基本設定

この章では、ASA 上でコンフィギュレーションを機能させるために通常必要な基本設定を行う方法について説明します。

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブルパスワード、Telnetパスワードを設定するには、次の手順を実行します。

始める前に

ホスト名、ドメイン名、イネーブルパスワード、Telnetパスワードを設定する前に、次の要件を確認します。

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブル パスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。

- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[設定（Configuration）] > [デバイスリスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[設定（Configuration）] > [デバイス設定（Device Setup）] > [デバイス名/パスワード（Device Name/Password）]** を選択します。

ステップ 2 ホスト名を入力します。デフォルトのホスト名は「ciscoasa」です。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名は syslog メッセージでも使用されます。

マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドラインプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

ステップ 3 ドメイン名を入力します。デフォルト ドメイン名は default.domain.invalid です。

ASA は、修飾子を持たない名前のサフィックスとして、ドメイン名を追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバーとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 4 特権モード（イネーブル）パスワードを変更します。デフォルトのパスワードは空白ですが、CLI で **enable** コマンドを最初に入力したときに変更するように求められます。

enable 認証を設定しない場合、イネーブルパスワードによって特権 EXEC モードが開始されます。HTTP 認証を設定しない場合、イネーブル パスワードによって空のユーザー名で ASDM にログインできます。 ASDM では、CLI アクセスのように、イネーブル パスワードの変更は適用されません。

a) [特権モードパスワードを変更（Change the privileged mode password）] チェックボックスをオンにします。
b) 新しいパスワードを入力し、新しいパスワードを確認します。8 ～ 127 文字のパスワードを設定します。大文字と小文字が区別されます。以下を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。
   - スペースは使用できません。
   - 疑問符は使用できません。
   - 3 文字以上連続した、順番に並んだ ASCII 文字または繰り返される ASCII 文字は使用できません。たとえば、次のパスワードは拒否されます。
     - **abc**user1
     - user**543**
     - user**aaaa**

- user2**666**

パスワードを空白の値にリセットすることはできません。

ステップ 5 Telnetアクセスのためのログイン パスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログイン パスワードは Telnet アクセスに使用されます。

a) [セキュリティアプライアンスのコンソールにアクセスするためのパスワードを変更する（Change the password to access the console of the security appliance）] チェックボックスをオンにします。

b) 古いパスワード（新しい ASA の場合はこのフィールドを空白にしておきます）、新しいパスワードを入力し、新しいパスワードを確認します。パスワードには最大 16 文字の長さを使用できます。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

ステップ 6 [Apply] をクリックして変更内容を保存します。

日時の設定

（注） Firepower 4100/9300 の日時を設定しないでください。ASA はシャーシから日時の設定を受信します。

NTP サーバを使用した日付と時刻の設定

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は一番下の階層からサーバを選択し、データ信頼度の尺度にします。

手動で設定した時刻はすべて、NTP サーバーから取得された時刻によって上書きされます。

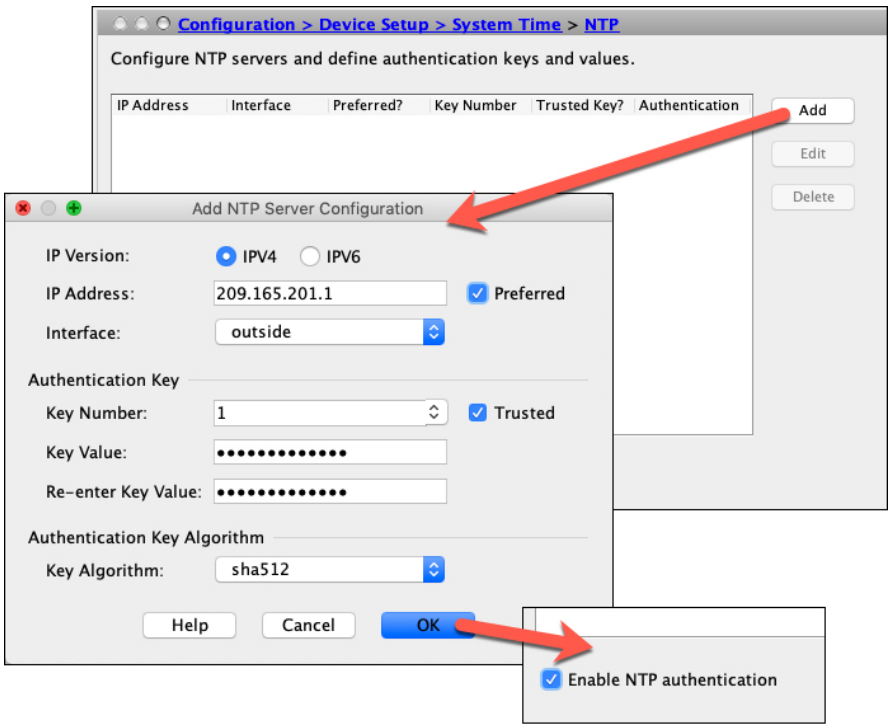
ASA は NTPv4 をサポートします。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** を選択します。



