マルチ コンテキスト モード

この章では、ASA でマルチ セキュリティ コンテキストを設定する方法について説明します。

セキュリティ コンテキストについて

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、マルチ コンテキスト モードのガイドライン （15 ページ）を参照してください。

この項では、セキュリティ コンテキストの概要について説明します。

セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチ セキュリティ コンテキストを有効にすることによって、費用対効果の高

い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。

- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用する場合。

コンテキスト コンフィギュレーション ファイル

この項では、ASA がマルチ コンテキスト モードのコンフィギュレーションを実装する方法について説明します。

コンテキスト コンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロン デバイスで設定できるすべてのオプションが指定されています。コンテキスト コンフィギュレーションはフラッシュ メモリ内に保存することも、TFTP、FTP、または HTTP（S）サーバーからダウンロードすることもできます。

システム設定（System Configuration）

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングル モードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メ

モリに自動的に作成されます。このコンテキストの名前は "admin" です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA がパケットを分類する方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。

（注） 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子基準

この項では、分類子で使用される基準について説明します。

（注） インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが 1 つだけの場合、ASA はパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意の MAC アドレスが分類子で使用されます。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。MAC アドレスの自動生成を有効にできます。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

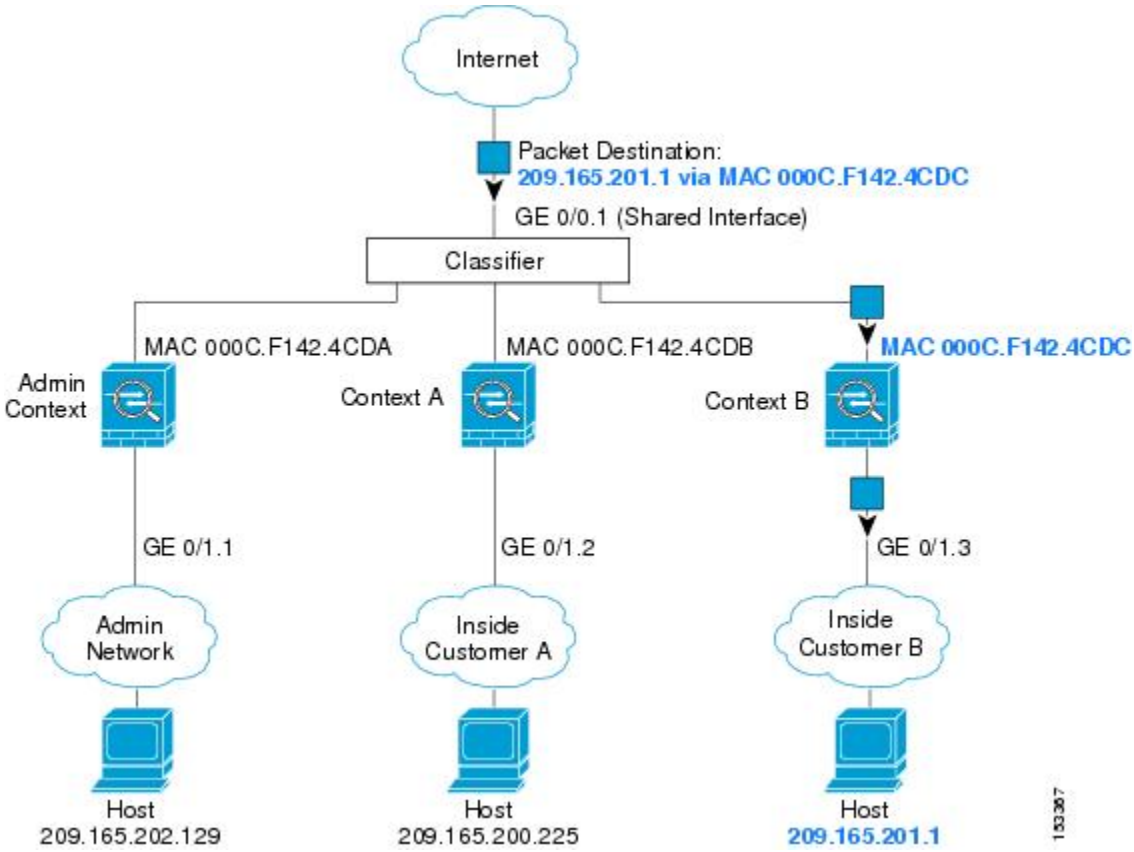
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類例

