Cisco Secure Firewall Threat Defense バージョン 7.2 強化ガイド

初版：2022 年 4 月 30 日

Cisco Firepower Threat Defense Hardening Guide, Version 7.2

Firepower はネットワークの資産やトラフィックをサイバー脅威から守りますが、Firepower が「強化」されるように Firepower 自体の設定を行うことも必要です。これにより、サイバー攻撃に対する Firepower の脆弱性がさらに軽減されます。このガイドでは、お使いの Firepower 環境の強化について、特に Secure Firewall Threat Defense（Threat Defense）を中心に説明します。Firepower 環境にある他のコンポーネントの強化については、次のドキュメントを参照してください。

- *Cisco Firepower Management Center Hardening Guide, Version 7.2*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

このガイドでは、Threat Defense デバイスを設定する 2 つの異なる方法について参照していますが、関係するどちらのインターフェイスについてもマニュアルとしてその詳細を説明するものではありません。

- 一部の Threat Defense 設定は、Management Center Web インターフェイスを使用して確立できます。該当する製品の相互参照については、『』、『』を参照してください。
- Threat Defense の設定の一部は Threat Defense コマンド ライン インターフェイス（CLI）を使用して確立できます。このドキュメントで参照されているすべての CLI コマンドに関する完全な情報は、『*Cisco Firepower Threat Defense Command Reference*』で入手できます。

このドキュメント内のすべての機能の説明は、Firepower バージョン 7.2 に関連しています。このマニュアルで説明している設定のすべてが、Firepower のすべてのバージョンで使用できるわけではありません。Firepower 環境の設定の詳細については、ご使用のバージョンに対応した Firepower のマニュアルを参照してください。

セキュリティ認定準拠

お客様の組織が、米国国防総省や他の政府/自治体認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。該当する認定当局による認定を受けた後、認定に固有のガイダンス文書に従って設定を行うことで、Firepower 環境は次の認定基準に準拠するようになります。

- コモン クライテリア（CC）：国際コモン クライテリア承認アレンジメントによって確立された、セキュリティ製品の要件を定義するグローバル標準規格
- Department of Defense Information Network Approved Products List（DoDIN APL）：米国国防情報システム局（DISA）によって制定された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を DoDIN APL に変更しました。Firepower のドキュメントおよび Secure Firewall Management Center Web インターフェイスでの UCAPL の参照は、DoDIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

認定ガイダンス文書は、製品認定が完了すると個別に入手できます。この強化ガイドの公開によってこれらの製品認定の完了が保証されるわけではありません。

このドキュメントで説明している Firepower の設定は、認定機関が定める現在のすべての要件に厳密に準拠することを保証するものではありません。必要な強化手順の詳細については、認定機関から提供される本製品に関するガイドラインを参照してください。

このドキュメントでは、Threat Defense のセキュリティを強化するためのガイダンスを説明していますが、Threat Defense の一部の機能については、ここで説明している設定を行っても認定準拠がサポートされません。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Security Certifications Compliance Recommendations」を参照してください。この強化ガイドと『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』が認定固有のガイダンスと矛盾しないように努めてきました。シスコのドキュメントと認定ガイダンスとの間で不一致がある場合は、認定ガイダンスを使用するか、システムの所有者にお問い合わせください。

シスコのセキュリティ アドバイザリおよびレスポンスの確認

Cisco Product Security Incident Response Team（PSIRT）では、シスコ製品のセキュリティ関連の問題についての PSIRT アドバイザリを投稿しています。比較的重大度の低い問題については、シスコではセキュリティ レスポンスも投稿しています。セキュリティ アドバイザリおよびレスポンスは、「シスコのセキュリティ アドバイザリおよびアラート（Cisco Security Advisories and Alerts）」ページで確認できます。これらのコミュニケーション手段の詳細については、「シスコのセキュリティ脆弱性ポリシー」を参照してください。

セキュアなネットワークを維持するため、シスコのセキュリティ アドバイザリおよびレスポンスを常にご確認ください。これらは、脆弱性がネットワークにもたらす脅威を評価するうえで必要な情報を提供します。この評価プロセスのサポートについては、「セキュリティ脆弱性アナウンスメントに対するリスクのトリアージ」を参照してください。

システムの最新状態の維持

シスコでは、問題に対処し改善を行うために、Firepower ソフトウェア アップデートを定期的にリリースしています。システム ソフトウェアを最新の状態に保つことは、強化されたシステムを維持するうえで不可欠です。システムソフトウェアが適切に更新されていることを確認するには、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』、『*Firepower Management Center Upgrade Guide*』の「System Updates」の章の情報をご利用ください。

また、シスコでは、Firepower がネットワークと資産を保護するために使用するデータベースのアップデートも定期的に発行しています。Management Center によって管理される Threat Defense デバイスが最適な状態で保護されるように、管理用 Management Center の位置情報データベース、侵入ルールデータベース、および脆弱性データベースを最新の状態に維持してください。Firepower 環境のいずれかのコンポーネントを更新する場合は、アップデートに付属する「Cisco Firepower リリース ノート」を必ずお読みください。これらは、互換性、前提条件、新機能、動作の変更、警告など、重要かつリリースに固有の情報を提供します。アップデートによってはサイズが大きくなり、完了までに時間がかかる場合があります。システム パフォーマンスへの影響を軽減するため、更新はネットワークの使用量が少ない時間帯に行ってください。

位置情報データベース

地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出された IP アドレスと一致する GeoDB 情報が Firepower で検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。

Management Center Web インターフェイスから GeoDB を更新するには、**[システム（System）]** > **[更新（Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** を使用し、次のいずれかの方法を選択します。

- インターネットにアクセスせずに Management Center で GeoDB を更新します。
- インターネットにアクセスし、Management Center で GeoDB を更新します。
- インターネットにアクセスし、Management Center で GeoDB の定期的な自動更新をスケジュールします。

詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Update the Geolocation Database」を参照してください。