ステップ 2 [Add] をクリックして、[Add NTP Server Configuration] ダイアログボックスを表示します。

ステップ 3 NTP サーバーの **IPv4** または **IPv6 IP アドレス**を入力します。

サーバーのホスト名を入力することはできません。ASA は、NTP サーバーの DNS ルックアップをサポートしていません。

ステップ 4 （任意） [Preferred] チェックボックスをオンにして、このサーバーを優先サーバーに設定します。

NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバーよりも精度が大幅に高いサーバーがある場合、ASA は精度の高いそのサーバーを使用します。

ステップ 5 （任意） ドロップダウンリストから [Interface] を選択します。

この設定では、NTP パケットの発信インターフェイスが指定されます。インターフェイスが空白の場合、ASA が使用するデフォルトの管理コンテキストインターフェイスは、管理ルーティングテーブルによって決まります。

ステップ 6 （任意） NTP 認証を設定します。

a) 1 ～ 4294967295 の間の**キー番号**を入力するか、または、再利用する別の NTP サーバーのキーを以前に作成した場合は、ドロップダウンリストから既存のキー番号を選択します。

この設定では、この認証キーのキー ID を指定します。これにより、認証を使用して NTP サーバーと通信できます。NTP サーバーのパケットも、常にこのキー ID を使用する必要があります。

b) [Trusted] チェックボックスをオンにします。
c) [Key Value] を入力します。これは、最大 32 文字の文字列です。その後、キー値を再入力します。
d) ドロップダウンリストから [Key Algorithm] を選択します。
e) [OK] をクリックします。

ステップ 7 [Enable NTP authentication] チェックボックスをオンにして、NTP 認証を有効にします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

手動での日時の設定

日付と時刻を手動で設定するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[System Time]** > **[Clock]** を選択します。

ステップ 2 ドロップダウン リストからタイム ゾーンを選択します。この設定では、適切な時差を GMT に加えた（または GMT から差し引いた）タイム ゾーンを指定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、3 月の第 2 日曜日の午前 2 時から 11 月の第 1 日曜日の午前 2 時間での時間が自動的に夏時間に調整されます。

（注）
ASA の時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

ステップ 3 [Date] ドロップダウン リストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付を検索します。

- 月の名前をクリックし、月のリストを表示し、次に目的の月をクリックします。カレンダーがその月に変わります。
- 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
- 年月の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。

- カレンダーの日にちをクリックして日を設定します。

ステップ 4 時刻（時間、分、および秒）を手動で入力します。

ステップ 5 [Update Display Time] をクリックして、ASDM ペインの右下に表示される時刻を更新します。現在時刻は 10 秒ごとに自動更新されます。

Precision Time Protocol の設定（ISA 3000）

高精度時間プロトコル（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。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定およびコントロールシステム向けに設計されており、必要な帯域幅は最小限で、処理オーバーヘッドが少ないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせで構成される分散ネットワークシステムです。PTP デバイスには、オーディナリクロック、境界クロック、およびトランスペアレントクロックが含まれます。非 PTP デバイスには、ネットワークスイッチ、ルータ、およびその他のインフラストラクチャ デバイスが含まれます。

ASA デバイスは、トランスペアレントクロックとして設定できます。ASA デバイスは、自身のクロックを PTP クロックと同期しません。ASA デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTP デバイスを設定する場合は、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定し、特定の 1 つのドメインに PTP クロックを使用するように PTP 以外の各デバイスを設定できます。

