもできます。ライフタイムを期限なしに設定することもできます。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。ライフタイムに到達すると、エンドポイントで新しいセキュリティ アソシエーションと秘密キーがネゴシエートされます。 FDM を使用してこれらの機能を設定することはできません。ただし、API を使用してこれらのオプションを設定すれば、後で FDM で接続プロファイルを編集することで設定を保存できます。 dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited、rriEnabled の各属性を SToSConnectionProfile リソースに追加しました。
IKE ポリシーの Diffie-Hellman グループ14、15、および 16 のサポート。	Dh グループ 14 を使用するように IKEv2 ポリシーを設定し、DH グループ 14、15、および 16 を使用するように IKEv1 ポリシーを設定できるようになりました。IKEv1 を使用している場合は、グループ 2 と 5 が今後のリリースで削除されるため、すべてのポリシーを DH グループ 14 にアップグレードしてください。また、IKEv2 ポリシーで DH グループ 24 を使用したり、IKE バージョンで MD5 を使用したりしないでください。これらも今後のリリースで削除されます。

機能	説明
変更を展開する際のパフォーマンスの向上。	システムの強化により、アクセス制御ルールを追加、編集、または削除した場合に、以前のリリースと比べて変更がより迅速に展開されるようになりました。 フェールオーバー用のハイ アベイラビリティ グループに設定しているシステムでは、展開した変更をスタンバイ デバイスに同期させるプロセスが改良され、同期がより迅速に完了するようになりました。
システム ダッシュボード上の CPU およびメモリ使用率の計算の改良。	CPU とメモリの使用率を計算する方法が改良され、システム ダッシュボードに表示される情報に、デバイスの実際の状態がより正確に反映されるようになりました。
FTD 6.5 にアップグレードした場合に履歴レポート データは使用できなくなる。	既存のシステムを FTD 6.5 にアップグレードした場合、データベース スキーマの変更のために履歴レポート データが使用できなくなります。そのため、アップグレード前の時点における使用状況データはダッシュボードに表示されません。

システムへのログイン

Firepower Threat Defense デバイスには、次の 2 つのインターフェイスがあります。

Firepower Device Manager Web インターフェイス

Firepower Device Manager はお使いの Web ブラウザで実行されます。このインターフェイスを使用して、システムを設定、管理、モニタできます。

コマンドライン インターフェイス（CLI、コンソール）

CLI はトラブルシューティングに使用します。Firepower Device Manager の代わりに、初期設定にも使用できます。

次に、これらのインターフェイスにログインし、ユーザ アカウントを管理する方法を説明します。

ユーザ ロールで表示および実行可能な対象の制御

ユーザ名はロールに割り当てられ、Firepower Device Manager で何を実行できるか、また何を表示できるかがユーザ ロールによって決まります。ローカルに定義される [管理者（admin）] ユーザにはすべての権限がありますが、別のアカウントを使用してログインすると権限が少なくなります。

Firepower Device Manager ウィンドウの右上隅にユーザ名と権限レベルが表示されます。

権限は次のとおりです。

- [管理者（Administrator）]：すべての機能を表示および使用できます。
- [読み取り/書き込みユーザ（Read-Write User）]：読み取り専用ユーザが実行できることをすべて実行できます。また、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Firepower Device Managerユーザセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- [読み取り専用ユーザ（Read-Only User）]：ダッシュボードおよび設定を表示できますが、変更することはできません。変更しようとすると、権限がないことを示すエラーメッセージが表示されます。

これらの権限は、CLI ユーザが利用できる権限とは関連していません。

Firepower Device Manager へのログイン

Firepower Device Manager を使用して、システムを設定、管理、およびモニタします。ブラウザで設定可能な機能を、コマンドライン インターフェイス（CLI）で設定することはできません。セキュリティ ポリシーを実装するには、Web インターフェイスを使用する必要があります。

Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

（注） 誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは 5 分間ロックされます。再度ログインを試みる前に待つ必要があります。

始める前に

最初は、**admin** ユーザ名を使用してのみ Firepower Device Manager にログインできます。ただし、FDM および FTD ユーザ アクセスの管理に説明されているように、外部 AAA サーバに定義されている追加ユーザの認証は設定できます。

手順

ステップ 1 ブラウザを使用して、システムのホームページ（https://ftd.example.com など）を開きます。

次のいずれかのアドレス使用できます。設定済みのものであれば、IPv4 アドレス、IPv6 アドレス、または DNS 名を使用できます。

- 管理アドレス。デフォルトでは、これは管理/診断インターフェイスの 192.168.45.45 です。

- HTTPS アクセス用に開いたデータ インターフェイスのアドレス。デフォルト（ほとんどのハードウェア プラットフォーム）では、「内部」インターフェイスで HTTPS アクセスが許可されているため、デフォルトの内部アドレス 192.168.1.1 に接続できます。 ISA 3000 の場合、デフォルトでは管理インターフェイスにのみ接続できます。

ヒント　ブラウザがサーバ証明書を認識するように設定されていない場合、信頼できない証明書に関する警告が表示されます。証明書を例外として受け入れるか、または信頼できるルート証明書ストアの証明書を受け入れます。

ステップ 2　デバイスに定義されているユーザ名とパスワードを入力し、[ログイン（Login）] をクリックします。

事前定義されたユーザであるユーザ名 **admin** を使用できます。デフォルトの admin パスワードは Admin123 です。

セッションは非アクティブの状態が 30 分間続くと期限切れになり、再度ログインするように求められます。ページの右上にある [ユーザ（user）] アイコンのドロップダウン リストから [ログアウト（Log Out）] を選択するとログアウトできます。

CLI（コマンドライン インターフェイス）へのログイン

コマンドライン インターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。

CLI にログインするには、次のいずれかを実行します。

- デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナルエミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

（注）　Firepower 2100/4100/9300 デバイスでは、コンソールポートの CLI は FXOS です。Firepower 2100 の場合は、**connect ftd** コマンドを使用して FTD CLI にアクセスできます。Firepower 4100/9300 の場合は、アプリケーションのコンソールへの接続を参照してください。FXOS CLI はシャーシ レベルのトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには FTD CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

- Firepower Threat Defense Virtual の場合は、仮想コンソールを開きます。
- SSH クライアントを使用して、管理 IP アドレスに接続します。 SSH 接続用のインターフェイスを開いている場合、データインターフェイス上のアドレスにも接続できます（管理アクセス リストの設定を参照）。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。**admin** ユーザ名（デフォルトのパスワードは **Admin123** です）または別の CLI ユーザ アカウントを使用してログインします。

ヒント

- ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法の情報については、『Cisco Firepower Threat Defense Command Reference』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。
- **configure user add** コマンドを使用して、CLI にログインできるローカルユーザアカウントを作成できます。ただし、これらのユーザは CLI のみにログインできます。Firepower Device Manager の Web インターフェイスにはログインできません。
- 外部サーバで SSH アクセス用のユーザアカウントを作成できます。SSH アクセス用の外部認証の設定については、FTD CLI（SSH）ユーザ用の外部認証（AAA）設定を参照してください。

パスワードの変更

パスワードは定期的に変更する必要があります。次の手順では、Firepower Device Manager にログインしているときにパスワードを変更する方法について説明します。

（注） CLI にログインしている場合は、**configure password** コマンドを使用してパスワードを変更できます。別の CLI ユーザのパスワードを変更するには、**configure user password** *username* コマンドを使用します。

始める前に

この手順は、ローカル ユーザにのみ適用されます。ユーザ アカウントが外部 AAA サーバで定義されている場合、そのサーバでパスワードを変更する必要があります。

手順

ステップ 1 メニューの右上にある [ユーザ（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [パスワード（Password）] タブをクリックします。
ステップ 3 現在のパスワードを入力します。
ステップ 4 新しいパスワードを入力して確認します。
ステップ 5 [変更（Change）] をクリックします。

ユーザ プロファイルの設定

ユーザ インターフェイスの設定を行い、パスワードを変更できます。

手順

ステップ 1 メニューの右上にある [ユーザ（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [プロファイル（Profile）] タブで次の設定を行い、[保存（Save）] をクリックします。

- [スケジュールするタスクのタイム ゾーン（Time Zone for Scheduling Tasks）]：バックアップや更新などのタスクのスケジュールに使用するタイムゾーンを選択します。別のゾーンを設定すると、ブラウザのタイム ゾーンはダッシュボードやイベントに使用されます。
- [カラー テーマ（Color Theme）]：ユーザ インターフェイスで使用するカラー テーマを選択します。

ステップ 3 [パスワード（Password）] タブで新しいパスワードを入力し、[変更（Change）] をクリックします。

システムの設定

ネットワークでシステムが正しく機能するためには、初期設定を完了する必要があります。展開を成功させるには、ケーブルを正しく接続し、デバイスをネットワークに挿入し、インターネットや他のアップストリーム ルータに接続するために必要なアドレスを設定する必要があります。次の手順で、このプロセスについて説明します。