侵入ルール

新たな脆弱性が明らかになると、Cisco Talos Security Intelligence and Research Group（Talos）から侵入ルールの更新がリリースされます。これらの更アップデートを Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装

できます。それらの更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。

Management Center Web インターフェイスでは、侵入ルールを更新するための 3 つのアプローチが提供されており、すべて**[システム（System）]** > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]** で使用できます。

- インターネットにアクセスできない Management Center の侵入ルールを更新します。
- インターネットにアクセスできる Management Center の侵入ルールを更新します。
- インターネットにアクセスできる Management Center の侵入ルールの定期的な自動更新をスケジュールします。

詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Update Intrusion Rules」を参照してください。

また、**[システム（System）]** > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]** を使用してローカル侵入ルールをインポートすることもできます。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル侵入ルールを作成することができます。それらを Management Center にインポートする前に、『』の「Guidelines for Importing Local Intrusion Rules」、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Best Practices for Importing Local Intrusion Rules」を参照し、ローカル侵入ルールのインポートがセキュリティポリシーに準拠していることを確認します。

脆弱性データベース

脆弱性データベース（VDB）は、ホストが影響を受ける可能性がある既知の脆弱性、およびオペレーティングシステム、クライアント、アプリケーションのフィンガープリントを格納するデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

Management Center Web インターフェイスでは、VDB を更新するための 2 つのアプローチが提供されています。

- VDB（**[システム（System）]** > **[更新（Updates）]** > **[製品の更新（Product Updates）]**）を手動で更新します。
- VDB の更新（**[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]**）をスケジュールします。

詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Update the Vulnerability Database」を参照してください。

セキュリティ インテリジェンスのリストとフィード

セキュリティインテリジェンスのリストとフィードは、リストまたはフィードのエントリに一致するトラフィックをすばやくフィルタリングするために使用できる IP アドレス、ドメイン名、および URL のコレクションです。

システム提供のフィードと、事前定義されたリストがあります。カスタムフィードとリストを使用することもできます。これらのリストとフィードを表示するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）]** を選択します。 システム提供のフィードの一部として、シスコはセキュリティ インテリジェンス オブジェクトとして次のフィードを提供しています。

- セキュリティ インテリジェンス フィードは、Talos の最新の脅威インテリジェンスで定期的に更新されます。
  - Cisco-DNS-and-URL-Intelligence-Feed（[DNS Lists and Feeds] の下）
  - Cisco-Intelligence-Feed（IPアドレス用、[Network Lists and Feeds] の下）

  システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。Management Center は、5 分または 15 分ごとに Cisco-Intelligence-Feed データを更新できるようになりました。
- Cisco-TID-Feed（[Network Lists and Feeds] の下）

  TID 監視可能データのコレクションであるこのフィードを使用するには、Threat Intelligence Director を有効にして設定する必要があります。

詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Security Intelligence Lists and Feeds」を参照してください。

CC または UCAPL モードの有効化

1 つの設定で複数の強化設定変更を適用するには、Threat Defense の CC または UCAPL モードを選択します。この設定は、Management Center Web インターフェイスの Threat Defense プラットフォーム設定ポリシー（**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**）を使用して適用します。新しい設定を展開するまで、変更は Threat Defense で有効になりません。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Enable Security Certifications Compliance」を参照してください。

これらの設定オプションの 1 つを選択すると、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Security Certification Compliance Characteristics」に記載されている変更が有効になります。Firepower 環境内のアプライアンスはすべて、同じセキュリティ認定準拠モードで動作する必要があることに注意してください。

注意 この設定を有効にした後は、無効にすることはできません。CC または UCAPL モードを有効にする前に、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Security Certifications Compliance」で詳細な情報を参照してください。この設定を元に戻す必要が生じた場合は、Cisco TAC にご連絡ください。

（注） セキュリティ認定準拠を有効にしても、選択したセキュリティ モードのすべての要件への厳密な準拠が保証されるわけではありません。このドキュメントでは、CC または UCAPL モードで提供されるものを超えて展開を強化するために推奨されるその他の設定について説明します。完全準拠に必要な強化手順の詳細については、認定機関から提供される本製品に関するガイドラインを参照してください。

NetFlow によるトラフィックの可視性の向上

シスコの IOS NetFlow を使用すると、ネットワークのトラフィック フローをリアルタイムで監視できます。Threat Defense デバイスは、ランタイム カウンタの表示やリセットなど、いくつかの NetFlow 機能と連携して機能できます（**show flow-export counters** および **clear flow-export counters** CLI コマンドを参照してください）。

Management Center Web インターフェイスを使用して、NetFlow によってキャプチャされるものと同じ冗長な Threat Defense syslog メッセージを無効にすることができます。それには、**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、メニューから [Syslog] を選択します。[Syslogの設定（Syslog Settings）] タブで、[NetFlowと同等のSyslog（NetFlow Equivalent Syslogs）] チェックボックスをオンにします（どの syslog メッセージが冗長であるかを判別するには、**show logging flow-export-syslogs** CLI コマンドを使用します）。

NetFlow を使用してネットワーク デバイスを設定する場合は、これらの機能を利用できます。フロー情報がリモート コレクタにエクスポートされるかどうかに関係なく、必要に応じて NetFlow を受動的に使用できます。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「NetFlow Data in the Firepower System」を参照してください。

ローカル ネットワーク インフラストラクチャの保護

Firepower 環境では、さまざまな目的で他のネットワーク リソースとやり取りする場合があります。これらの他のサービスを強化することで、Firepower システムだけでなくネットワーク資産のすべてを保護できます。対処する必要があるすべてのものを特定するには、ネットワークとそのコンポーネント、資産、ファイアウォール設定、ポート設定、データ フロー、およびブリッジング ポイントを図式化することを試みてください。

セキュリティ上の問題を考慮した、ネットワークの運用セキュリティ プロセスを確立し、遵守します。

ネットワーク タイム プロトコル サーバーの保護

Firepower を正常に動作させるには、Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。セキュアで信頼された Network Time Protocol（NTP）サーバーを使用して、 Management Center とその管理対象デバイスのシステム時刻を同期させることを強く推奨します。