始める前に

- この機能は、ISA 3000 のみで使用できます。
- PTP の使用は、シングルコンテキストモードでのみサポートされます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- デフォルトでは、トランスペアレントモードのすべての ISA 3000 インターフェイスで PTP がイネーブルになっています。ルーテッドモードでは、PTP パケットがデバイスを通過できるようにするために必要な設定を追加する必要があります。
- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。
- PTP 設定は、スタンドアロンかブリッジグループメンバーかを問わず、物理イーサネットインターフェイスでサポートされます。次のものではサポートされません。
  - 管理インターフェイス。
  - サブインターフェイス、EtherChannel、BVI、その他の仮想インターフェイス。

- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。
- PTP パケットが確実にデバイスを通過できるようにする必要があります。トランスペアレントファイアウォールモードでは、PTP トラフィックを許可するアクセスリストがデフォルトで設定されています。PTP トラフィックは UDP ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのためルーテッド ファイアウォール モードでは、このトラフィックを許可するすべての ACL が受け入れられます。
- さらにルーテッド ファイアウォール モードでは、PTP マルチキャストグループ用のマルチキャストルーティングを次のようにイネーブルにする必要もあります。
  - グローバル コンフィギュレーション モードのコマンド **multicast-routing** を入力します。
  - また、ブリッジグループメンバーではなく、PTP が有効になっているインターフェイスごとに、インターフェイス コンフィギュレーション コマンド **igmp join-group 224.0.1.129** を入力して、PTP マルチキャスト グループ メンバーシップを静的に有効にします。このコマンドは、ブリッジグループメンバーに対してはサポートされておらず、必要もありません。

手順

ステップ 1 **[Configuration]** > **[Device Management** > **PTP]** を選択します。

ステップ 2 **Domain value** を入力します。

これは、デバイスのすべてのポートのドメイン番号です。異なるドメインで受信されたパケットは、通常のマルチキャストパケットのように扱われるため、PTP 処理は行われません。この値の範囲は 0 ～ 255、デフォルト値は 0 です。ネットワーク内の PTP デバイスに設定されているドメイン番号を入力します。

ステップ 3 （オプション）**Enable End-to-End Transparent Clock Mode** を選択し、PTP がイネーブルになっているすべてのインターフェイスでエンドツーエンド トランスペアレント モードをイネーブルにします。

トランスペアレント クロックは、滞留時間を測定し、PTP パケット内の `correctionField` を更新することによって遅延を修正するクロックです。

ステップ 4 インターフェイスを選択し、[Enable] または [Disable] をクリックして、1 つ以上のデバイスインターフェイスで PTP を有効にします。

システムが設定ドメイン内の PTP クロックに接続できる各インターフェイスで、PTP を有効にします。

ステップ 5 [Apply] をクリックします。

次のタスク

[Monitoring] > **[Properties]** > **[PTP]** を選択し、PTP クロックとインターフェイス/ポート情報を表示します。

マスター パスフレーズの設定

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスターパスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- Logging
- 共有ライセンス

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

始める前に

- この手順を実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。
- フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

  [Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Shared Key] フィールドに任意の文字を入力するか、またはフェールオーバー 16 進キーを選択している場合はバックスペースを除く 32 の 16 進数（0-9A-Fa-f）を入力します。次に、[Apply] をクリックします。
- アクティブ/スタンバイ フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行されます。これは、アクティブな構成をスタンバイ ユニットに複製します。この複製が行われない場合、スタンバイ ユニットの暗号化されたパスワード

は、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、アクティブ/アクティブ モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリ ユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリ ユニットにグループ 2 コンテキストを復元する必要があります。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告メッセージが表示されます。[OK] または [Cancel] をクリックして続行できます。

後からパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードはいずれも変更されず、マスターパスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにして、新しいマスター パスフレーズを入力および確認できるようにします。デフォルトでは、これらはディセーブルです。

新しいマスター パスフレーズの長さは 8 ～ 128 文字にする必要があります。

既存のパスフレーズを変更する場合は、新しいパスフレーズを入力する前に、古いパスフレーズを入力する必要があります。

マスター パスフレーズを削除するには [New] および [Confirm master passphrase] フィールドを空白のままにします。

ステップ 4 [Apply] をクリックします。

マスター パスフレーズの無効化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキストパスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