始める前に

初期設定を開始する前に、デバイスにはいくつかのデフォルト設定が含まれています。詳細は、初期設定前のデフォルト設定 （32 ページ）を参照してください。

手順

ステップ 1 インターフェイスの接続 （18 ページ）

ステップ 2 初期設定の完了 （28 ページ）

設定の結果の詳細については、初期セットアップ後の設定 （35ページ）を参照してください。

インターフェイスの接続

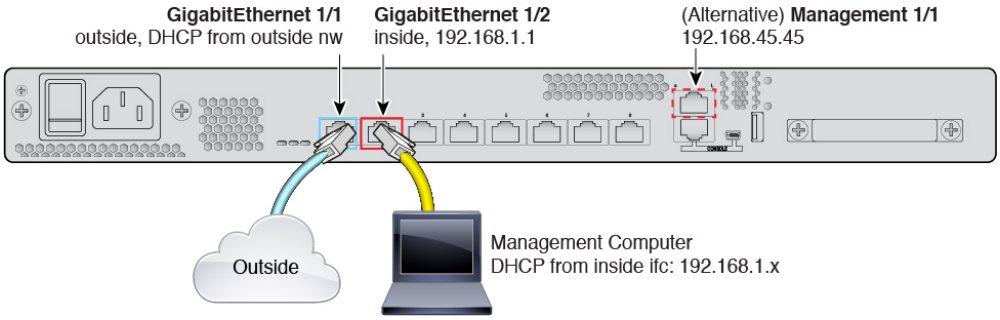
デフォルト設定では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワーク ケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

ハードウェア モデルのデフォルト設定は、内部インターフェイスにワークステーションを直接接続できるように設計されています。内部インターフェイスがブリッジグループであるデバイス モデルでは、すべてのメンバー インターフェイスに接続できます。あるいは、管理ポートに直接ワークステーションを接続することもできます。正しいネットワークでアドレスを取得するには、DHCPを使用します。インターフェイスはさまざまなネットワーク上にあるため、内部インターフェイスと管理ポートを同じネットワークに接続しようとしないでください。

内部インターフェイスまたは管理インターフェイスを、アクティブなDHCPサーバがあるネットワークに接続しないでください。接続すると、内部ポートおよび管理ポートに対して実行されている既存の DHCP サーバとの競合が生じます。ネットワークに別の DHCP サーバを使用する必要がある場合、ワークステーションを直接管理ポートに接続し、初期設定を完了してから、不要なDHCPサーバを無効にします。その後、デバイスをネットワークに接続できます。

次に、デバイスを設定するために内部インターフェイスを使用するときの、このトポロジでのシステムの配線方法を示します。

ASA 5508-X および 5516-X の配線

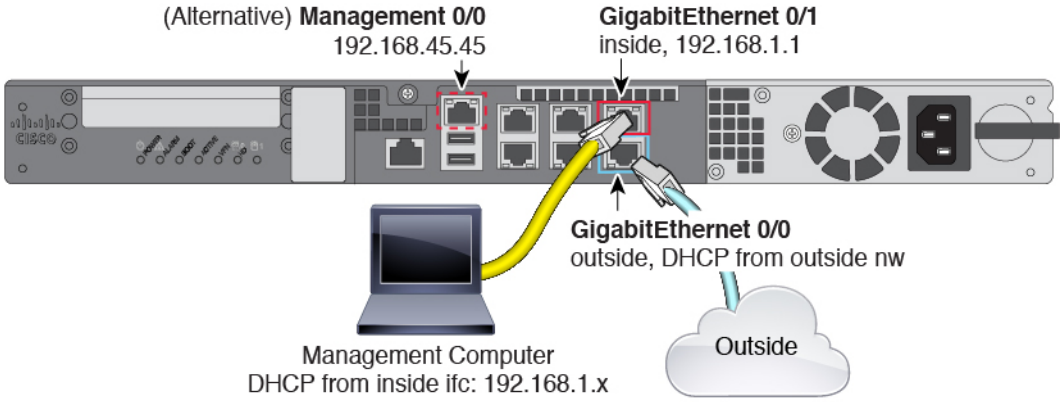


- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。

- GigabitEthernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 にそのスイッチを接続することです。ただし、スイッチのネットワーク上の他のデバイスが DHCP サーバを実行しないように徹底する必要があります。内部インターフェイス 192.168.1.1 上で実行されているデバイスと競合するためです。

ASA 5525-X、5545-X、および 5555-X の配線

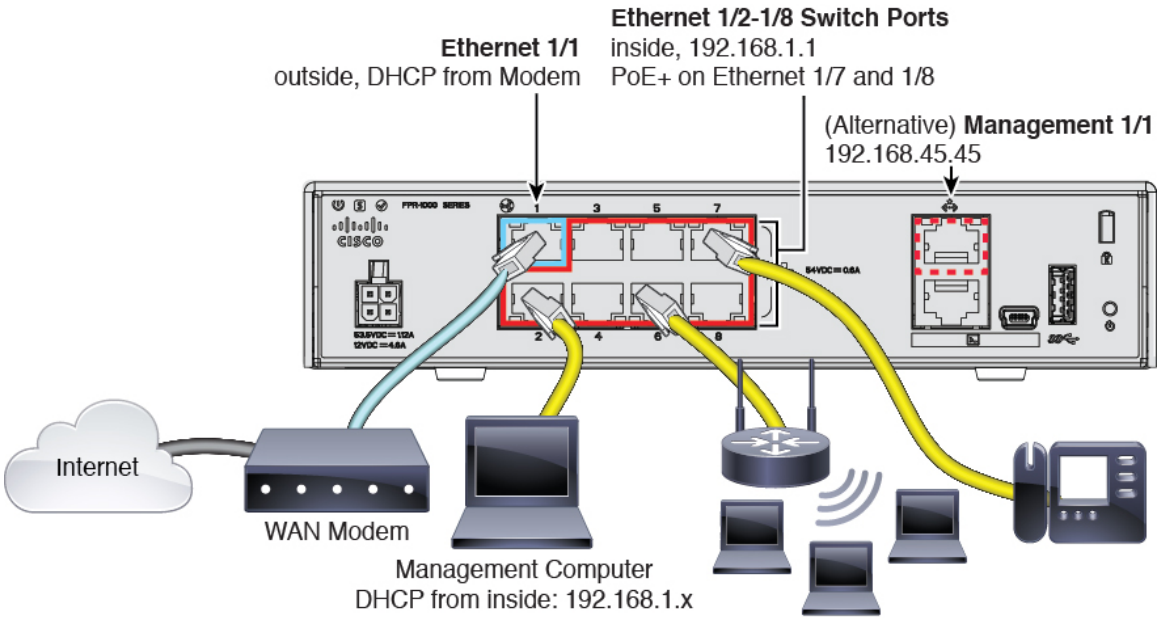


- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 0/0 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 0/1 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 0/1 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部インターフェイス 192.168.1.1 で実行中のデバイスと競合するためです。

Firepower 1010 のケーブル配線

図 *1 : Firepower 1010* のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - Ethernet 1/2 ～ 1/8：管理コンピュータをいずれかの内部スイッチ ポート（Ethernet 1/2 ～ 1/8）に直接接続します。内部にはデフォルトの IP アドレス（192.168.1.1）があり、クライアントに IP アドレスを提供するために DHCP サーバも実行されます（管理コンピュータを含む）。したがって、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
  - Management 1/1：管理コンピュータを Management 1/1 に直接接続します。または、Management 1/1 を管理ネットワークに接続します。Management 1/1 にはデフォルトの IP アドレス（192.168.45.45）があり、クライアント（管理コンピュータを含む）に IP

アドレスを提供するためにDHCPサーバも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください。

- 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

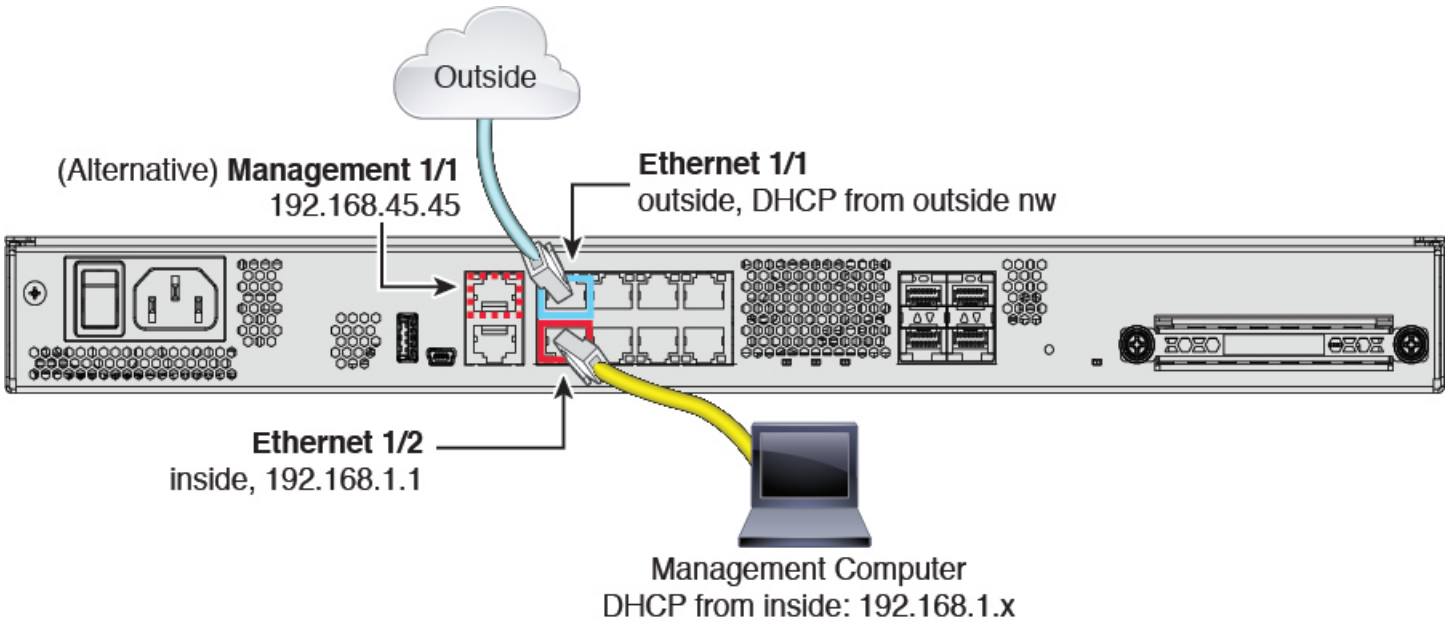
  デフォルトでは、IPアドレスはDHCPを使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。