Management Center Web インターフェイスから Threat Defense デバイスの NTP 時刻同期を設定するには、**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**で Threat Defense プラットフォーム設定ポリシーを作成し、ポリシー ページ内の [時刻同期（Time Synchronization）] タブを選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure NTP Time Synchronization for Threat Defense」を参照してください。

MD5、SHA-1、または AES-128 CMAC 対称キー認証を使用して、NTP サーバーとの通信を保護することをお勧めします。

注意 Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。適切な同期を確保するため、Management Center とそのすべての管理対象デバイスについて、同じ NTP サーバーを使用するように設定してください。

ドメイン ネーム システム（DNS）の保護

ネットワーク環境で相互に通信しているコンピュータは、DNS プロトコルを利用して、IP アドレスとホスト名の間のマッピングを提供します。DNS の管理インターフェイスを介した通信をサポートするためにローカルのドメイン ネーム システムと接続するように Threat Defense デバイスを設定することは、初期設定プロセスの一部となっており、ご使用のモデルのクイック スタート ガイドで説明しています。

データ インターフェイスまたは診断インターフェイスを使用する特定の Threat Defense 機能も DNS を使用します。たとえば、NTP、アクセス コントロール ポリシー、Threat Defense /ping/traceroute により提供される VPN サービスなどがあります。DNS をデータ インターフェイスまたは診断インターフェイス用に設定するには、**[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [DNS] を選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure DNS」を参照してください。

DNS は、セキュリティを考慮して設定されていない DNS サーバーの弱点を利用するようにカスタマイズされた、特定のタイプの攻撃の影響を受ける可能性があります。業界で推奨されているセキュリティのベスト プラクティスに従って、ローカル DNS サーバーを設定してください。シスコでは http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html でガイドラインを提供しています。

セキュアな SNMP ポーリングおよびトラップ

『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure SNMP for Threat Defense」で説明されているように、SNMP ポーリングとトラップをサポートするように Threat Defense を設定できます。SNMP ポーリングを使用する場合は、SNMP 管理情報ベース（MIB）に、連絡先情報、管理情報、位置情報、サービス情報、IP アドレッシングおよびルーティング情報、伝送プロトコルの使用統計情報など、環境の攻撃に利用される可能性のあるシステムの詳細情報が含まれていることに注意する必要があります。SNMP に基づく脅威からシステムを保護するための設定オプションを選択します。

Threat Defense デバイスの SNMP 機能を設定するには、**[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [SNMP] を選択します。詳細な手順については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure SNMP for Threat Defense」を参照してください。

Threat Defense デバイスへの SNMP アクセスを強化するには、次のオプションを使用します。

- SNMP ユーザーを作成する際、以下をサポートする SNMPv3 を選択します。
  - SHA、SHA224、SHA256、SHA384 などの認証アルゴリズム。
  - AES256、AES192、および AES128 による暗号化。
  - 読み取り専用ユーザー。
- 次のオプションを使用して SNMPv3 ユーザを作成します。
  - [セキュリティレベル（Security Level）]として [特権（Priv）] を選択します。
  - [暗号化パスワードタイプ（Encryption Password Type）] として [暗号化 (Encrypted）] を選択します。

詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Add SNMPv3 Users」を参照してください。

重要 Firepower から SNMP サーバーへのセキュアな接続を確立することはできますが、認証モジュールは FIPS に準拠していません。

セキュアなネットワーク アドレス変換（NAT）

通常、ネットワーク接続されたコンピュータは、ネットワーク トラフィック内の送信元 IP アドレスや宛先 IP アドレスを再割り当てするために、ネットワーク アドレス変換（NAT）を使用します。Firepower 環境を保護し、NAT に基づく悪用からネットワーク インフラストラクチャ全体を保護するため、業界のベスト プラクティスや NAT プロバイダーからの推奨事項に従って、ネットワーク内の NAT サービスを設定します。

NAT 環境で動作するように Firepower 展開を設定する方法については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「NAT Environments」を参照してください。この情報は、環境を確立する際に次の 2 つの段階で使用します。

- お使いのハードウェア モデルの『Cisco Firepower Management Center Getting Started Guide』の説明に従って、Management Center の初期設定を実行する場合。
- 『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Add Devices to the Firepower Management Center」の説明に従って、管理対象デバイスを Management Center に登録する場合。

環境内にある FMC とその他のアプライアンスの保護

Firepower 環境には、Management Center と、Management Center によって管理されるセキュリティデバイスが含まれており、それぞれが異なるアクセス手段を提供します。管理対象デバイスは Management Center との間で情報を交換しますが、デバイスのセキュリティは環境全体のセキュリティにとって重要です。環境内にあるアプライアンスを分析して、ユーザーアクセスの保護や不要な通信ポートのクローズなど、必要に応じて強化の設定を適用してください。

ネットワーク プロトコル設定の強化

Threat Defense デバイスは、いくつかのプロトコルを使用して他のネットワーク デバイスとやり取りできます。Threat Defense デバイスや FTD が送受信するデータを保護するために、ネットワーク通信の設定を選択してください。

- デフォルトでは、Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合は、ネットワーク上でフラグメントを許可する必要がある場合があります。ただし、フラグメント化されたパケットはサービス妨害（DoS）攻撃に利用されることが多いため、フラグメントを許可しないことを推奨します。
  - Threat Defense デバイスのフラグメント設定を行うには、**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [フラグメント設定（Fragment Settings）] を選択します。
  - Threat Defense デバイスによって処理されるネットワーク トラフィック内のフラグメントを禁止するには、[チェーン（フラグメント）（Chain (Fragment)）]] オプションを 1 に設定します。