始める前に

- ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

  マスター パスフレーズをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスターパスフレーズがない場合は、[Apply] をクリックすると警告文が表示されます。[OK] または [Cancel] をクリックして続行します。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにします。

ステップ 4 [Old master passphrase] フィールドに、古いマスターパスフレーズを入力します。ディセーブルにする古いマスター パスフレーズを指定する必要があります。

ステップ 5 [Newmaster master passphrase] フィールドと [Confirm master passphrase] フィールドを空白のままにします。

ステップ 6 [適用（Apply）] をクリックします。

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセスルールに完全修飾ドメイン名（FQDN）ネットワークオブジェクトを使用するように、DNS サーバーを設定する必要があります。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバーと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

デフォルトでは、DefaultDNS と呼ばれるデフォルトの DNS サーバーグループがあります。複数の DNS サーバーグループを作成できます。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。PN トンネル グループ用に他の DNS サーバー グループを設定できます。詳細については、コマンドリファレンスの **tunnel-group** コマンドを参照してください。

（注） ASA では、機能に応じて DNS サーバーの使用が限定的にサポートされます。

始める前に

DNS ドメインルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセス ルールを設定し、DNS サーバーに到達できるようにしてください。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** の順に選択します。

ステップ 2 [DNS Setup] 領域で、次のいずれかのオプションを選択します。

- Configure one DNS server group：このオプションは DefaultDNS グループにサーバーを定義します。
- [複数のDNSサーバーグループを設定（Configure multiple DNS server groups）]：このオプションを使用すると、DefaultDNS グループだけでなく、特定のドメインに関連付けることが可能なその他のグループやリモートアクセス SSL VPN グループポリシーに使用するグループを設定できます。DefaultDNS グループのみを設定したとしても、グループで使用するタイムアウトやその他の特性を変更する場合は、このオプションを選択する必要があります。

ステップ 3 [1 つの DNS サーバ グループを設定（Configure one DNS server group）] を選択した場合は、DefaultDNS グループ内にサーバを設定します。

a) [Primary DNS Server] に、可能な限り使用する必要がある DNS サーバーの IP アドレスを入力します。必要に応じて、このサーバーと各セカンダリ サーバーに対し、ASA がサーバーとの接続に使用する *interface_name* を指定します。インターフェイスを指定しなかった場

合、ASA はデータ ルーティング テーブルを確認し、一致するものが見つからなければ、管理専用ルーティング テーブルを確認します。

b) [Add] をクリックして、セカンダリ DNS サーバーを追加します。

最大 6 個の DNS サーバを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバーを優先度の順に並べます。

c) 完全修飾されていない場合、ホスト名に追加する DNS ドメイン名を入力します。

ステップ 4 [Configure multiple DNS server groups] を選択した場合は、サーバー グループのプロパティを定義します。

a) [追加（Add）] をクリックして新しいグループを作成するか、グループを選択して [編集（Edit）] をクリックします。

DefaultDNS グループは常にリストに表示されます。

b) グループのプロパティを設定します。

- [Server IP Address to Add]、[Source Interface]：DNS サーバーの IP アドレスを入力し、[Add>>] をクリックします。各サーバーについて、必要に応じて ASA がサーバーとの通信に使用する *interface_name* を指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

  最大 6 個の DNS サーバを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[上へ移動（Move Up）]/[下へ移動（Move Down）] ボタンを使用して、サーバを優先度の順に並べます。

- [Timeout]：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルトは 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウトは 2 倍に増えます。

- [再試行（retries）]：ASA が応答を受信しない場合に DNS サーバのリストを再試行する回数。0 ～ 10 の範囲で指定します。

- Expire Entry Timer（DefaultDNS またはアクティブグループのみ）：DNS エントリの最小 TTL（分単位）。有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。有効期限が切れると、DNS ルックアップテーブルからエントリが削除されます。エントリの削除にはテーブルをコンパイルする必要があります。したがって、削除を頻繁に行うとデバイス上の処理負荷が増加する可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、すべての解像度の最小 TTL は 1 分です）。指定できる範囲は 1 ～ 65535 分です。FQDN ネットワーク オブジェクトを解決する場合にのみ、このオプションを使用します。