- 内部デバイスを残りのスイッチ ポート（Ethernet 1/2 ～ 1/8）に接続します。

  Ethernet 1/7 および 1/8 は Power over Ethernet+（PoE+）ポートです。

Firepower 1120、1140 のケーブル配線

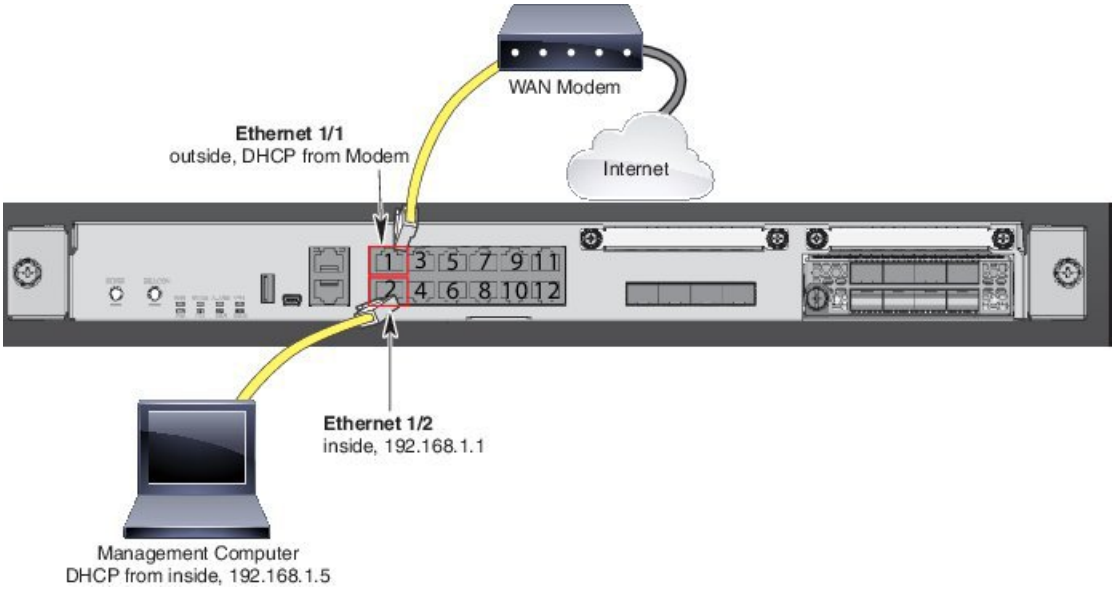
図 *2 : Firepower 1120、1140* のケーブル配線



- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCPを使用してIPアドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、Ethernet 1/2 にそのスイッチを接続することです。ただし、スイッチのネットワーク上の他のデバイスが DHCP サーバを実行しないように徹底する必要があります。内部インターフェイス 192.168.1.1 上で実行されているデバイスと競合するためです。

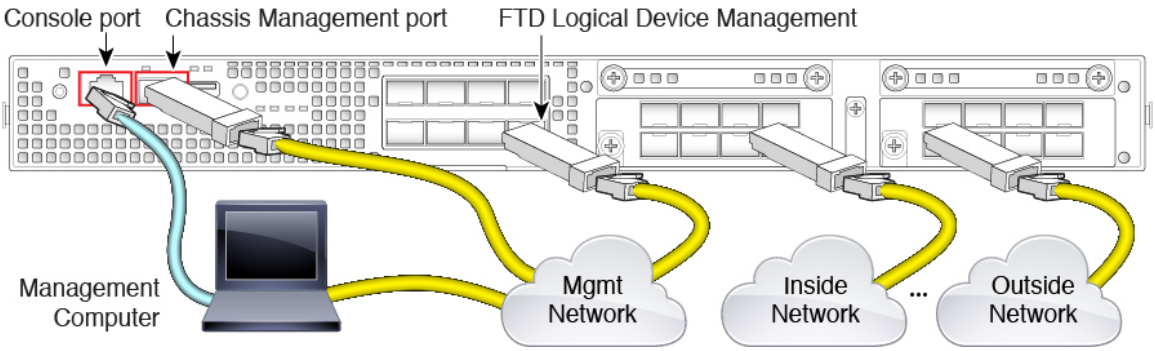
Firepower 2100の配線



- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、Ethernet 1/2 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが Ethernet 1/2、192.168.1.1 で実行中のデバイスと競合するためです。

Firepower 4100 のケーブル配線



論理デバイスの管理インターフェイスで FTD の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。FTD では、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、FTD の展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で FDM でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

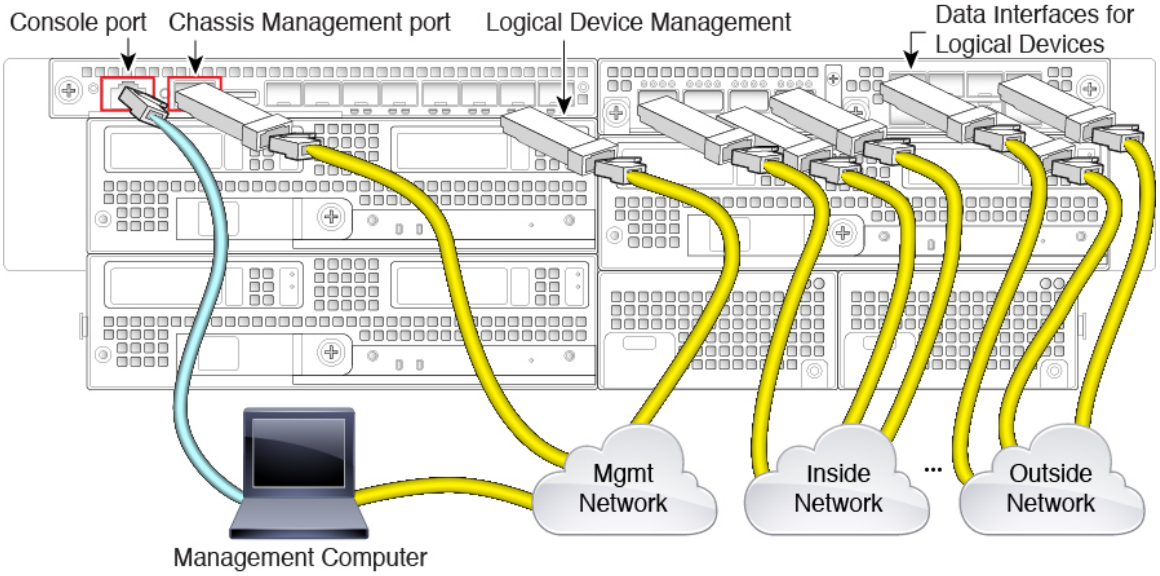
- コンソール ポート：管理コンピュータをコンソール ポートに接続して、シャーシの初期設定を実行します。Firepower 4100 には、RS-232 - RJ-45 シリアル コンソール ケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。
- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- FTD 論理デバイス管理インターフェイス：シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。

- データ インターフェイス：データ インターフェイスを論理デバイス データ ネットワークに接続します。物理インターフェイス、Etherchannel、およびブレイクアウト ポートを設定して、大容量のインターフェイスを分割できます。

  ハイ アベイラビリティの場合は、フェールオーバー/ステートリンクにデータ インターフェイスを使用します。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Hardware Installation Guide』を参照してください。

Firepower 9300 のケーブル配線



論理デバイスの管理インターフェイスで FTD の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。FTD では、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、FTD の展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で FDM でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソール ポート：管理コンピュータをコンソール ポートに接続して、シャーシの初期設定を実行します。Firepower 9300 には、RS-232 - RJ-45 シリアル コンソール ケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。

- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- 論理デバイス管理インターフェイス：1 つ以上のインターフェイスを使用して論理デバイスを管理します。シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。管理インターフェイスは論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェイスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。
- データ インターフェイス：データ インターフェイスを論理デバイス データ ネットワークに接続します。物理インターフェイス、Etherchannel、およびブレイクアウト ポートを設定して、大容量のインターフェイスを分割できます。ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークにケーブル接続できます。トラフィックはすべて、1 つのインターフェイス上のシャーシを終端とし、別の論理デバイスに到達する場合は別のインターフェイスに戻る必要があります。

  ハイ アベイラビリティの場合は、フェールオーバー/ステートリンクにデータ インターフェイスを使用します。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Hardware Installation Guide』を参照してください。

仮想ケーブル接続： Firepower Threat Defense Virtual

Firepower Threat Defense Virtual をインストールするには、http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html でお使いの仮想プラットフォームに対応した『Cisco Firepower Threat Defense Virtual Quick Start Guid』を参照してください。Firepower Device Manager は、VMware、KVM、Microsoft Azure の各仮想プラットフォームでサポートされています。

