システム設定

ここでは、[システム設定（System Settings）] ページでグループ化されているさまざまなシステム設定の設定方法について説明します。設定は、システムの機能全体を網羅しています。

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、デバイスの Firepower Device Manager ウェブまたは管理アドレスの CLI インターフェイスにアクセスできます。システム アクセスは、ユーザ名/パスワードのみで保護されています。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセス リストを設定し、さらにレベルの高い保護を提供することができます。

注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスへのアクセスを削除し、「任意」のアドレスへのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセス リストを設定する場合は、特に注意してください。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックし、[システム設定（System Settings）] > [管理アクセス リスト（Management Access List）] リンクをクリックします。
すでにシステム設定ページにアクセスしている場合、目次の [管理アクセス リスト（Management Access List）]をクリックします。

ルールのリストは、指定したポートへのアクセスが許可されるアドレスを定義します。Firepower Device Manager（HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 2 管理アドレスのルールを作成するには、以下の手順に従います。

a) [+]をクリックし、次のオプションを入力します。

- [プロトコル（Protocol）] : ルールが HTTPS（ポート 443）または SSH（ポート 22）用かを選択します。
- [IP アドレス（IP Address）] : システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4](0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

b) [追加（Add）]をクリックします。

診断ロギングの設定

診断ロギングは、接続に関係していないイベントの syslog メッセージを提供します。個々のアクセス コントロール ルール内に接続ロギングを設定します。次に、診断メッセージのロギングを設定する方法について説明します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [ロギングの設定（Logging Settings）] リンクをクリックします。
[システム設定（System Settings）]ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）]をクリックします。

ステップ 2 [診断ログの設定（Diagnostic Log Settings）] > [オン（On）] をクリックします。
このページの残りのフィールドを設定しても、この設定を有効にしない限り、診断ログ メッセージは生成されません。

ステップ 3 診断ログ メッセージを表示する各々の場所のスライダを[オン（On）]にしてから、最小重大度レベルを選択します。
次の場所にメッセージをロギングすることができます。

- [コンソール（Console）]：コンソール ポートの CLI にログインすると診断ログ メッセージが表示されます。**show console-output** コマンドを使用して、他のインターフェイス（管理アドレスを含む）への SSH セッションでこれらのログを表示することもできます。
- [Syslog]：診断ログ メッセージは、指定した外部 syslog サーバに送信されます。[+]をクリックして、syslog サーバのオブジェクトを選択し、ポップアップ ダイアログボックスで[OK]をクリックします。サーバのオブジェクトがすでに存在しなくなっている場合、[Syslog サーバの追加（Add Syslog Server）]をクリックして作成します。

ステップ 4 [保存（Save）]をクリックします。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。

表 *1*：*syslog* メッセージの重大度

レベル番号	重大度	説明
0	**emergencies**	システムが使用不可能な状態です。
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態です。
5	**notification**	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。

（注） Firepower Threat Defenseは、重大度 0（緊急）の syslog メッセージを生成しません。

DHCP サーバの設定

DHCP サーバは、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。Firepower Threat Defenseデバイスは、インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク構成パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャスト アドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。DHCP サーバは、BOOTP 要求をサポートしていません。

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。つまり、スイッチがあるとしても、サーバとクライアントの間にルータを介在させることはできません。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [DHCP サーバ（DHCP Server）] リンクをクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [DHCP サーバ（DHCP Server）]をクリックします。

リストには、DHCP サーバを設定したインターフェイスと、サーバが有効にされているかどうか、そしてサーバのアドレス プールが表示されます。

（注） サーバを削除するには、サーバのごみ箱アイコン（）をクリックします。

ステップ 2 自動設定とグローバル設定を設定します。
DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) 自動設定を利用する場合、[自動設定を有効にする（Enable Auto Configuration）]>[オン（On）] をクリックしてから（スライダは右側に移動）、は、DHCP を介してアドレスを取得するインターフェイスを [次のインターフェイスから取得（From Interface）] で選択します。
b) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバル オプションを設定します。これらの設定は、DHCP サーバをホストするすべてのインターフェイスで DHCP クライアントに送信されます。