- [ポール タイマー（Poll Timer）]（DefaultDNS またはアクティブなグループのみ）：FQDN ネットワーク/ホスト オブジェクトを IP アドレスに解決するために使用するポー

リングサイクルの分単位の時間。FQDN オブジェクトは、ファイアウォール ポリシーで使用されている場合にのみ解決されます。タイマーによって、解決間隔の最大時間が決定されます。また、DNS エントリの存続可能時間（TTL）の値を使用しても、IP アドレス解決に更新するタイミングを決定できます。したがって、個々の FQDN がポーリング サイクルよりも頻繁に解決される可能性があります。デフォルトは 240（4 時間）です。指定できる範囲は 1 ～ 65535 分です。

- **[ドメイン名（Domain Name）]**（DefaultDNS またはアクティブ グループのみ）：完全修飾されていない場合のホスト名に追加するドメイン名。

c) [OK] をクリックします。

d) 複数のグループがある場合は、グループを 1 つ選択して [アクティブに設定（Set Active）] をクリックすることでデフォルトグループを変更できます。

グループにドメインがマッピングされていない場合にのみ、グループをデフォルトとして使用できます（「ステップ 8 （14 ページ）」を参照）。

ステップ 5 DNS ルックアップが少なくとも 1 つのインターフェイスで有効になっていることを確認します。DNS サーバー グループの表の下にある [DNS lookup] インターフェイス リストで、[DNS Enabled] カラムをクリックして [True] を選択し、インターフェイスでのルックアップを有効化します。

DNS サーバーへのアクセスに使用されるすべてのインターフェイスで DNS ルックアップを有効にしてください。

インターフェイスで DNS ルックアップを有効にしないと、DNS サーバーの [Source Interface] またはルーティング テーブルを使用して検出したインターフェイスを使用できません。

ステップ 6 （任意）[信頼されたDNSサーバ（Trusted DNS Server）] で、ネットワーク サービス オブジェクトのドメイン名を解決するときに信頼するサーバを決定するオプションを設定します。

a) （任意） 明示的に設定された信頼された DNS サーバを追加または削除します。

- [追加（Add）] をクリックして新しいサーバを追加し、IP タイプ（IPv4 または IPv6）を選択し、サーバの IP アドレスを入力して、[OK] をクリックします。
- アドレスを変更するには、サーバを選択し、[編集（Edit）] をクリックします。
- サーバを選択し、[削除（Delete）] をクリックして信頼されたサーバのリストからそのサーバを削除します。

b) 次のオプションを選択または選択解除します。

- [任意（Any）]：すべての DNS サーバを信頼し、すべてをスヌーピングします。このオプションはデフォルトでは無効になっています。
- [構成されたサーバ（Configured-Servers）]：DNS サーバグループで設定されたサーバを信頼するかどうか。このオプションは、デフォルトで有効です。

- [DHCPクライアント（DHCP-Client）]：DHCP クライアントと DHCP サーバ間のスヌーピングメッセージによって学習されたサーバが、信頼された DNS サーバと見なされるかどうか。このオプションは、デフォルトで有効です。
- [DHCPプール（DHCP-Pools）]：デバイスインターフェイスで実行されている DHCP サーバを介してアドレスを取得するクライアントの DHCP プールに設定されている DNS サーバを信頼するかどうか。このオプションは、デフォルトで有効です。
- [DHCPリレー（DHCP-Relay）]：DHCP クライアントと DHCP サーバ間のスヌーピング リレー メッセージによって学習されたサーバが、信頼された DNS サーバと見なされるかどうか。このオプションは、デフォルトで有効です。

ステップ 7 （任意） クエリーごとに 1 つの DNS 応答を強制するには、[Enable DNS Guard on all interfaces] チェックボックスをオンにします。

DNS インスペクションを設定するときに、DNS ガードも設定できます。特定のインターフェイスでは、DNS インスペクションで設定されている DNS ガードの設定がこのグローバル設定より優先されます。デフォルトでは、DNSインスペクションはDNSガードがイネーブルになっているすべてのインターフェイスでイネーブルになっています。

