Basic Settings

この章では、ASA 上で機能を果たすコンフィギュレーションに通常必要とされる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。マルチ コンテキスト モードのスイッチから ASASM へのセッションを実行する場合、ASASM は管理コンテキストで設定したログイン パスワードを使用します。

- 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、[Configuration] > [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 **[Configuration]** > **[Device Setup]** > **[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ブランクです。

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名で ASDM にログインできます。

a) [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。最大 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。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 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。**session** コマンドを使用してスイッチから ASASM にアクセスする場合にも、このパスワードを使用します。

a) [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） ASASM または FirePOWER 9300 ASA セキュリティ モジュールの日時は設定しないでください。これらは、ホスト デバイスから日時設定を受け取ります。

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、データ信頼度の尺度となる一番下のストラタムのサーバを選択します。

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

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 サーバの IP アドレスを入力します。

ステップ 4 [Preferred] チェックボックスをオンにして、このサーバを優先サーバに設定します。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、優先サーバよりも精度が大幅に高いサーバがある場合、ASA は精度の高いそのサーバを使用します。

ステップ 5 ドロップダウン リストからインターフェイスを選択します。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、ルーティング テーブルによって決まります。管理コンテキスト（および使用可能なインターフェイス）を変更する際の安定性のために [None]（デフォルトのインターフェイス）を選択します。

ステップ 6 ドロップダウン リストから、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、MD5 認証を使用して NTP サーバと通信できます。NTP サーバのパケットも、常にこのキー ID を使用する必要があります。以前に別のサーバに対してキー ID

を設定した場合は、そのキーIDをリストから選択できます。それ以外の場合は、1～4294967295の数字を入力します。

ステップ 7 [Trusted] チェックボックスをオンにして、この認証キーを信頼できるキーとして指定します。これは、認証を成功させるために必要です。

ステップ 8 認証キーを設定するめのキー値を入力します。この値は、最大 32 文字の文字列です。

ステップ 9 このキー値を再入力して、正しく 2 回入力したことを確認します。

ステップ 10 [OK] をクリックします。

ステップ 11 [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 12 [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。

PTP（ISA 3000）を使用した日付と時刻の同期

Precision Time Protocol（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させるために開発された時刻同期プロトコルです。 通常、これらのデバイス クロックの精度と安定性はさまざまに異なります。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制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、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による、分散型のネットワーク 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 スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

（注） PTP トラフィックが検査のために ASA FirePOWER モジュールに送信されないようにするために、ASA のデフォルト設定に以下のコマンドが追加されています。既存の導入がある場合は、次のコマンドを手動で追加する必要があります。

```
object-group service bypass_sfr_inspect
service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
```

始める前に

- この機能は、Cisco ISA 3000 アプライアンス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 の設定は、すべての物理イーサネット 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、チャネル グループ、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、PTP がイネーブル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イネーブルにします。

PTP 時刻同期をイネーブルにするには、次の手順に従ってください。

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 処理が行われません。この値の範囲は 0 ～ 255、デフォルト値は 0 です。

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 1 つ以上のデバイス インターフェイスで PTP をイネーブルにします。

a) インターフェイスを選択して、**Enable** または **Disable** をクリックします。

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 [Apply] をクリックします。

DNS サーバの設定

DNS サーバを設定して、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。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。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。

（注） ASA では、機能に応じて DNS サーバ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 グループにサーバを定義します。
- Configure multiple DNS server groups：このオプションでも、DefaultDNS グループは設定する必要があります。FQDN ネットワーク オブジェクトの名前解決に使用されるのは DefaultDNS グループのみです。DefaultDNS はアクティブ グループのままにします。ただし、リモート アクセス SSL VPN グループ ポリシーで使用する追加のグループを作成することもできます。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 [Configure one DNS server group] を選択した場合は、DefaultDNS グループ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 サーバの IP アドレスを入力します。必要に応じて、このサーバと各セカンダリ サーバに対し、ASA がサーバ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、サーバを優先度の順に並べます。

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

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

a) [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 [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 プロパティを設定します。

- [Server IP Address to Add]、[Source Interface]：DNS サーバの IP アドレスを入力し、[Add>>] をクリックします。各サーバについて、必要に応じて ASA がサーバ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。[Move Up]/[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）。デフォルト値は 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倍増します。

- [Retries]：ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数（0 ～ 10）。

- [Expire Entry Timer]（DefaultDNS またはアクティブ グループのみ）：DNS エントリの期限が切れた（TTL が経過した）後、そのエントリが DNS ルックアップ テーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくな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、TTL が経過してから 1 分後にエントリが削除されます）。指定できる範囲は 1 ～ 65535 分です。このオプションは、FQDN ネットワーク オブジェクトの解決時にのみ使用されます。

- [Poll Timer]（DefaultDNS またはアクティブ 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されるポーリング サイクルの時間（分単位）。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まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間（TTL）値も使用されるため、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場合があります。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。

- [Domain Name]：ホスト名に追加するドメイン名（完全修飾されていない場合）。

c) [OK] をクリックします。
d) 複数のグループがある場合は、DNS 要求に使用するグループを選択して [Set Active] をクリックすれば変更できます。

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イネーブルになっていることを確認します。DNS サーバ 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。

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）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 7 [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 で単一電源が想定されており、装備してい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。

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。

ルール エンジンはさらに迅速なルール ルックアップを実現するためにルールをコンパイルするため、パフォーマンスに影響します。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。
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。

ヒント 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。

ルール エンジンのトランザクション コミット モデルを有効にするには、次の手順を使用します。

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、ASAv で無効になっています。DPDK（データプレーン開発キット）を ASAv の高速セキュリティ パス（ASP）に統合すると、ASAv 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 サーバに DNS クエリーが送信されます。外部 DNS サーバ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
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]**。
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。

機能名	プラットフォーム リリース	説明
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。
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 ASAv 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]。

機能名	プラットフォーム リリース	説明
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。
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]**

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、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]**
自動 ASP ロードバランシングが ASAv 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]。
ASP ロードバランシングは、ASAv で無効になっています。	9.10(1)	DPDK（データプレーン開発キット）の ASAv の高速セキュリティ パス（ASP）への最近の統合により、ASAv 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。