Firepower Threat Defense Virtual のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマート ライセンスを使用する場合やシステム データベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、Management 0/0 と GigabitEthernet 0/1（内部）の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management 0/0 を接続するオプションもあります。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

管理インターフェイスの IP 設定は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** で定義されている点に注意してください。**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** > **[設定の表示（View Configuration）]** に一覧されている Management0/0（診断）インターフェイスの IP アドレスと同じではありません。

Firepower Threat Defense の物理インターフェイスへの VMware ネットワーク アダプタとインターフェイスのマッピング方法

VMware Firepower Threat Defense Virtual デバイス用に最大 10 のインターフェイスを設定できます。少なくとも 4 つのインターフェイスを設定する必要があります。

Management0-0 送信元ネットワークが、インターネットにアクセスできる VM ネットワークに関連付けられていることを確認します。これは、システムが Cisco Smart Software Manager にアクセスしてシステムデータベース更新をダウンロードすることを可能にするために必要です。

OVF をインストールするときにネットワークを割り当てます。インターフェイスを設定しておけば、後で VMware クライアントを介して仮想ネットワークを変更できます。ただし、新しいインターフェイスを追加する必要がある場合は、必ずリストの最後にインターフェイスを追加してください。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤った順番になります。

次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Firepower Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を 1 つずつ増やします。すべての追加インターフェイスはデータ インターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンライン ヘルプを参照してください。

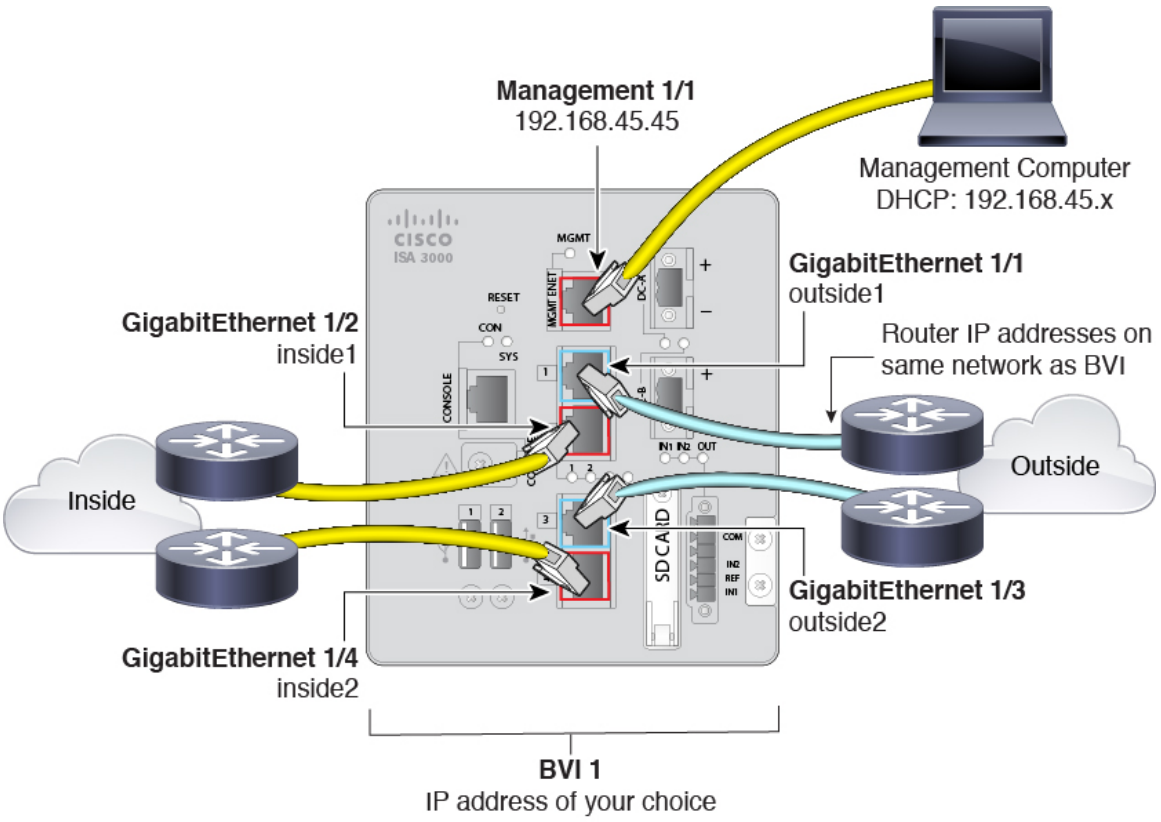
表 *2:* 送信元から宛先ネットワークへのマッピング

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
Network adapter 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
Network adapter 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部データ
Network adapter 5	GigabitEthernet0-2	GigabitEthernet0/2	データ トラフィック

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
Network adapter 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データ トラフィック
Network adapter 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データ トラフィック
Network adapter 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データ トラフィック
Network adapter 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データ トラフィック
Network adapter 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データ トラフィック

ISA 3000 のケーブル配線

図 *3 : ISA 3000*



- GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

  これらのインターフェイスによってハードウェア バイパス ペアが形成されます。

- GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

銅線ポートを備えたモデルの場合は、これらのインターフェイスによってハードウェア バイパス ペアが形成されます。ファイバはハードウェアバイパスをサポートしていません。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワーク パスを提供します。これら4つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

- Management 1/1 を管理 PC（またはネットワーク）に接続します。

初期設定の完了

Firepower Device Manager に初めてログインする際には、デバイスのセットアップ ウィザードを使用してシステムの初期設定を完了します。

ハイ アベイラビリティ設定でデバイスを使用する予定の場合は、2 台の装置でのハイ アベイラビリティの準備を参照してください。

（注） Firepower 4100/9300 および ISA 3000 ではセットアップ ウィザードがサポートされていないため、この手順はこれらのモデルには適用されません。Firepower 4100/9300 では、シャーシから論理デバイスを展開するときに、すべての初期設定が設定されます。ISA 3000 の場合は、出荷前に特別なデフォルト設定が適用されます。

始める前に

データ インターフェイスがゲートウェイ デバイス（たとえば、ケーブル モデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンター導入の場合は、これがバックボーン ルータになります。使用モデルのデフォルトの「外部」インターフェイスを使用します（インターフェイスの接続（18 ページ）および初期設定前のデフォルト設定 （32 ページ）を参照）。

次に、使用ハードウェア モデルの「内部」インターフェイスにワークステーションを接続します。内部インターフェイスがブリッジ グループであるモデルの場合、外部インターフェイス以外のデータ ポートである任意のブリッジ グループ メンバー インターフェイスに接続できます。また、管理/診断物理インターフェイスに接続できます。Firepower Threat Defense Virtual については、管理 IP アドレスに接続できることを確認するだけで十分です

（管理 IP アドレスからインターネットへの接続が必要な Firepower Threat Defense Virtual を除く）。管理/診断用の物理インターフェイスは、ネットワークに接続する必要はありません。デフォルトでは、インターネットに接続するデータ インターフェイス（通常、外部インターフェイス）を介してシステムのライセンシングとデータベースおよびその他の更新が取得されます。代わりに別の管理ネットワークを使用する場合は、初期設定の完了後、管理/診断インターフェイスをネットワークに接続して、別の管理ゲートウェイを設定できます。

手順

ステップ 1 Firepower Device Manager にログインします。

a) CLI で初期設定を完了していない場合、**https://***ip-address* にアクセスして Firepower Device Manager を開きます。このアドレスは次のいずれかになります。

- 内部インターフェイス、またはデフォルトの内部ブリッジ グループがあるモデルのいずれかの内部ブリッジ グループのデータ インターフェイスに接続している場合は、[https://192.168.1.1]。
- （Firepower Threat Defense Virtual に必要）。Management 物理インターフェイスに接続されている場合は **https://192.168.45.45**。

b) 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。

ステップ 2 これがシステムへの初めてのログインであり、CLI セットアップ ウィザードを使用していない場合、エンド ユーザ ライセンス契約を読んで承認し、管理パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 3 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

注意 [次へ（Next）] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティ ゾーンに追加されます。設定値が正しいことを確認します。

外部インターフェイス

- [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動で静的 IP アドレス、サブネット マスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。デフォルトの内部アドレスと同じサブネットに（静的に、または DHCP を介して）IP アドレスを設定しないでください（初期設定前のデフォルト設定 （32 ページ）を参照）。
- [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動で静的 IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

管理インターフェイス

- [DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。ISP は、特定の DNS サーバを使用するよう要求する場合があります。ウィザードを完了し

た後に DNS 解決が機能しない場合は、管理インターフェイスの DNS のトラブルシューティングを参照してください。

- [ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

ステップ 4 システム時刻を設定し、[次へ（Next）] をクリックします。

- [タイムゾーン（Time Zone）]：システムのタイム ゾーンを選択します。
- [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。Firepower 4100/9300 デバイスでは、FDM を使用して NTP を設定しません。FXOS で NTP を設定します。

ステップ 5 システムのスマート ライセンスを設定します。

スマート ライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマート ライセンスを設定できます。

デバイスを今すぐ登録するには、デバイスを登録するオプションを選択し、リンクをクリックして Smart Software Manager（SSM）のアカウントにログインして、新しいトークンを作成し、編集ボックスにそのトークンをコピーします。また、サービス リージョンを選択し、Cisco Success Network に使用状況データを送信するかどうかを決定する必要もあります。前述の設定については、画面上のテキストで詳しく説明されています。