ステップ 8 （任意） ドメインを特定の DNS サーバーグループにマッピングします。

最大 30 のドメインをマッピングできます。同じドメインを複数の DNS サーバーグループにマッピングすることはできませんが、複数のドメインを同じサーバーグループにマッピングすることは可能です。（DefaultDNS などの）デフォルトに使用するグループにドメインをマッピングしないでください。

a) [DNSグループマップ（DNS Group Map）] 領域で、[DNSグループマップを有効にする（Enable DNS Group Map）] をオンにします。
b) [追加（Add）] をクリックします。

   [DNSサーバーグループへのドメインの追加（Add Domains to DNS Server Group）] ダイアログボックスが表示されます。

c) [DNSサーバーグループからドメイン名へのマッピング（DNS server group to domain name mapping）] ドロップダウンリストで、DNS サーバーグループ名を選択します。
d) [ドメイン名（Domain Name）] フィールドに、DNS グループにマッピングするドメイン名を入力します。
e) [OK] をクリックします。
f) さらにマッピングを追加するには、これらの手順を繰り返します。

ステップ 9 [Apply] をクリックして変更内容を保存します。

ハードウェア バイパスおよびデュアル電源（Cisco ISA 3000）の設定

ハードウェア バイパスを有効化して、停電時にもインターフェイス ペア間のトラフィックのフローを継続することができます。サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。次のハードウェア バイパスのガイドラインを参照してください。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。
- ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのはサポートされているインターフェイス ペアだけになります。つまり、デフォルトの設定を使用している場合、inside1 と inside2 間および outside1 と outside2 間は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。
- シスコでは、TCP シーケンスのランダム化を無効にすることを推奨しています（下記の手順を参照）。ランダム化が有効化されている場合（デフォルト）、ハードウェア バイパスを有効化するときに TCP セッションを再確立する必要があります。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスが有効化されると、ISA 3000 はデータ パスに存在しなくなり、シーケンス番号を変換しません。受信するクライアントは予期しないシーケンス番号を受信し、接続をドロップします。TCP シーケンスのランダム化が無効になっていても、スイッチオーバーの際に一時的にダウンしたリンクのために、一部の TCP 接続は再確立される必要があります。
- ハードウェアのバイパス インターフェイスでの Cisco TrustSec の接続は、ハードウェアのバイパスが有効化されているときにはドロップされます。ISA 3000 の電源がオンになり、ハードウェアのバイパスが非アクティブ化されている場合、接続は再ネゴシエートされます。
- ハードウェア バイパスを非アクティブ化し、トラフィックが ISA 3000 のデータ パスを経由することを再開した場合、スイッチオーバー時に一時的にダウンしたリンクがあるために、既存の TCP セッションの一部を再確立する必要があります。
- ハードウェア バイパスをアクティブにすると、イーサネット PHY が切断され、ASA はインターフェイスのステータスを判断できなくなります。インターフェイスはダウン状態であるかのように表示されます。

ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電

源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。

始める前に

- ハードウェア バイパス インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

手順

ステップ 1 ハードウェア バイパスを設定するには、**[Configuration]** > **[Device Management]** > **[Hardware Bypass]** の順に選択します。

ステップ 2 [Enable Bypass during Power Down] チェックボックスをオンにして、各インターフェイス ペアのハードウェア バイパスを有効化するように設定します。

ステップ 3 （任意） **[Stay in Bypass after Power Up]** チェック ボックスをオンにして、電源が回復してアプライアンスが起動した後にハードウェア バイパス モードの状態に維持されるように、各インターフェイス ペアを設定します。

ハードウェア バイパスを非アクティブ化すると、ASA がフローを引き継ぐため、接続が短時間中断されます。この場合、準備が整った時点でハードウェアバイパスを手動でオフにする必要があります。このオプションを使用すると、短時間の割り込みがいつ発生するかを制御できます。

ステップ 4 インターフェイス ペアに対しては、[Bypass Immediately] チェックボックスをオン/オフして、手動でハードウェア バイパスを有効化または非アクティブ化します。

ステップ 5 （任意） **[Stay in Bypass Mode until after the ASA Firepower Module Boots Up]** チェック ボックスをオンにして、ASA Firepower モジュールの起動後までハードウェア バイパスがアクティブであり続けるように設定します。