  詳細な手順については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure Fragment Handling」を参照してください。
- Management Center によって管理されている Threat Defense デバイスでは、Threat Defense との HTTPS 接続は、トラブルシューティングの目的でパケット キャプチャ ファイルをダウンロードする場合にのみ使用できます。

  パケットキャプチャのダウンロードを許可する必要がある IP アドレスに対してのみ HTTPS アクセスを許可するように FTD デバイスを設定します。Management Center Web インターフェイスの **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [HTTP] を選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure HTTP」を参照してください。
- デフォルトでは、Threat Defense は IPv4 か IPv6 を使用して任意のインターフェイスで ICMP パケットを受信できます。ただし、2 つの例外があります。
  - Threat Defense は、ブロードキャストアドレス宛ての ICMP エコー要求に応答しません。

- Threat Defense は、トラフィックが着信するインターフェイス宛てのICMPトラフィックにのみ応答します。ICMP トラフィックは、Threat Defense インターフェイス経由で離れたインターフェイスに送信できません。

ICMP に基づく攻撃から Threat Defense デバイスを保護するために、ICMP ルールを使用して、選択したホスト、ネットワーク、または ICMP タイプに ICMP アクセスを限定できます。Management Center Web インターフェイスの **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [ICMPアクセス（ICMP Access）] を選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure ICMP Access Rules」を参照してください。

- DHCP サービスと DDNS サービスを提供するように Threat Defense を設定できます（『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「DHCP and DDNS Services for Threat Defense」を参照）。これらのプロトコルはその性質上、攻撃に対して脆弱です。Threat Defense デバイスで DHCP または DDNS を設定する場合は、セキュリティに関する業界のベストプラクティスを適用し、ネットワーク資産を物理的に保護する機能を用意し、Threat Defense デバイスへのユーザー アクセスを強化することが重要です。

- Firepower 1000 シリーズ、2100 シリーズ、および Secure Firewall 3100 で、LLDP を有効にすることができます。この機能により、Threat Defense は LLDP 対応ピアとパケットを交換できます。デフォルトでは、LLDP 送受信はポートで無効になっています。LLDP を介して送信される情報は、攻撃に対して脆弱です。Threat Defense デバイスで LLDP を設定する場合は、セキュリティに関する業界のベストプラクティスを適用し、FTD デバイスへのユーザーアクセスを強化することが重要です。セキュリティを強化するために、ファイアウォールがピアから LLDP パケットを受信できるようにすることをお勧めします。このアクションにより、ファイアウォールは、その識別情報を他のピアデバイスに公開することなく、ピアデバイスに関する情報を取得できるようになります。詳細については、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Enable the Physical Interface and Configure Ethernet Settings」を参照してください。

セキュア VPN サービス

Threat Defense は、リモートアクセス仮想プライベートネットワーク（RA VPN）とサイト間仮想プライベート ネットワークの 2 種類の仮想プライベートネットワーク（VPN）サービスを提供するように設定できます。デバイスのライセンスによっては、サイト間 および RA VPN 送信に強力な暗号化を適用できる場合があります。強力な暗号化を備えた VPN には特別なライセンスが必要です。『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Licensing for Export-Controlled Functionality」を参照してください。

リモートアクセス仮想プライベートネットワーク

RA VPN 接続を介してリモートクライアント間で送受信されるメッセージの送信を保護する場合、Threat Defense は Transport Layer Security（TLS）または IPsec IKEv2 を使用できます。

Threat Defense に RA VPN 設定を展開する前に、Management Center は次のことを確認します。

- 『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「AnyConnect Licenses」に記載されている基準を満たしています。
- Threat Defense で輸出規制対象機能が有効になっています。

Threat Defense の RA VPN は、認証用の AD、LDAP、SAML ID プロバイダー、および RADIUS AAA サーバーをサポートします。ユーザーが RAVPN の AAA 設定を構成する場合、セキュリティを強化するために、次の認証方法のいずれかを使用することをお勧めします。

- [クライアント証明書とSAML（Client Certificate and SAML）]：各ユーザーはクライアント証明書と SAML サーバーの両方を使用して認証されます。
- [クライアント証明書とAAA（Client Certificate and AAA）]：各ユーザーはクライアント証明書とAAAサーバーの両方を使用して認証されます。

RA VPN は、ローカル認証と複数証明書認証をサポートしています。

- [ローカル認証（Local Authentication）]：この認証方式は、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。ローカル認証には、強力なパスワードを使用することをお勧めします。詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Associating a Local Realm with a Remote Access VPN Policy」を参照してください。
- [複数証明書認証（Multi-certificate Authentication）]：この認証方式を使用して、単一の証明書認証を使用したマシンまたはデバイスの証明書を検証できます。この認証により、デバイスが企業支給のデバイスであることを確認し、ユーザー ID 証明書を認証して VPN アクセスを許可します。この認証方式を使用することをお勧めします。詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configuring Multiple Certificate Authentication」を参照してください。

サイト間仮想プライベートネットワーク

サイト間 VPN 接続を介してリモートネットワーク間で送受信されるメッセージの送信を保護する場合、Threat Defense は IPsec IKEv1 または IPsec IKEv2 を使用できます。

サイト間 VPN には、ポリシーベース（暗号マップ）とルートベース（仮想トンネルインターフェイス（VTI））の2種類があります。セキュリティを強化するために、ルートベースの VTI VPN を使用することを推奨します。詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Site-to-Site VPNs for Firepower Threat Defense」を参照してください。

FTD VPN IKE および IPsec オプションを設定する場合（**[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [追加（Add）]** をクリックし、[IKE] または [IPsec] タブをクリック）、次の点を推奨します。

- IKEv2 を選択してください。
- 事前共有手動キーには強力なキーを使用してください。

- デフォルトの IKEv2 ポリシーを使用してください。たとえば、AES-GCM-NULL-SHA-LATEST などのポリシーです。
- [セキュリティアソシエーション（SA）の強度適用の有効化（Enable Security Association (SA) Strength Enforcement）] チェックボックスをオンにしてください。

  このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません。
- [Perfect Forward Secrecyの有効化（Enable Perfect Forward Secrecy）] オプションをオンにします。

  このオプションは、暗号化された交換ごとに一意のセッションキーを生成して使用します。この一意のセッションキーにより、交換は、後続の復号化から保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] ドロップダウンリストから、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムを選択します。

FTD VPN IKE オプションに関する詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』を参照してください。

これらのサービスを設定するには、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「VPN Overview」を参照してください。

Firepower は、幅広い暗号化アルゴリズムとハッシュ アルゴリズムをサポートしており、Diffie-Hellman グループを選択できます。強固な暗号化はシステムのパフォーマンスを低下させる可能性があるため、効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出す必要があります。利用可能なオプションと考慮すべき要素については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「How Secure Should a VPN Connection Be?」を参照してください。

FTD ユーザー アクセスの強化

Threat Defense は次の 2 種類のユーザーをサポートしています。

- 内部ユーザー：デバイスは、ローカル データベースでユーザー認証を確認します。
- 外部ユーザ：ユーザがローカル データベースに存在しない場合、システムは外部 LDAP または RADIUS の認証サーバに問い合わせます。

ユーザー管理をネットワーク環境の既存のインフラストラクチャと統合したり、二要素認証などの機能を活用したりする目的で、LDAP や RADIUS などの外部認証メカニズムを使用したユーザー アクセスの確立を検討する場合があります。外部認証を確立するには、Management Center Web インターフェイス内で外部認証オブジェクトを作成する必要があります。外部認証オブジェクトを共有して、Management Center だけでなく Threat Defense でも外部ユーザーを認証できます。

外部認証を使用するには、環境用にドメイン ネーム サーバーを設定する必要があることに注意してください。DNS の強化に関する推奨事項に必ず従ってください（「ドメイン ネーム システム（DNS）の保護」を参照してください）。

ここでのユーザー管理の説明では、Firepower バージョン 7.0 で使用可能な機能を示しています。この項で説明しているすべてのユーザーアカウント設定機能がすべての Firepower バージョンに適用されるわけではありません。システムに固有の情報については、ご使用のバージョンの Firepower のマニュアルを参照してください。

Management Center によって管理される Secure Firewall Threat Defense デバイスは、単一のユーザー アクセス手段としてコマンド ライン インターフェイスを提供します。物理デバイスの場合は、SSH、シリアル、またはキーボードとモニターの接続を使用してコマンド ライン インターフェイスにアクセスできます。特定の設定を適切に行うことで、これらのユーザーは Linux シェルにもアクセスできます。

設定権限の制限

デフォルトでは、Threat Defense デバイスは、すべての Threat Defense CLI コマンドに対して完全な管理者権限を持つ、単一の「admin」ユーザーを提供します。このユーザは、追加のアカウントを作成でき、 **configure user access** CLI コマンドを使用して、次の 2 つのレベルのアクセス権限のいずれかを付与できます。

- Basic：ユーザーは、システム設定に影響を与えない Threat Defense CLI コマンドを使用できます。
- Config：ユーザーは、重要なシステム設定機能を提供するコマンドを含めて、すべての Threat Defense CLI コマンドを使用できます。

アカウントに Config アクセス権を割り当てる場合や、Config アクセス権を持つアカウントへのアクセス権を付与するユーザーを選択する場合は、慎重に検討してください。

Linux シェルへのアクセスの制限

Management Center によって管理される Threat Defense は、自身の管理インターフェイスを介して、SSH、シリアル、またはキーボードとモニタの接続を使用した CLI アクセスのみをサポートします。このアクセスは「admin」アカウント、内部ユーザーが使用でき、外部ユーザーにも使用を許可できます。

Config レベルのアクセス権を持つユーザは、CLI の **expert** コマンドを使用して Linux シェルにアクセスできます。

⚠

注意 すべてのデバイスで、CLI の Config レベルのアクセス権または Linux シェルへのアクセス権を持つアカウントは、Linux シェルの sudoer 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムのセキュリティを強化するには、次のことを推奨します。

- Threat Defense デバイス上の外部認証されたアカウントへのアクセス権をユーザーに付与する場合は、Threat Defense デバイス上の外部認証されたすべてのアカウントが CLI Config レベルのアクセス権を持つことに注意してください。
- 新しいアカウントを Linux シェルに直接追加しないでください。Threat Defense デバイスで、**configure user add** CLI コマンドのみを使用して新しいアカウントを作成してください。
- Threat Defense の CLI コマンド **configure ssh-access-list** を使用して、Threat Defense デバイスが自身の管理インターフェイス上で SSH 接続を受け入れる IP アドレスを制限してください。

管理者はまた、**system lockdown-sensor** CLI コマンドを使用して Linux シェルへのすべてのアクセスをブロックするように Threat Defense を設定することもできます。システムのロックダウンが完了すると、Threat Defense にログインしているユーザーはすべて、Threat Defense の CLI コマンドにのみアクセスできます。これは大きな強化措置となる可能性がありますが、Cisco TAC からのホットフィックスがないと元に戻すことができないため、使用にあたっては慎重に検討してください。

内部ユーザー アカウントの強化

個々の内部ユーザーを設定する場合、Config アクセス権を持つユーザーは **configure user** Threat Defense CLI コマンドを使用することで、Web インターフェイスのログイン メカニズムを利用した攻撃に対してシステムの保護を強化できます。以下の設定を使用できます。

- ログインの最大失敗回数を制限します（**configure user maxfailedlogins**）。この回数を超えるとユーザーがロックアウトされ、管理者による再アクティブ化が必要になります。
- パスワードの最小長さを適用します（**configure user minpasswdlen**）。
- パスワードの有効日数を設定します（**configure user aging**）。
- 強力なパスワードを必須にします（**configure user strengthcheck**）。
- ユーザーが必要とするアクセスのタイプにのみ適したユーザーアクセス権限を割り当てます（**configure user access**）。
- 次回のログイン時にユーザーにアカウントパスワードのリセットを強制します（**configure user forcereset**）。