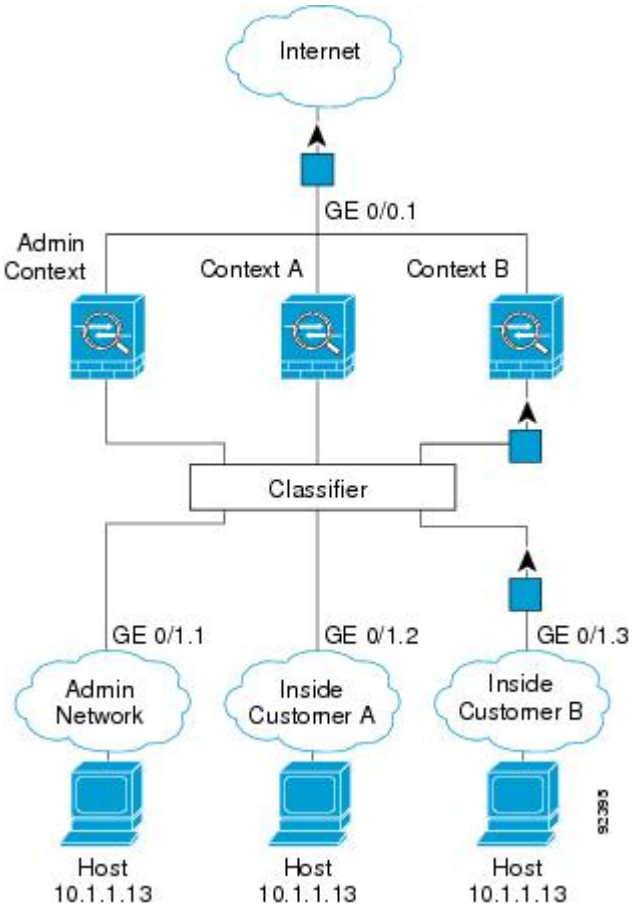
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 *1: MAC* アドレスを使用した共有インターフェイスのパケット分類



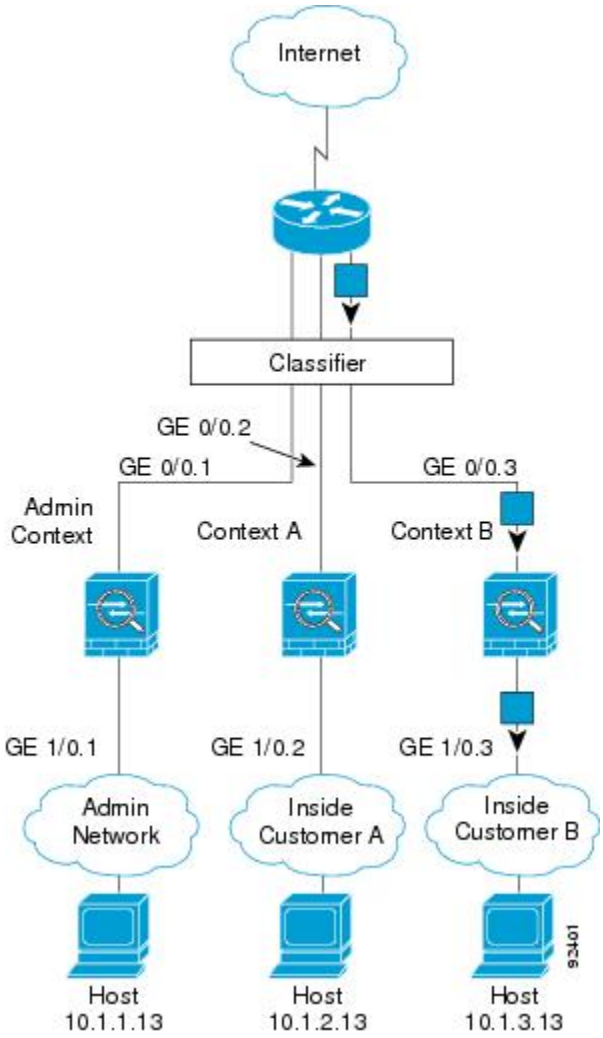
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *2:* 内部ネットワークからの着信トラフィック



トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *3:* トランスペアレント ファイアウォール コンテキスト



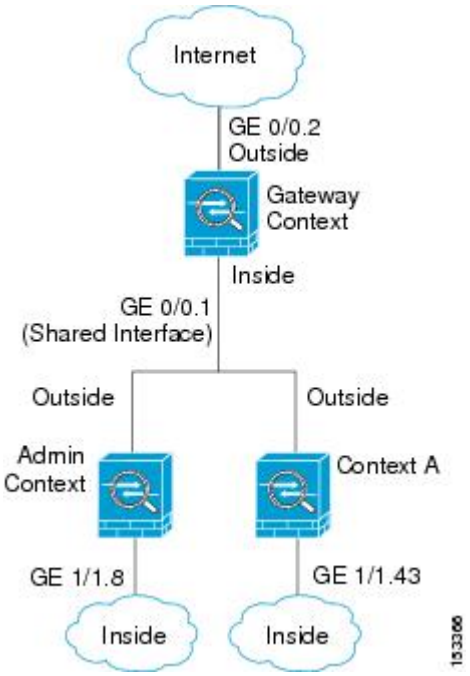
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストのすぐ前に置くことを、コンテキストをカスケード接続するといいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注） コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスが必要です。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