- [プライマリ WINS IP アドレス（Primary WINS IP Address）]、[セカンダリ WINS IP アドレス（Secondary WINS IP Address）] ：Windows インターネット ネーム サービス（WINS）サーバ クライアントのアドレスは、NetBIOS の名前解決に使用されます。

- [プライマリDNS IP アドレス（Primary DNS IP Address）]、[セカンダリ DNS IP アドレス（Secondary DNS IP Address）]：ドメイン ネーム サーバ（DNS）のサーバ クライアントのアドレスは、ドメインの名前解決に使用されます。OpenDNS パブリック DNS サーバを設定するには、[OpenDNS を使用する（Use OpenDNS）]をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

c) [保存（Save）]をクリックします。

ステップ 3 次のいずれかを実行します。

- まだリストされていないインターフェイスのDHCPサーバを設定するには、[+]をクリックします。
- 既存のDHCPサーバを編集するには、そのサーバの編集アイコン（  ）をクリックします。

ステップ 4 サーバ プロパティを設定します。

- [DHCP サーバを有効にする（Enable DHCP Server）]：サーバを有効にするかどうかを決定します。サーバを設定することができますが、使用する準備が整うまでサーバは無効にしておきます。
- [インターフェイス（Interface）]：クライアントにDHCPアドレスを提供するインターフェイスを選択します。インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。
- [アドレス プール（Address Pool）]：アドレスを要求するクライアントにサーバが提供できるIPアドレスの最小から最大までの範囲。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、10.100.10.12-10.100.10.250 のように指定します。

ステップ 5 新しいサーバの [追加（Add）]と、既存のサーバの [保存（Save）] をクリックします。

DNS の設定

ドメインネームシステム（DNS）サーバは、IPアドレスのホスト名の解決に使用されます。これらのサーバは管理インターフェイスによって使用されます。DNS サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変更することができます。

configure network dns servers コマンドと **configure network dns searchdomains** コマンドを使用して、CLI で DNS 設定を変更することも可能です。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [DNS サーバ（DNS Server）] リンクをクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [DNS サーバ（DNS Server）]をクリックします。

ステップ 2 [プライマリ、セカンダリ、ターシャリ DNS IP アドレス（Primary, Secondary, Tertiary DNS IP address）]に、DNS サーバの IP アドレスを優先順位に従って 3 つまで入力します。
使用していたプライマリ DNS サーバからの応答がなくなると、セカンダリが使用され、最後にターシャリが使用されます。

OpenDNS パブリック DNS サーバを設定するには、[OpenDNS を使用する（Use OpenDNS）]をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

ステップ 3 [ドメイン検索名（Domain Search Name）]に、example.com などのネットワークのドメイン名を入力します。
このドメインは、完全修飾されていないホスト名に追加されます（たとえば serverA.example.com ではなく serverA のようなホスト名）。

ステップ 4 [保存（Save）]をクリックします。

管理 IP アドレスの設定

CLI セットアップ ウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。これは、Firepower Device Manager の Web インターフェイス および CLI にアクセスするアドレスです。

Firepower Device Manager のセットアップ ウィザードを使用すると、管理アドレスとゲートウェイアドレスはデフォルトのまま変更されません。

必要に応じて、Firepower Device Manager を通じてこれらのアドレスを変更できます。また、CLI で **configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用することで、管理アドレスとゲートウェイを変更することもできます。または、CLIから設定する場合は、DHCP または IPv6 自動設定を使用するように管理インターフェイスを設定できます。

注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に、Firepower Device Manager にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

手順

ステップ 1 メニューでデバイスの名前をクリックし、[システム設定（System Settings）] > [デバイス管理 IP（Device Management IP）] リンクをクリックします。
すでにシステム設定ページを開いている場合、目次の [デバイス管理 IP（Device Management IP）] をクリックします。