Firepower 環境でマルチテナンシーを使用している場合は、Threat Defense デバイスへのユーザアクセスを許可するときに、そのデバイスが属するドメインについて考慮してください。

詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Domain Management」を参照してください。

外部ユーザ アカウントの強化

Threat Defense のユーザ認証に外部サーバを使用する場合は、外部ユーザが常に Config 権限を持っていることに注意してください。他のユーザ ロールはサポートされていません。[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [外部認証（External Authentication）] を選択して、Management Center Web インターフェイスから Threat Defense ユーザーの外部認証を設定します。外部ユーザ アカウントを設定するには、外部認証オブジェクトを使用して LDAP または RADIUS サーバとの接続を確立する必要があります。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure External Authentication for SSH」を参照してください。

重要 LDAP または RADIUS サーバーとのセキュアな接続は Firepower からセットアップできますが、認証モジュールは FIPS に準拠していません。

- すべての Threat Defense 外部ユーザは Config アクセス権を持ち、**system lockdown-sensor** コマンドを使用して Linux シェルへのアクセスをブロックしない限り、これらのユーザは Linux シェルにアクセスできることに注意してください。Linux シェル ユーザは root 権限を取得できます。このため、セキュリティ上のリスクが生じます。
- 外部認証に LDAP を使用する場合は、[拡張オプション（Advanced Options）] で TLS または SSL 暗号化を設定します。

セッション タイムアウトの確立

Threat Defense への接続時間を制限すると、権限のないユーザが無人セッションを悪用する機会が減少します。

Threat Defense デバイスでセッション タイムアウトを設定するには、**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から[タイムアウト（Timeouts）]を選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure Global Timeouts」を参照してください。

FTD REST API の考慮事項

Secure Firewall Threat Defense の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準HTTPメソッドを使用してアプライアンス設定を表示および管理するための軽量のインターフェイスを提供します。APIについては『*Cisco Firepower Threat Defense REST API Guide*』で説明しています。

重要 TLS を使用して Threat Defense と REST API クライアント間でセキュアな接続を確立できますが、認証モジュールは FIPS に準拠していません。

バックアップの保護

システム データとその可用性を保護するため、Threat Defense デバイスの定期的なバックアップを実行してください。バックアップ機能は Management Center Web インターフェイスの **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** に表示されます。この機能については『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Backup Devices Remotely」で説明されています。保存されている FTD 設定を復元するには、Threat Defense CLI **restore** コマンドを使用します。

Management Center は、リモート デバイスにバックアップを自動的に保存する機能を備えています。強化システムでこの機能を使用することはお勧めできません。これは、FMC とリモート ストレージ デバイス間の接続を保護できないためです。

Threat Defense アップグレードを元に戻す

Management Center を使用して、Threat Defense のメジャーおよびメンテナンスアップグレードを元に戻すことができます。元に戻すと、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレード（スナップショットとも呼ばれます）の直前の状態に戻ります。パッチ適用後に元に戻すと、パッチが削除されます。元に戻す動作は、Management Center とデバイス間の通信が中断された場合にのみ発生します。高可用性や拡張性の展開では、すべてのユニットを同時に元に戻すと、元に戻す操作が成功する可能性が高くなります。

元に戻される設定には、Snort バージョン、デバイス固有の設定、デバイス固有の設定で使用されるオブジェクトが含まれます。元に戻されない設定には、複数のデバイスで使用できる共有ポリシーが含まれます。

アップグレードが成功した後に元に戻す必要があると思われる場合は、管理センターで **[システム（System）] > [更新（Updates）]** を選択して Threat Defense をアップグレードし、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを設定します。デフォルトで、このオプションは有効になっています。このオプションを有効にすることを推奨します。

復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。詳細については、『*Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2*』の「Revert the Upgrade」を参照してください。

データのエクスポートの保護

Threat Defense CLI は、特定のファイルを Threat Defense からローカル コンピュータにダウンロードする機能を備えています。この機能は、システムのトラブルシューティング時に Cisco

TACに提供する情報を収集できるように提供されているものであり、必要な場合以外は使用しないでください。Threat Defense からダウンロードするファイルを保護するための予防措置を講じてください。ダウンロード時は使用可能なオプションから最も安全なものを選択し、データの保存場所となるローカル コンピュータを保護してください。また、TAC にファイルを送信する際は使用可能なプロトコルから最も安全なものを使用してください。特に、次のコマンドを使用する場合に起こりうるリスクに注意してください。

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  export オプションでは TFTP のみサポートされています。

- **file copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  このコマンドは、セキュリティで保護されていないFTPを使用してリモートホストにファイルを転送します。

- **copy [/noverify] /noconfirm** {**/pcap capture:/**[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

  src_url および *dest_url* の次のオプションは、コピーされたデータを保護する方法を提供します。

  - 内部フラッシュ メモリ
  - システム メモリ
  - オプションの外部フラッシュ ドライブ
  - パスワードで保護された HTTPS
  - パスワードで保護されたSCP（SCPサーバーでターゲットインターフェイスを指定）
  - パスワードで保護された FTP
  - パスワードで保護された TFTP（TFTP サーバーでターゲット インターフェイスを指定）

  強化システムでは、*src_url* および *dest_url* で次のオプションを使用しないことをお勧めします。

  - SMB UNIX サーバーのローカル ファイル システム
  - クラスタ トレース ファイル システム（セキュリティ認定準拠が有効になっているシステムではクラスタはサポートされません）

- **cpu profile dump** *dest_url*

  dest_url の次のオプションは、データ ダンプをセキュリティで保護する方法を提供します。

  - 内部フラッシュ メモリ
  - オプションの外部フラッシュ ドライブ
  - パスワードで保護された HTTPS

- SMB UNIX サーバーのローカル ファイル システム
- パスワードで保護されたSCP（SCPサーバーでターゲットインターフェイスを指定）
- パスワードで保護された FTP
- パスワードで保護された TFTP（TFTP サーバーでターゲット インターフェイスを指定）