ブート遅延が動作するには、[Stay in Bypass after Power Up] オプションを使用せずにハードウェア バイパスを有効化する必要があります。このオプションを使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェアバイパスが非アクティブになる可能性があります。たとえば、モジュールをフェールクローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

ステップ 6 [Apply] をクリックします。

ステップ 7 TCP のランダム化を無効化します。この例では、デフォルト設定に設定を追加することによって、すべてのトラフィックのランダム化を無効化する方法を示します。

a) **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。
b) **sfrclass** ルールを選択して [Edit] をクリックします。
c) [Rule Actions] に続いて、[Connection Settings] をクリックします。
d) [Randomize Sequence Number] チェック ボックスをオフにします。
e) [OK]、続いて [Apply] をクリックします。

ステップ 8 予期する構成としてデュアル電源を設定するには、**[Configuration]** > **[Device Management]** > **[Power Supply]** の順に選択し、[Enable Redundant Power Supply] チェック ボックスをオンにして、[Apply] をクリックします。

この画面は利用可能な電源も表示します。

ステップ 9 [保存（Save）] をクリックします。

システムがオンラインになった後のハードウェアバイパスの動作は、スタートアップ コンフィギュレーションの設定によって決定されるため、実行コンフィギュレーションを保存する必要があります。

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

ルール エンジンのトランザクション コミット モデルの選択

デフォルトでは、ルールベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかります。パフォーマンス コストは、1秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルール エンジンがトランザクション モデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクション モデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します（接続数/秒のレートは減少します）。	新しいルールに一致します。

モデル	コンパイル前	コンパイル中	コンパイル後
トランザクション	古いルールに一致します。	古いルールに一致します （接続数/秒のレートは影響を受けません）。	新しいルールに一致します。

トランザクション モデルのその他のメリットには、インターフェイス上の ACL を交換するときに、古い ACL を削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。

始める前に

- 解決が頻繁に変わる可能性があるホスト名にFQDNオブジェクトを使用する場合、トランザクション コミットはアクセス制御ルールでは推奨されません。これは、DNS のチャーンが原因でアクセス グループのコンパイルが完全に解決されない可能性があるためです。引き続きトランザクションコミットを使用する場合は、DNSの有効期限の延長を検討してください。
- ルール タイプのトランザクション モデルをイネーブルにする場合、コンパイルの先頭と末尾をマークする Syslog が生成されます。これらの Syslog には 780001 ～ 780004 までの番号が付けられます。

手順

[Configuration] > [Device Management] > [Advanced] > [Rule Engine] の順に選択し、目的のオプションを選択します。

- **Access group**：グローバルにまたはインターフェイスに適用されるアクセス ルール。
- **NAT**：ネットワーク アドレス変換ルール。

ASP ロード バランシングの有効化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

ASP ロードバランシングにより、1 つのインターフェイス受信リングから受信したパケットを複数のコアが同時に処理できます。システムがパケットをドロップし、**show cpu** コマンドの出

力が 100% を大きく下回る場合、互いに関連のない多数の接続にパケットが属しているのであれば、この機能によってスループットが向上することがあります。

（注） ASP ロードバランシングは、ASA 仮想 で無効になっています。ASA 仮想 の高速セキュリティパス（ASP）に対する DPDK（データプレーン開発キット）の統合により、ASA 仮想 でこの機能を無効にしたときのパフォーマンスが向上します。

手順

ステップ 1 ASP ロード バランシングの自動切り替えをイネーブルまたはディセーブルにするには、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[ASP Load Balancing]** の順に選択して、[Dynamically enable or disable ASP load balancing based on traffic monitoring] チェックボックスをオンにします。

ステップ 2 手動で ASP ロード バランシングをイネーブルまたはディセーブルにするには、[Enable ASP load balancing] チェックボックスをオンまたはオフにします。

手動で ASP ロード バランシングをイネーブルにすると、動的オプションをイネーブルにした場合でも、手動でディセーブルにするまではイネーブル状態となります。手動で ASP ロード バランシングをイネーブルにした場合にのみ、ASP ロード バランシングの手動ディセーブル化が適用されます。動的オプションもまたイネーブルにすると、システムは ASP ロード バランシングの自動イネーブル/ディセーブル化に戻ります。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバーに DNS クエリーが送信されます。外部 DNS サーバーによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