デバイスをまだ登録しない場合は、評価モードオプションを選択します。これは、Cisco Defense Orchestrator を使用してデバイスを管理する場合に推奨されるオプションです。評価期間は 90 日です。後でデバイスを登録してスマートライセンスを取得する場合は、[デバイス（Device）] をクリックしてから、[スマートライセンス（Smart Licenses）] グループでリンクをクリックします。

ステップ 6 [終了（Finish）] をクリックします。

次のタスク

- オプションライセンスでカバーされている機能（カテゴリベースの URL フィルタリング、侵入インスペクション、マルウェア対策など）を使用する場合は、必要なライセンスを有効にします。オプション ライセンスの有効化と無効化を参照してください。
- 新しいシステムの場合、デフォルトの内部ブリッジ グループがあるデバイス モデル上のその他のインターフェイスは、内部ブリッジグループのメンバーとして使用可能な状態になっています。エンドポイントをインターフェイスに直接接続できます。デフォルトの単一の物理インターフェイスがあるモデルの場合、その他のデータインターフェイスを異なるネットワークに接続して、インターフェイスを設定できます。ブリッジ グループ メンバー インターフェイスの場合、ブリッジ グループからそれらのインターフェイスを削除して、追加の固有ネットワークを設定することもできます。インターフェイスの設定の詳細については、サブネットを追加する方法およびインターフェイスを参照してください。

- 内部インターフェイスまたはブリッジ グループ メンバー インターフェイスを介してデバイスを管理し、内部インターフェイスを介してCLIセッションを開きたい場合は、SSH接続に対して内部インターフェイスまたはブリッジ グループを開きます。管理アクセス リストの設定を参照してください。
- 製品の使用方法については、使用例で学習してください。Firepower Threat Defense の使用例を参照してください。

外部インターフェイスの IP アドレスを取得できない場合の対処方法

デフォルトのデバイス設定には内部インターフェイスのスタティック IPv4 アドレスが含まれています。初期デバイス セットアップ ウィザードを使用してこのアドレスを変更することはできません。ただし、後で変更することはできます。

デフォルトの内部 IP アドレスが、デバイスに接続されている他のネットワークと競合する可能性があります。これは特に、外部インターフェイスでDHCPを使用してインターネット サービスプロバイダー（ISP）からアドレスを取得する場合に該当します。一部のISPは、内部ネットワークと同じサブネットをアドレスプールとして使用しています。同じサブネットのアドレスを持つ2つのデータ インターフェイスを持つことはできないため、ISP からの競合するアドレスを外部インターフェイスに設定することはできません。

内部スタティック IP アドレスと外部インターフェイスの DHCP が提供するアドレスの間に競合がある場合は、接続図には、外部インターフェイスは管理上動作しているが IPv4 アドレスが割り当てられていないことが示されます。

この場合セットアップ ウィザードは正常に完了し、デフォルト NAT、アクセス、およびその他のポリシーや設定がすべて設定されます。競合を解消するには、次の手順に従います。

始める前に

ISP に正常に接続できることを確認します。サブネット競合がある場合外部インターフェイスのアドレスを取得できませんが、単にISPへの接続がない場合にも外部インターフェイスのアドレスを取得できません。

手順

ステップ 1 [デバイス（Device）] をクリックして、[インターフェイス（Interfaces）] サマリーのリンクをクリックします。

ステップ 2 内部インターフェイス行の [操作（Actions）] カラムにカーソルを置き、[編集（edit）] アイコン（  ）をクリックします。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブで、一意のサブネットのスタティック アドレス（192.168.2.1/24、192.168.46.1/24 など）を入力します。デフォルトの管理アドレスは 192.168.45.45/24 であるため、このサブネットは使用しないでください。

内部ネットワークでDHCPサーバがすでに実行されている場合、DHCPを使用してアドレスを取得することもできます。ただし最初に、[このインターフェイスにDHCPサーバを定義済み

（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] グループで [削除（Delete）] をクリックして、インターフェイスから DHCP サーバを削除する必要があります。

ステップ 4 [このインターフェイスにDHCPサーバを定義済み（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] 領域で [編集（Edit）] をクリックして、DHCP プールを新しいサブネットの範囲に変更します（たとえば、192.168.2.5-192.168.2.254）。

ステップ 5 [OK] をクリックしてインターフェイスの変更を保存します。

ステップ 6 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

ステップ 7 [今すぐ展開（Deploy Now）] をクリックします。

展開が完了すると、外部インターフェイスに IP アドレスが割り当てられていることが接続グラフィックで示されるはずです。内部ネットワークのクライアントを使用して、インターネットまたはその他のアップストリーム ネットワークに接続できることを確認します。

初期設定前のデフォルト設定

ローカル マネージャ（Firepower Device Manager）を使用して Firepower Threat Defense デバイスの初期設定を行う前、デバイスには次のデフォルト設定が含まれています。

多数のモデルにおいて、この設定では、Firepower Device Manager を内部インターフェイス経由で開き（通常、コンピュータをインターフェイスに直接接続する）、内部インターフェイス上に定義された DHCP サーバを使用してコンピュータに IP アドレスを提供することを前提としています。または、管理/診断用物理インターフェイスにコンピュータを接続し、DHCP を使用してアドレスを取得することもできます。ただし、一部のモデルではデフォルト設定や管理要件が異なります。詳細については、次の表を参照してください。

デフォルト設定

設定	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123 Firepower 4100/9300：論理デバイスの展開時にパスワードを設定します。	可。デフォルトパスワードを変更する必要があります。
管理 IP アドレス	192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に管理 IP アドレスを設定します。	番号 Firepower 4100/9300 の場合：可。

設定	デフォルト	初期設定時に変更できるか
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。このゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。 Firepower 4100/9300：論理デバイスの展開時にゲートウェイ IP アドレスを設定します。 Firepower Threat Defense Virtual192.168.45.1	番号 Firepower 4100/9300 の場合：可。
管理インターフェイスの DHCP サーバ	アドレス プール 192.168.45.46 ～ 192.168.45.254 で有効です。 Firepower 4100/9300：DHCP サーバが有効になっていません。 Firepower Threat Defense Virtual：DHCP サーバが有効になっていません。	不可。
管理インターフェイスの DNS サーバ	OpenDNS のパブリック DNS サーバ、208.67.220.220 および 208.67.222.222。 Firepower 4100/9300：論理デバイスの展開時に DNS サーバを設定します。	可。
内部インターフェイスの IP アドレス	192.168.1.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスが事前設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。 Firepower Threat Defense Virtual：192.168.45.1/24	不可。

設定	デフォルト	初期設定時に変更できるか
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ～ 192.168.1.254 の内部インターフェイスで実行されます。 Firepower 4100/9300：DHCP サーバが有効になっていません。 ISA 3000：DHCP サーバが有効になっていません。 Firepower Threat Defense Virtual：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	不可。
内部クライアントの DHCP 自動設定（自動設定では、WINS サーバおよび DNS サーバのアドレスをクライアントに提供）	外部インターフェイスで有効です。	可（ただし間接的）。外部インターフェイスにスタティック IPv4 アドレスを設定した場合、DHCP サーバの自動設定が無効になります。
外部インターフェイスの IP アドレス	インターネット サービス プロバイダー（ISP）または上流に位置するルータから DHCP 経由で取得されます。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスが事前設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。	可。

デバイス モデル別のデフォルト インターフェイス

初期設定時に異なる内部および外部インターフェイスを選択することはできません。設定後にインターフェイスの割り当てを変更するには、インターフェイス設定と DHCP 設定を編集します。非交換インターフェイスとして設定するには、ブリッジグループからインターフェイスを削除する必要があります。

Firepower Threat Defense デバイス	外部インターフェイス	内部インターフェイス
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet 0/0	GigabitEthernet 0/1

Firepower Threat Defense デバイス	外部インターフェイス	内部インターフェイス
Firepower 1010	Ethernet1/1	VLAN1。物理ファイアウォール インターフェイスである外部インターフェイスを除く他のすべてのスイッチポートが含まれます。
Firepower 1120、1140、1150	Ethernet1/1	Ethernet1/2
Firepower 2100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower 4100 シリーズ	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower 9300 アプライアンス	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 および GigabitEthernet1/3 GigabitEthernet1/1（外部 1）と 1/2（内部 1）、および GigabitEthernet1/3（外部 2）と 1/4（内部 2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 すべての内部インターフェイスと外部インターフェイスはBVI1の一部です。	GigabitEthernet1/2 および GigabitEthernet1/4

初期セットアップ後の設定

セットアップ ウィザードを完了すると、デバイス設定は次のようになります。この表では、個々の設定項目の値が、ユーザが明示的に選択したものとなるのか、または他の項目の設定に基づき自動的に定義されたものかを示します。「暗黙的」な設定を検証し、ニーズに合わない場合は編集します。

（注） Firepower 4100/9300 と ISA 3000 は、セットアップ ウィザードをサポートしていません。Firepower 4100/9300 では、シャーシから論理デバイスを展開するときに、すべての初期設定が設定されます。ISA 3000 の場合は、出荷前に特別なデフォルト設定が適用されます。