強化システムでは、*src_url* および *dest_url* のオプションでクラスタ ファイル システムを使用しないことをお勧めします。

- **file secure-copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  SCP を使用してリモート ホストにファイルをコピーします。

Secure Syslog

Threat Defense は、syslog メッセージを外部の syslog サーバに送信できます。syslog 機能を設定する場合は、セキュアなオプションを選択します。

1. **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシーを作成し、目次から [syslog] を選択します。[syslog サーバ（Syslog Servers）] タブで syslog サーバを追加するときに、必ずTCPプロトコルを選択し、[セキュアな syslog を有効にする（Enable secure syslog）] チェック ボックスをオンにします。これらのオプションは、デバイス設定の別の場所で上書きしなければ、Threat Defense によって生成される syslog メッセージに適用されます。

（注） デフォルトでは、セキュアな syslog が有効になっていると、TCP を使用する syslog サーバーがダウンした場合に Threat Defense はトラフィックを転送しません。この動作を無効にするには、[TCP syslog サーバーがダウンした場合にユーザー トラフィックの通過を許可する（Allow user traffic to pass when TCP syslog server is down）] チェック ボックスをオンにします。

2. プラットフォーム設定ポリシーからロギング設定を継承するように、アクセス コントロール ポリシーのロギングを設定します（**[Policies] > [Access Control]** <each policy> の [ロギング（Logging）] で、[デバイスに展開されているFTDプラットフォーム設定ポリシーで設定されたsyslog設定を使用する（Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）] チェックボックスをオンにします）。

これら 2 つの設定を適用すると、Threat Defense の syslog は次のように動作します。

- プラットフォーム設定ポリシーの syslog 設定は、デバイスとシステムのヘルスに関連する syslog メッセージ、およびネットワーク設定に関連する syslog メッセージに適用されます。
- 『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuration Locations for Syslogs for Configuration and Security Intelligence Events (All

Devices)」に一覧表示されているいずれかの場所で、アクセス コントロール ポリシーの設定をオーバーライドしない限り、プラットフォーム設定の syslog 設定は、接続イベントとセキュリティ インテリジェンス イベントの syslog に適用されます。これらのオーバーライドではセキュアな syslog オプションは提供されないため、セキュアな環境での使用はお勧めできません。

- 『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuration Locations for Syslogs for Intrusion Events」に一覧表示されているいずれかの場所で、アクセス コントロール ポリシーの設定をオーバーライドしない限り、プラットフォーム設定ポリシーの syslog 設定は、侵入イベントの syslog に適用されます。これらのオーバーライドではセキュアな syslog オプションは提供されないため、セキュアな環境での使用はお勧めできません。

ログイン バナーのカスタマイズ

ユーザが CLI にログインするときにユーザに必要な情報を伝えるように、Threat Defense デバイスを設定できます。セキュリティの観点から、ログインバナーでは不正アクセスを防止する必要があります。次の例のようなテキストを考慮してください。

> 安全なデバイスにログインしました。このデバイスにアクセスする権限を持っていない場合は、すぐにログアウトしないと犯罪と認識されるおそれがあります。

Threat Defense デバイスのログイン バナーを設定するには、**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** で Threat Defense プラットフォーム設定ポリシー作成し、目次から [バナー（Banner）] を選択します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure Banners」を参照してください。

ネットワークユーザーの権限のあるログイン、認識、および制御をサポートするサーバーへのセキュアな接続

Firepower アイデンティティ ポリシーは、アイデンティティ ソースを使用してネットワーク ユーザーを認証し、ユーザーを認識し制御する目的でユーザー データを収集します。ユーザ アイデンティティ ソースを確立するには、 Management Center または管理対象デバイスと、次のいずれかのタイプのサーバとの間の接続が必要です。

- Microsoft Active Directory
- Linux OpenLDAP
- RADIUS

重要 LDAP、Microsoft AD、または RADIUS サーバへのセキュアな接続を Firepower から設定できますが、認証モジュールは FIPS に準拠していません。

（注） 外部認証に LDAP または Microsoft AD を使用する場合は、「外部ユーザ アカウントの強化 （15 ページ）」の情報を確認してください。

（注） Firepower はこれらの各サーバを使用して、ユーザ アイデンティティ機能の候補のさまざまな組み合わせをサポートします。『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「About User Identity Sources」を参照してください。

Active Directory サーバーおよび LDAP サーバーとの接続の保護

Firepower には「レルム」と呼ばれるオブジェクトがあります。レルムは、Active Directory サーバーまたは LDAP サーバー上のドメインに関連付けられている接続設定を記述するものです。レルム設定の詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Create and Manage Realms」を参照してください。

Management Center Web インターフェイスの **[システム（System）] > [統合（Integration）] > [レルム（Realms）]** でレルムを作成する場合は、AD サーバーまたは LDAP サーバーとの接続を保護するため、次の点に注意してください。

Active Directory サーバーに関連付けられるレルムの場合：

- [AD 参加パスワード（AD Join Password）] と [ディレクトリ パスワード（Directory Password）] で強力なパスワードを選択します。
- Active Directory レルムにディレクトリを追加する際に次のようにします。
  - [暗号化（Encryption）] モードとして [STARTTLS] または [LDAPS] を選択します（[なし（None）] は選択しないでください）。
  - Active Directory ドメイン コントローラへの認証に使用する [SSL 証明書（SSL Certificate）] を指定します。世界的に知られていて信頼できる認証局が生成した証明書を使用することをお勧めします。

LDAP サーバーに関連付けられるレルムの場合：

- [ディレクトリ パスワード（Directory Password）] で強力なパスワードを選択します。
- LDAP レルムにディレクトリを追加する際に次のようにします。
  - [暗号化（Encryption）] モードとして [STARTTLS] または [LDAPS] を選択します（[なし（None）] は選択しないでください）。
  - LDAP サーバーへの認証に使用する [SSL 証明書（SSL Certificate）] を指定します。世界的に知られていて信頼できる認証局が生成した証明書を使用することをお勧めします。