DNS キャッシュのモニタリングについては、次のコマンドを参照してください。

- **show dns-hosts**

  DNS キャッシュを表示します。これには、DNS サーバーからダイナミックに学習したエントリと name コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

基本設定の履歴

機能名	プラットフォーム リリース	説明
複数の DNS サーバーグループ	9.18(1)	複数の DNS サーバーグループを使用できるようになりました。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [DNS] > [DNSクライアント（DNS Client）]**
ネットワーク サービス オブジェクト ドメイン解決用の信頼された DNS サーバ。	9.17(1)	ネットワーク サービス オブジェクトのドメイン名を解決するときに、システムが信頼する DNS サーバを指定できます。この機能により、すべての DNS ドメイン名解決が、信頼された送信元から IP アドレスを取得するようになります。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [DNS] > [DNSクライアント（DNS Client）]**
DNS エントリの TTL 動作の変更	9.17(1)	以前は、設定値は各エントリの既存の TTL に追加されていました（デフォルトは 1 分でした）。現在は、有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [DNS] > [DNSクライアント（DNS Client）] > [複数の DNS サーバーグループを構成します（Configure multiple DNS server groups）]**

機能名	プラットフォームリリース	説明
より強力なローカルユーザーと有効なパスワード要件	9.17(1)	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。 • パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。 • 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。 • **abc**user1 • user**543** • user**aaaa** • user2**666** 新規/変更された画面： • **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** • **[Configuration]** > **[Device Setup]** > **[Device Name/Password]**
NTPv4 のサポート	9.14(1)	ASA が NTPv4 をサポートするようになりました。 変更された画面はありません。
追加の NTP 認証アルゴリズム	9.13(1)	以前は、NTP 認証では MD5 だけがサポートされていました。ASA は、次のアルゴリズムをサポートするようになりました。 • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新しい/変更された画面： **[構成（Configuration）]** > **[デバイス設定（Device Setup）]** > **[システム時間（System Time）]** > **[NTP]** > **[追加（Add）]**ボタン > [NTPサーバ構成の追加（Add NTP Server Configuration）] ダイアログボックス > [キーアルゴリズム（Key Algorithm）] ドロップダウンリスト

機能名	プラットフォーム リリース	説明
IPv6 での NTP サポート	9.12(1)	NTP サーバーに IPv6 アドレスを指定できるようになりました。 新しい/変更された画面： **[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** > **[Add]** ボタン > [Add NTP Server Configuration] ダイアログボックス
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 ～ 127 文字の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブルパスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 変更された画面はありません。
ASP ロードバランシングは、ASA 仮想 で無効になっています。	9.10(1)	ASA 仮想の高速セキュリティパス（ASP）に対する最近の DPDK（データプレーン開発キット）の統合により、ASA 仮想 でこの機能を無効にしたときのパフォーマンスが向上します。
自動 ASP ロードバランシングが ASA 仮想 でサポートされるようになりました。	9.8(1)	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。

機能名	プラットフォームリリース	説明
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、SHA-512 を使用する PBKDF2（パスワードベースキー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**
ISA 3000 のデュアル電源サポート	9.6(1)	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 次の画面が導入されました。**[Configuration] > [Device Management] > [Power Supply]**
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**
ISA 3000 ハードウェア バイパス	9.4(1.225)	ISA 3000 は、トラフィックが電源喪失時にアプライアンスを通過し続けるようにするハードウェア バイパス機能をサポートします。 次の画面が導入されました。**[Configuration] > [Device Management] > [Hardware Bypass]** この機能は、バージョン *9.5(1)* では使用できません。

機能名	プラットフォーム リリース	説明
自動 ASP ロード バランシング	9.3(2)	ASP ロードバランシング機能の自動切替を有効または無効に設定できるようになりました。 （注） 自動機能は ASA 仮想 ではサポートされません。手動による有効化または無効化のみがサポートされます。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。 （注） ログイン パスワードが使用されるのは、Telnetユーザー認証を設定しない場合の Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。
マスターパスフレーズ	8.3(1)	この機能が導入されました。マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。 次の画面が導入されました。 **[Configuration] > [Device Management] > [Advanced] > [Master Passphrase]。** **[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase]。**

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。