設定	設定（Configuration）	明示的/暗黙的な設定、またはデフォルト設定
管理者ユーザのパスワード	任意の入力値	明示的

設定	設定（**Configuration**）	明示的/暗黙的な設定、またはデフォルト設定
管理 IP アドレス	192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に設定した管理 IP アドレス。	デフォルト
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。管理ゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。 Firepower 4100/9300：論理デバイスの展開時に設定したゲートウェイ IP アドレス。 Firepower Threat Defense Virtual192.168.45.1	デフォルト
管理インターフェイス上の DHCP サーバ	アドレス プール 192.168.45.46 ～ 192.168.45.254 で有効です。 Firepower 4100/9300：DHCP サーバが有効になっていません。 Firepower Threat Defense Virtual：DHCP サーバが有効になっていません。	デフォルト
管理インターフェイスの DNS サーバ	任意の入力値 Firepower 4100/9300：論理デバイスの展開時に設定した DNS サーバ。 ISA 3000：なし。	明示的
管理ホスト名	**firepower** または任意の入力値 Firepower 4100/9300：論理デバイスの展開時に設定したホスト名。	明示的

設定	設定（Configuration）	明示的/暗黙的な設定、またはデフォルト設定
データ インターフェイスを通過する管理アクセス	データ インターフェイスの管理アクセス リスト ルールにより、内部インターフェイスを通過する HTTPS アクセスが許可されます。内部ブリッジ グループを持つモデルでは、内部ブリッジ グループの全メンバー インターフェイスがこの対象となります。SSH 接続は許可されません。IPv4 および IPv6 接続はいずれも許可されます。 Firepower 4100/9300: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。 ISA 3000：デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。 Firepower Threat Defense Virtual: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。	暗黙的
システム時間	選択したタイム ゾーンおよび NTP サーバ。 Firepower 4100/9300：システム時刻はシャーシから継承されます。 ISA 3000：なし。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。 サブスクリプション ライセンスは有効化されていません。スマート ライセンスのページに移動して、スマート ライセンスを有効化してください。	明示的
内部インターフェイスの IP アドレス	192.168.1.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1 の IP アドレスを手動で設定する必要があります。 Firepower Threat Defense Virtual：192.168.45.1/24	デフォルト
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ～ 192.168.1.254 の内部インターフェイスで実行されます。 Firepower 4100/9300：DHCP サーバが有効になっていません。 ISA 3000：DHCP サーバが有効になっていません。 Firepower Threat Defense Virtual：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	デフォルト

設定	設定（Configuration）	明示的/暗黙的な設定、またはデフォルト設定
内部クライアントに対するDHCP自動設定（自動設定では、WINSサーバおよびDNSサーバ用のアドレスがクライアントに提供）	DHCPを使用して外部インターフェイスのIPv4アドレスを取得している場合、DHCP自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP自動設定は無効になります。	明示的（ただし間接的）
データ インターフェイスの設定	• Firepower 1010：外部インターフェイス（Ethernet1/1）は物理ファイアウォール インターフェイスです。その他のインターフェイスはすべてスイッチ ポートです。これらのポートは有効になり、内部インターフェイスであるVLAN1の一部となります。これらのポートにエンド ポイントまたはスイッチを接続すると、内部インターフェイスのアドレスをDHCPサーバから取得できます。 • Firepower 4100/9300：データ インターフェイスはすべて無効になります。 • ISA 3000：すべてのデータ インターフェイスが有効になり、同じブリッジ グループ BVI1 の一部となります。GigabitEthernet1/1 および 1/3 は外部インターフェイスとなり、GigabitEthernet1/2 および 1/4 は内部インターフェイスとなります。GigabitEthernet1/1（外部1）と 1/2（内部 1）、およびGigabitEthernet1/3（外部2）と1/4（内部2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 • それ以外のすべてのモデル：外部および内部インターフェイスのみが設定され有効になります。他のすべてのデータ インターフェイスは無効になります。	デフォルト
外部の物理インターフェイスおよびIPアドレス	デバイス モデルに基づくデフォルトの外部ポート。初期設定前のデフォルト設定 （32 ページ）を参照してください。 IPアドレスはDHCPによって取得するか、入力したスタティック アドレスです（IPv4、IPv6、またはその両方）。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1 の IP アドレスを手動で設定する必要があります。	インターフェイスはデフォルト、 アドレッシングは明示的

設定	設定（**Configuration**）	明示的/暗黙的な設定、またはデフォルト設定
スタティック ルート	外部インターフェイスに対してスタティック IPv4 または IPv6 アドレスを設定すると、スタティックなデフォルト ルートも IPv4 または IPv6 用に適宜設定され、このアドレス タイプ用に定義されたゲートウェイをポイントします。DHCP を選択した場合は、デフォルト ルートは DHCP サーバから取得されます。 ネットワーク オブジェクトもこのゲートウェイ、および「any」アドレス（IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0）に合わせて作成されます。	暗黙的
セキュリティ ゾーン	内部インターフェイスを含む **inside_zone**。Firepower 4100/9300 では、このセキュリティ ゾーンにインターフェイスを手動で追加する必要があります。 外部インターフェイスを含む **outside_zone**。Firepower 4100/9300 では、このゾーンにインターフェイスを手動で追加する必要があります。 （これらのゾーンを編集して他のインターフェイスを追加することも、独自のゾーンを作成することも可能）。	暗黙的
アクセス コントロール ポリシー	inside_zone から outside_zone に送信されるすべてのトラフィックを信頼するルール。これにより、インスペクションなしで、ネットワーク内のユーザからのすべてのトラフィックを外部に出すことができ、これらの接続のすべてのリターン トラフィックが許可されます。 他のすべてのトラフィックに対するデフォルト アクションは、ブロックです。つまり、外部から開始され、ネットワークに進入しようとするすべてのトラフィックが阻止されます。 Firepower 4100/9300：事前に設定されたアクセス ルールはありません。 ISA 3000：inside_zone から outside_zone へのすべてのトラフィックを信頼するルールと、outside_zone から inside_zone へのすべてのトラフィックを信頼するルール。トラフィックはブロックされません。また、デバイスには、inside_zone 内のインターフェイスと outside_zone 内のインターフェイス間におけるすべてのトラフィックを信頼するルールもあります。これにより、内部のユーザ間のすべてのトラフィックと、外部のユーザ間のすべてのトラフィックを検査する必要がなくなります。	暗黙的

設定	設定（Configuration）	明示的/暗黙的な設定、またはデフォルト設定
NAT	インターフェイスの動的PATルールは、外部インターフェイスへの任意の IPv4 トラフィックの発信元アドレスを、外部インターフェイスの IP アドレス上の一意のポートに変換します。 補足的な非表示の PAT ルールにより、内部インターフェイスを通過する HTTPS アクセス、およびデータ インターフェイスを経由する管理アドレスのルーティングが有効化されます。これらは NAT テーブルには含まれませんが、CLI で **show nat** コマンドを使用すれば確認することができます。 Firepower 4100/9300：NAT は事前に設定されていません。 ISA 3000：NAT は事前に設定されていません。	暗黙的

設定の基本

ここでは、デバイスの設定に関する基本的な手順について説明します。

デバイスの設定

Firepower Device Manager に最初にログインするとき、基本設定の構成のセットアップ ウィザードを利用できます。ウィザードを完了したら、次の方法を使用してその他の機能を設定し、デバイス設定を管理します。

各項目が視覚的に区別しにくい場合、ユーザ プロファイルから異なるカラー スキームを選択します。ページ右上の [ユーザ（user）] アイコンのドロップダウン メニューから、[プロファイル（Profile）] を選択します。

手順

ステップ 1 [デバイス（Device）] をクリックして **[デバイス概要（Device Summary）]** に移動します。

ダッシュボードには、有効なインターフェイスやキー設定が設定されているか（緑色）またはまだ設定が必要であるかなど、デバイスの視覚的なステータスが表示されます。詳細については、インターフェイスと管理ステータスの表示 （46 ページ）を参照してください。

ステータス イメージの上にはデバイス モデルの概要、ソフトウェア バージョン、VDB（システムと脆弱性のデータベース）バージョンがあり、前回の侵入ルールは更新されています。こ

の領域には、機能を設定するためのリンクを含め、ハイ アベイラビリティ ステータスも表示されます。ハイ アベイラビリティ（フェールオーバー）を参照してください。

イメージの下には設定可能なさまざまな機能のグループがあり、各グループの設定の概要、およびシステム設定を管理するために行うことができるアクションが表示されます。

ステップ2 設定を行うか、またはアクションを実行するには、各グループのリンクをクリックします。

次に、グループの概要を示します。

- [インターフェイス（Interface）]：管理インターフェイスに加えて、少なくとも2つのデータインターフェイスを設定する必要があります。インターフェイスを参照してください。
- [ルーティング（Routing）]：ルーティングの設定。デフォルトルートを定義する必要があります。他のルートは設定に応じて必要になります。ルーティングを参照してください。
- [更新（Updates）]：地理位置情報、侵入ルールと脆弱性のデータベースの更新、およびシステム ソフトウェアのアップグレード。これらの機能を使用する場合、最新のデータベースの更新情報を確実にするため、定期的な更新スケジュールを設定します。定期的なスケジュールの更新が発生する前に更新をダウンロードする必要がある場合にも、このページにアクセスできます。システムデータベースおよびフィードの更新を参照してください。
- [システム設定（System Settings）]：このグループにはさまざまな設定が含まれます。デバイスの初期設定時に構成し、その後ほとんど変更しない基本設定などがあります。システム設定を参照してください。
- [スマートライセンス（Smart License）]：システム ライセンスの現在のステータスを示します。システムを使用するには、適切なライセンスをインストールする必要があります。一部の機能では追加のライセンスが必要です。システムのライセンスを参照してください。
- [バックアップと復元（Backup and Restore）]：システム設定をバックアップするか、以前のバックアップを復元します。システムのバックアップと復元を参照してください。
- [トラブルシューティング（Troubleshoot）]：Cisco Technical Assistance Center の依頼により、トラブルシューティング ファイルを生成します。トラブルシューティング ファイルの作成を参照してください。
- [サイト間VPN（Site-to-Site VPN）]：このデバイスとリモート デバイス間のサイト間バーチャル プライベート ネットワーク（VPN）接続。サイト間 VPN の管理を参照してください。
- [リモートアクセスVPN（Remote Access VPN）]：内部ネットワークへの外部クライアントの接続を可能にするリモートアクセス仮想プライベートネットワーク（VPN）構成です。リモート アクセス VPN の設定を参照してください。
- [詳細設定（Advanced Configuration）]：FlexConfig および Smart CLI を使用して、Firepower Device Manager を使用して設定できない機能を設定します。詳細設定を参照してください。
- [デバイス管理（Device Administration）]：監査ログを表示するか、設定のコピーをエクスポートします。監査と変更管理を参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （44 ページ）を参照してください。