RADIUS サーバーとの接続の保護

RADIUS サーバとの接続を設定するには、Management Center Web インターフェイスの **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[RADIUS サーバ グループ（RADIUS Server Group）]** で RADIUS サーバ グループ オブジェクトを作成し、そのグループに RADIUS サーバを追加します。RADIUS サーバとの接続を保護するには、[新しい RADIUS サーバ（New RADIUS Server）] ダイアログで次のオプションを選択します。

- 管理対象デバイスと RADIUS サーバ間でデータを暗号化するための [キー（Key）] と [キーの確認（Confirm Key）] を指定します。
- セキュアなデータ送信をサポートできる接続用のインターフェイスを指定します。

（注） Firepower は、リモート アクセス VPN（ユーザ アイデンティティ ソースとして使用されます）を提供するように環境内の管理対象 Threat Defense デバイスが設定されている場合にのみ、ユーザ アイデンティティのために RADIUS サーバと接続します。リモート アクセス VPN の設定と保護の詳細については、「ネットワーク プロトコル設定の強化」を参照してください。

セキュアな証明書登録

Enrollment over Secure Transport（EST）を使用した証明書登録の設定

安全なチャネルを介した Threat Defense の証明書登録を設定できます。Enrollment over Secure Transport（EST）は、CA から ID 証明書を取得するためにデバイスによって使用されます。EST は、セキュアなメッセージ転送に TLS を使用します。

EST の設定方法：

1. [オブジェクト（Objects）]>[オブジェクト管理（Object Management）] を選択し、ナビゲーションウィンドウから [PKI] > [証明書登録（Cert Enrollment）] を選択します。
2. [証明書登録の追加（Add Cert Enrollment）] をクリックし、[CA情報（CA Information）] タブをクリックします。
3. [登録タイプ（Enrollment Type）] ドロップダウンリストから、[EST] を選択します。

Threat Defense に EST サーバー証明書を検証させたくない場合は、[ESTサーバー証明書の検証を無視する（Ignore EST Server Certificate Validations）] チェックボックスをオンにしないことをお勧めします。デフォルトでは、Threat Defense は EST サーバー証明書を検証します。EST 登録タイプは、RSA キーと ECDSA キーのみをサポートし、EdDSA キーをサポートしません。詳細については、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Certificate Enrollment Object EST Options」を参照してください。

Management Center と Threat Defense のバージョン 7.0 以降では、RSA キーサイズが 2048 ビット未満の証明書と、SHA-1 を使用するキーは登録できません。7.0 より前のバージョンを実行している Threat Defense を管理する Management Center 7.0 で該当する制限をオーバーライドす

るには、[Weak-Cryptoの有効化（Enable Weak-Crypto）]オプションを使用できます（**[デバイス（Devices）] > [証明書（Certificates）]**）。デフォルトでは、Weak-Crypto オプションは無効になっています。weak-crypto キーを有効にすることは推奨しません。weak-crypto キーは、キーサイズが大きいキーほど安全ではないためです。FMC および FTD バージョン 7.0 以降では、weak-crypto を有効にして、ピア証明書の検証などを可能にすることができます。ただし、この設定は証明書の登録には適用されません。

証明書の検証の設定

特定の CA 証明書を使用して SSL や IPSec クライアントを検証したり、CA 証明書を使用して SSL サーバーからの接続を検証したりできます。検証使用法の種類を設定する方法：

1. [オブジェクト（Objects）]>[オブジェクト管理（Object Management）]を選択し、ナビゲーションウィンドウから [PKI] > [証明書登録（Cert Enrollment）] を選択します。
2. [証明書登録の追加（Add Cert Enrollment）] をクリックし、[CA情報（CA Information）] タブをクリックします。
3. [検証用法（Validation Usage）] ：VPN 接続中に証明書を検証するオプションから選択します。
   - [IPsecクライアント（IPsec Client）]：サイト間 VPN 接続の IPSec クライアント証明書を検証します。
   - [SSLクライアント（SSL Client）]：リモートアクセス VPN 接続の試行中に SSL クライアント証明書を検証します。
   - [SSLサーバー（SSL Server）]：Cisco Umbrella サーバー証明書など、SSL サーバー証明書を検証する場合に選択します。

詳細については、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Adding Certificate Enrollment Objects」を参照してください。

オブジェクトグループ検索設定の強化

動作中、Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイスオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [詳細設定（Advanced Settings）]**）。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイスオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。

オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセスコントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。1000 シリーズ、2110、2120 などのローエンドの Firepower デバイスでは、CPU 使用率の増大によりデバイスが遅くなります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネッ

ト運用が改善されます。デフォルトでは、オブジェクトグループ検索の設定が有効になっています。

オブジェクトグループの検索を有効にしてから、デバイスを設定し、しばらくの間操作した場合、この機能を無効にすると、望ましくない結果になる可能性があります。オブジェクトグループの検索を無効にすると、既存のアクセス制御ルールがデバイスの実行コンフィギュレーションで拡張されます。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。デバイスが正常に動作している場合は、一度有効にしたオブジェクトグループ検索を無効にしないでください。詳細については、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Configure Object Group Search」を参照してください。

サポート コンポーネントの強化

Threat Defense ソフトウェアは、基盤となる複雑なファームウェアとオペレーティング システム ソフトウェアに依存しています。これらの基盤となるソフトウェア コンポーネントには独自のセキュリティ リスクが潜んでおり、対処する必要があります。

- セキュリティ上の問題を考慮した、ネットワークの運用セキュリティ プロセスを確立してください。
- Threat Defense モデル 2100、4100、および 9300 デバイスでは、Threat Defense を実行する Firepower Extensible Operating System を保護してください。『*CiscoFirepower 4100/9300 FXOS Hardening Guide*』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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