ステップ 2 管理アドレス、サブネットマスクまたはIPv6プレフィックス、およびIPv4、IPv6、またはその両方のゲートウェイを設定します。
少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

ステップ 3 [保存（Save）]をクリックして警告を読み、[OK] をクリックします。

デバイスのホスト名の設定

デバイス ホスト名を変更できます。

CLI で **configure network hostname** コマンドを使用してホスト名を変更することもできます。

注意 ホスト名を使用してシステムに接続しているときにホスト名を変更すると、変更はただちに適用されるため、変更を保存するときに Firepower Device Manager へのアクセスが失われます。デバイスに接続し直す必要があります。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[システム設定（System Settings）] > [ホスト名（Hostname）] リンクをクリックします。
すでにシステム設定ページを開いている場合、目次の [ホスト名（Hostname）]をクリックします。

ステップ 2 新しいホスト名を入力します。

ステップ 3 [保存（Save）]をクリックして警告を読み、[続行（Proceed）] をクリックします。

Network Time Protocol（NTP）の設定

システムの時刻を定義するには、Network Time Protocol（NTP）サーバを設定する必要があります。NTP サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変

更することができます。NTP 接続に関する問題が発生した場合は、NTP のトラブルシューティングを参照してください。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックしてから、[システム設定（System Settings）] > [NTP] リンクをクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [NTP]をクリックします。

ステップ 2 [NTPタイム サーバ（NTP Time Server）]で、独自のサーバを（手動で）使用するか、シスコのタイム サーバを使用するかどうかを選択します。

- [Cisco NTP タイム サーバ（Cisco NTP Time Server）][デフォルト NTP タイム サーバ（Default NTP Time Server）]：このオプションを選択すると、NTP で使用されるサーバ名がサーバ一覧に表示されます。
- [手動入力（Manually Input）]：このオプションを選択する場合、使用する NTP の完全修飾ドメイン名または IP アドレスを入力します。たとえば、ntp1.example.com または 10.100.10.10 と入力します。複数の NTP サーバが存在する場合、[別の NTP タイム サーバを追加する（Add Another NTP Time Server）]をクリックして、アドレスを入力します。

ステップ 3 [保存（Save）]をクリックします。

Cisco 集合型セキュリティ インテリジェンス （CSI）の クラウド の基本設定の設定

システムは、レピュテーション、リスク、脅威インテリジェンスに関して Cisco 集合型セキュリティ インテリジェンス（CSI）を使用します。

URL フィルタリングと FirePOWER の AMP（マルウェア ファイル ポリシーに使用）に必要なライセンスを保有している場合、システムは、これらの機能を自動的に有効にし、Cisco CSI から必要な情報を取得するための通信を有効にします。とはいえ、通信を制御するためのオプションの一部はユーザが設定できます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [クラウドの基本設定（Cloud Preferences）] の順にクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [クラウドの基本設定（Cloud Preferences）]と [URL フィルタリングの基本設定（Filtering Preferences）]をクリックします。

ステップ 2 次のオプションを設定します。

- [自動更新の有効化（Enable Automatic Updates）]：カテゴリとレピュテーションを含む更新された URL データをチェックしてダウンロードすることをシステムに許可します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。デフォルトでは、更新が有効になっています。このオプションを選択解除した状態でカテゴリとレピュテーションのフィルタリングを使用している場合、このオプションを周期的に有効にして新しい URL データを取得してください。
- [不明な URL に対する Cisco CSI のクエリ （Query Cisco CSI for Unknown URLs）]：ローカル URL フィルタリング データベースのカテゴリおよびレピュテーションのデータを含まない URL の更新情報を Cisco CSI でチェックするかどうかを切り替えます。ルックアップが適度な制限時間内に更新情報を返した場合、その情報は、URL の状況に基づいてアクセス ルールを選択する際に使用されます。それ以外の場合、URL は分類されていないカテゴリと照合されます。

ステップ 3 [保存（Save）]をクリックします。