次のタスク

メイン メニューの [ポリシー（Policies）] をクリックし、システムのセキュリティ ポリシーを設定します。また、これらのポリシーで必要なオブジェクトを設定するには、[オブジェクト（Objects）] をクリックします。

セキュリティ ポリシーの設定

組織のアクセプタブル ユース ポリシーを実装して不正侵入やその他の脅威からネットワークを保護するにはセキュリティ ポリシーを使用します。

手順

ステップ 1 [ポリシー（Policies）] をクリックします。

[セキュリティポリシー（Security Policies）] ページには、システムを経由する接続の一般的な流れ、およびセキュリティ ポリシーが適用される順序が表示されます。

ステップ 2 ポリシーの名前をクリックして構成します。

アクセス制御ポリシーは常に必要ですが、各ポリシータイプを構成する必要はない場合があります。次に、ポリシーの概要を示します。

- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPSなど）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。SSL 復号ポリシーの設定を参照してください。
- [アイデンティティ（Identity）]：個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。アイデンティティ ポリシーの設定を参照してください。
- [セキュリティインテリジェンス（Security Intelligence）]：ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや

URLの定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。セキュリティインテリジェンスの設定を参照してください。

- [NAT]（ネットワーク アドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。NAT の設定を参照してください。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザ グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用してURLフィルタリングを実装します。アクセス コントロール ポリシーを設定するを参照してください。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。侵入ポリシーの管理を参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （44 ページ）を参照してください。

ルールまたはオブジェクトを検索

ポリシールールまたはオブジェクトのリストで全文検索を使用すると、編集する項目を探すことができます。これは、数百のルールのあるポリシーや長いオブジェクトリストを処理するときに特に便利です。

ルールおよびオブジェクトの検索を使用するための方法は、どの種類のポリシー（侵入ポリシーを除く）またはオブジェクトでも同じです。[検索（Search）] フィールドに検索する文字列を入力し、Enter キーを押します。

この文字列はルールまたはオブジェクトの任意の部分に存在することができ、部分的な文字列でも構いません。アスタリスク（*）を、0個以上の文字と一致するワイルドカードとして使用できます。検索文字列の一部としてサポートされていないため、?、~、!、{、}、<、>、:、% は使用しないでください。;、#、& は無視されます。

文字列は、グループのオブジェクト内に出現することがあります。たとえば、IPアドレスを入力し、そのアドレスを指定するネットワークオブジェクトまたはグループを検索することができます。

完了したら、検索ボックスの右側にある [x] をクリックしてフィルタをクリアします。

変更の展開

ポリシーまたは設定を更新した場合、変更がすぐにはデバイスに適用されません。設定の変更には、次の 2 つの手順を実行します。

1. 変更を行います。
2. 変更を展開します。

この手順により、デバイスを「部分的に設定された」状態で実行することなく、関連する変更のグループ化を行えるようになります。ほとんどの場合、展開には自分の変更内容のみが含まれています。ただし、必要に応じて、システムが設定全体を再適用し、これがネットワークに悪影響を及ぼす可能性があります。さらに、いくつかの変更ではインスペクションエンジンの再起動が必要であり、この再起動中にトラフィックがドロップされます。したがって、発生し得る混乱の影響が最小限になるタイミングで変更を展開するように検討してください。

目的の変更を完了した後、次の手順を使用して変更を展開します。

注意 Firepower Device Manager を使用する Firepower Threat Defense デバイスは、インスペクションエンジンがソフトウェアのリソースの問題が原因でビジー状態である、または設定の展開中にエンジンの再起動が必要なためダウンしているときに、トラフィックをドロップします。再起動が必要な変更の詳細については、インスペクション エンジンを再起動する設定の変更 （45 ページ）を参照してください。

手順

ステップ 1 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

[保留中の変更（Pending Changes）] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

展開でインスペクションエンジンの再起動が必要な場合は、再起動を必要とする変更の詳細を示すメッセージがページに表示されます。この時点で一時的なトラフィック損失を許容できない場合は、ダイアログを閉じ、変更を展開する良いタイミングを待ちます。

アイコンが強調表示されていない場合でも、アイコンをクリックすると最後に成功した展開ジョブの日時を確認できます。展開履歴を表示するリンクもあり、クリックすると展開ジョブだけを表示するようにフィルタ処理された監査ページに移動します。

ステップ 2 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じても、ジョブは停止しません。結果は、タスク リストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴（Deployment History）] リンクをクリックすると結果が表示されます。

状況に応じて、次の手順を実行できます。

- [ジョブの命名（Name the Job）]：展開ジョブに名前を付けるには、[今すぐ展開（Deploy Now）] ボタンのドロップダウン矢印をクリックして、[展開ジョブの命名（Name the Deployment Job）] を選択します。名前を入力して [展開（Deploy）] をクリックします。名前は、ジョブの一部として監査および展開履歴に表示されるため、ジョブの検索が容易になります。

  たとえば、ジョブの名前を「DMZ Interface Configuration」にした場合、成功した展開の名前は「Deployment Completed: DMZ Interface Configuration」になります。さらに、その名前は、展開ジョブに関連する [タスク開始（Task Started）] イベントと [タスク完了（Task Completed）] イベントの [イベント名（Event Name）] として使用されます。

- [変更の破棄（Discard Changes）]：保留中の変更をすべて破棄するには、**[詳細オプション（More Options）] > [すべて破棄（Discard All）]** をクリックします。確認を求められます。

- [変更のコピー（Copy Changes）]：変更の一覧をクリップボードにコピーするには、**[詳細オプション（More Options）] > [クリップボードにコピー（Copy to Clipboard）]** をクリックします。このオプションは、変更の数が 500 未満の場合にのみ機能します。

- [変更のダウンロード（Download Changes）]：変更の一覧をファイルとしてダウンロードするには、**[詳細オプション（More Options）] > [テキストとしてダウンロード（Download as Text）]** をクリックします。自分のワークステーションにファイルを保存するように求められます。このファイルは YAML 形式です。YAML 形式に対応しているエディタがない場合は、テキスト エディタで表示できます。

インスペクション エンジンを再起動する設定の変更

設定の変更を展開した場合、次の設定またはアクションはいずれもインスペクション エンジンを再起動します。

⚠

注意 展開時に、リソース需要が高まった結果、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、一部の設定の展開では、インスペクション エンジンを再起動する必要があり、トラフィック インスペクションが中断され、トラフィックがドロップされます。

展開

一部の変更ではインスペクションエンジンの再起動が必要で、これにより一時的なトラフィック損失が発生します。インスペクションエンジンの再起動が必要な変更は、次のとおりです。

- SSL 復号ポリシーが有効化または無効化された。
- 1 つ以上の物理インターフェイス上（サブインターフェイスではありません）で MTU が変更された。
- アクセス制御ルールのファイル ポリシーを追加または削除します。
- VDB が更新された。
- 高可用性設定が作成または破棄された。

さらに、Snort プロセスがビジー状態で CPU の合計使用率が 60% を超えている場合、展開中に一部のパケットがドロップされることがあります。**show asp inspect-dp snort** コマンドを使用して、Snort の現在の CPU 使用率を確認できます。

システム データベースの更新

ルール データベースまたは VDB に更新プログラムをダウンロードした場合は、それらをアクティブにするために更新プログラムを展開する必要があります。この展開により、インスペクション エンジンが再起動される場合があります。手動で更新プログラムをダウンロードする、または更新プログラムのスケジュールを設定する場合は、ダウンロードが完了した後に、システムが変更を自動で展開する必要があるかどうかを指定できます。更新プログラムを自動的に展開するシステムがない場合は、次に変更を展開したときに更新プログラムが適用され、その際にインスペクション エンジンが再起動される場合があります。

システム アップデート

システムを再起動せずに、バイナリの変更が含まれるシステム更新プログラムまたはパッチをインストールする場合は、インスペクション エンジンを再起動する必要があります。バイナリの変更には、インスペクション エンジン、プリプロセッサ、脆弱性データベース（VDB）または共有オブジェクト ルールの変更が含まれることがあります。場合によって、バイナリの変更を含まないパッチで、Snort の再起動が必要になることもある点に注意してください。

インターフェイスと管理ステータスの表示

[デバイスの概要（Device Summary）] には、デバイスのグラフィカル ビューと管理アドレス用の設定が含まれています。[デバイスの概要（Device Summary）] を開くには、[デバイス（Device）] をクリックします。

このグラフィックの要素は、要素のステータスに基づいて色が変わります。要素をマウス オーバーすると、追加情報が提供される場合があります。このグラフィックを使用して、次の項目をモニタできます。

（注） インターフェイス ステータス情報を含む、グラフィックのインターフェイス部分は、[インターフェイス（Interfaces）] ページおよび **[モニタリング（Monitoring）] > [システム（System）]** ダッシュボードでも使用可能です。

インターフェイス ステータス

ポートをマウス オーバーすると、その IP アドレスと有効なリンク ステータスが表示されます。IP アドレスはスタティックに割り当てることもできれば、DHCP を使用して取得することもできます。ブリッジ仮想インターフェイス（BVI）をマウス オーバーすると、メンバー インターフェイスのリストが表示されます。

インターフェイス ポートは、次のカラー コーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
- グレー：インターフェイスは無効です。
- オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

内部、外部ネットワーク接続

グラフィックは、次の条件に従い、外部（またはアップストリーム）ネットワークおよび内部ネットワークに接続されているポートを示します。

- 内部ネットワーク：「inside」という名前のインターフェイスの場合のみ、内部ネットワークのポートが表示されます。その他に内部ネットワークが存在する場合、それらは表示されません。いずれのインターフェイスにも「inside」と命名していない場合は、ポートは内部ポートとしてマークされません。
- 外部ネットワーク：「outside」という名前のインターフェイスの場合のみ、外部ネットワークのポートが表示されます。内部ネットワークと同様に、この名前は必須であり、存在しない場合は、ポートは外部ポートとしてマークされません。

管理設定のステータス

グラフィックは、管理アドレス用にゲートウェイ、DNS サーバ、NTP サーバ、スマート ライセンスが設定されているかどうか、さらに、それらの設定が正常に機能しているかどうかを示します。

緑は機能が設定され正常に動作していることを示し、グレーは機能が設定されていないか、正常に動作していないことを示しています。たとえば、サーバに到達不能な場合は、DNS ボックスがグレーになります。要素をマウス オーバーすると、詳細が表示されます。

問題が見つかった場合は、次のように修正します。

- 管理ポートおよびゲートウェイ：**[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を選択します。
- DNSサーバ：**[システム設定（System Settings）]** > **[DNSサーバ（DNS Server）]** を選択します。
- NTPサーバ：**[システム設定（System Settings）]** > **[NTP]** を選択します。NTP のトラブルシューティングも参照してください。
- スマート ライセンス：[スマートライセンス（Smart License）] グループ内の [設定の表示（View Configuration）] リンクをクリックします。

システム タスク ステータスの表示

システム タスクには、さまざまなデータベースの更新の取得や適用など、直接関与することなく実行されるアクションが含まれます。これらのタスクのリストとそのステータスを表示し、これらのシステム タスクが正常に完了したことを確認できます。

タスク リストには、システム タスクと展開ジョブの統合ステータスが表示されます。監査ログにはより詳細な情報が含まれており、**[デバイス（Device）]** > **[デバイス管理（Device Administration）]** > **[監査ログ（Audit Log）]** の下にあります。たとえば、監査ログにはタスクの開始とタスクの終了ごとに個別のイベントが表示されます。一方、タスク リストではそれらのイベントが単一のエントリにマージされます。さらに、展開の監査ログエントリには、展開された変更に関する詳細情報が含まれています。

手順

ステップ 1 メインメニューの [タスクリスト（Task List）] ボタンをクリックします。

タスク リストが開き、システム タスクのステータスと詳細が表示されます。

ステップ 2 タスクのステータスを評価します。

永続的な問題がある場合は、デバイス設定を修正する必要があります。たとえば、データベースの更新を永続的に取得できない場合、デバイスの管理 IP アドレスにインターネットへのパスがないと示される場合があります。タスクの説明に挙げられている問題については、Cisco Technical Assistance Center（TAC）に問い合わせる必要があります。

タスク リストでは、次の操作を実行できます。

- これらのステータスに基づいてリストをフィルタするには、[成功（Success）] または [失敗（Failures）] ボタンをクリックします。
- タスクをリストから削除するには、[削除（delete）] アイコン（）をクリックします。

- 進行中でないすべてのタスクのリストを空にするには、[完了したタスクをすべて削除（Remove All Completed Tasks）] をクリックします。

CLI コンソールを使用した設定の監視およびテスト

FTDデバイスには、監視およびトラブルシューティングに使用できるコマンドラインインターフェイス（CLI）が組み込まれています。SSH セッションを開いてすべてのシステムコマンドにアクセスすることができますが、Firepower Device Manager で CLI コンソールを開いて、さまざまな **show** コマンド、**ping**、**traceroute**、および **packet-tracer** などの読み取り専用コマンドを使用することもできます。管理者権限を持っている場合は、**failover**、**reboot**、および **shutdown** コマンドを入力することもできます。

ページ間の移動、設定、および機能の展開を行っている間、CLI コンソールを開いたままにしておくことができます。たとえば、新しいスタティックルートを展開した後で、CLI コンソールで **ping** を使用して、ターゲットネットワークに到達できることを確認できます。

CLI コンソールは基本 FTD CLI を使用します。CLI コンソールを使用して、診断 CLI、エキスパート モード、および FXOS CLI（FXOS を使用するモデル）に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

コマンドの詳細については、『Cisco Firepower Threat Defense Command Reference』（https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。

注：

- **ping** は CLI コンソールでサポートされていますが、**ping system** コマンドはサポートされていません。
- システムは最大で2つのコマンドを同時に処理できます。そのため、別のユーザが（たとえば、REST API を使用して）コマンドを発行している場合は、その他のコマンドの完了を待ってからコマンドを入力する必要があります。問題が解決しない場合は、CLI コンソールの代わりに SSH セッションを使用します。
- コマンドは、展開された設定に基づいて情報を返します。FDM で設定を変更しても、展開していない場合は、コマンド出力に変更の結果が表示されません。たとえば、新しいスタティックルートを作成しても展開していない場合、そのルートは **show route** 出力に表示されません。

手順

ステップ 1 Web ページの右上にある [CLIコンソール（CLI Console）] ボタンをクリックします。

ステップ 2 プロンプトにコマンドを入力し、[Enter] を押します。

コマンドの中には他より出力まで時間がかかるものもありますが、しばらくお待ちください。コマンドの実行がタイムアウトになったというメッセージが表示されたら、もう一度試してください。**show perfstats** など、対話型の応答が必要なコマンドを入力した場合にも、タイムアウトエラーが発生します。問題が解決しない場合は、CLI コンソールの代わりに SSH クライアントを使用する必要があります。

このウィンドウを使用する方法について、いくつかのヒントを次に示します。

- コマンドの一部を入力した後で [Tab] キーを押すと、オート コンプリートが作動します。また、Tab はコマンド内のその位置で使用可能なパラメータをリストします。また、Tab は 3 つのレベルまでキーワードを示します。3 つのレベルを過ぎると、コマンド リファレンスを使用して詳細を確認する必要があります。
- コマンドの実行を停止するには、Ctrl+C を押します。
- ウィンドウを移動するには、ヘッダー内の任意の箇所をクリックしたままウィンドウを目的の位置にドラッグします。
- ウィンドウサイズを変更するには、[展開（Expand）]（  ）または[折りたたみ（Collapse）]（  ）ボタンをクリックします。
- [別のウィンドウに切り離す（Undock Into Separate Window）]（  ）ボタンをクリックすると、ウィンドウが Web ページから独自のブラウザ ウィンドウに切り離されます。再度ドッキングするには、[メインウィンドウにドッキング（Dock to Main Window）]（  ）ボタンをクリックします。
- クリックしてドラッグすると、テキストが強調表示されます。次に Ctrl+C を押すと、出力がクリップボードにコピーされます。
- すべての出力を消去するには、[CLIのクリア（Clear CLI）]（  ）ボタンをクリックします。
- [最後の出力のコピー（Copy Last Output）]（  ）ボタンをクリックすると、最後に入力したコマンドからの出力がクリップボードにコピーされます。

ステップ 3 完了したら、コンソール ウィンドウを閉じます。**exit** コマンドは使用しないでください。

Firepower Device Manager へのログインに使用するクレデンシャルにより CLI へのアクセスが検証されますが、コンソール使用時は実際には CLI にログインしていません。

Firepower Device Manager と REST API の併用

ローカル管理モードでデバイスをセットアップする場合、Firepower Device Manager と Firepower Threat Defense REST API を使用してデバイスを設定できます。実際には、Firepower Device Manager は REST API を使用してデバイスを設定します。

ただし、REST API は Firepower Device Manager で利用できる機能に加えて、その他の機能を提供できることを理解してください。したがって、所定の機能について、Firepower Device Manager で設定を確認するときには表示できない、REST API を使用した設定を行うことができます。

REST API で利用できて Firepower Device Manager で利用できない機能を設定する場合は、設定が完了していない可能性がある、Firepower Device Manager を使用したすべての機能（リモートアクセス VPN など）に変更を加えます。API のみの設定が維持されるかどうかは状況により異なります。多くの場合、FDM で使用できない設定に対する API の変更は FDM の編集を通じて保存されます。対象の機能について、変更が保存されているかどうかを確認する必要があります。

通常は、対象の機能について Firepower Device Manager と REST API を同時に使用することは避けてください。代わりに、デバイスを設定するために、機能ごとにいずれかの方法を選択します。

APIエクスプローラを使用して、APIのメソッドを表示でき、試すことができます。[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。