次の図に、ゲートウェイの背後に2つのコンテキストがあるゲートウェイ コンテキストを示します。

図 *4:* コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。

システム管理者のアクセス

2 つの方法で、システム管理者として ASA をアクセスできます。

- ASA コンソールにアクセスする。

  コンソールからシステム実行スペースにアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

システム管理者として、すべてのコンテキストにアクセスできます。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザー名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。

インターフェイス使用率の管理

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

ルーテッド ファイアウォール モードでは、管理インターフェイスをすべてのコンテキストで共有できます。

トランスペアレント ファイアウォール モードの管理インターフェイスは特殊です。許可される最大通過トラフィック インターフェイスに加えて、この管理インターフェイスを個別の管理専用インターフェイスとして使用できます。ただし、マルチコンテキストモードでは、どのインターフェイスもトランスペアレントコンテキスト間で共有させることはできません。代わりに、管理インターフェイスのサブインターフェイスを使用して、各コンテキストにインターフェイスを 1 つ割り当てることができます。ただし、サブインターフェイスを使用できるのは、Firepower デバイスモデル の管理インターフェイスに限られます。の ASA モデルの場合は、データインターフェイスまたはデータインターフェイスのサブインターフェイスを使用して、コンテキスト内のブリッジグループに追加する必要があります。

Firepower 4100/9300 シャーシトランスペアレントコンテキストでは、管理インターフェイスとサブインターフェイスのいずれも、特別なステータスを保持しません。この場合は、コンテキストをデータインターフェイスとして扱い、ブリッジグループに追加する必要があります(シングルコンテキストモードでは、管理インターフェイスで特別なステータスが保持されるので注意してください)。

トランスペアレントモードに関するもう 1 つの考慮事項：マルチコンテキストモードを有効にすると、設定されているすべてのインターフェイスが自動的に管理コンテキストに割り当てられます。たとえば、デフォルト設定に管理インターフェイスが含まれている場合、そのインターフェイスは管理コンテキストに割り当てられます。メインインターフェイスを管理コンテキストに割り当てたままで、ネイティブ VLAN を使用してメインインターフェイスを管理し、サブインターフェイスを使用して各コンテキストを管理するという選択肢もあります。管理コンテキストを透過的にすると、その IP アドレスは削除されることに注意してください。管理コンテキストをブリッジグループに割り当て、BVI に IP アドレスを割り当てる必要があります。

リソース管理の概要

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管

理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

リソース クラス

ASAは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは1つのリソース クラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハード システム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASAはクラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASAはコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます割り当てられた量を超える、VPNセッションの一時的なバーストに対応できるように、ASAは「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バーストセッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

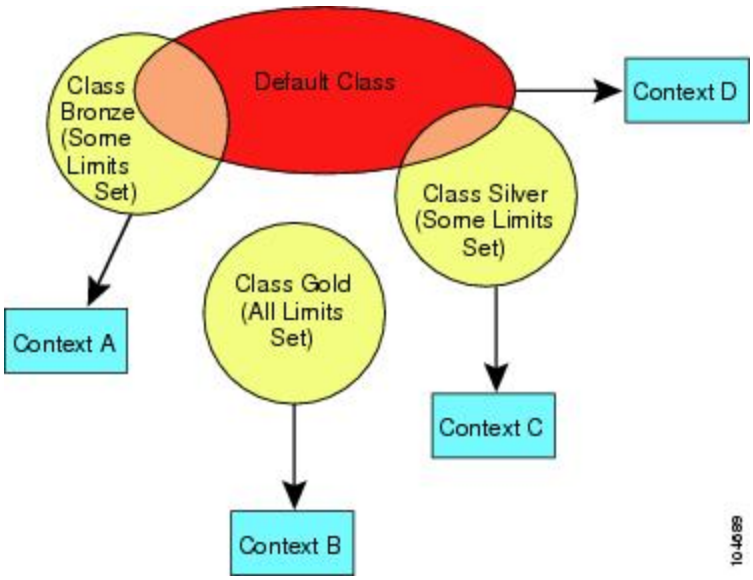
ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。

- ASDM セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（システムの最大値）。
- AnyConnect クライアント ピア — 0 セッション。（AnyConnect クライアント ピアを許可するようにクラスを手動で設定する必要があります）。
- VPN サイトツーサイトトンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。
- HTTPS セッション：6 セッション。（コンテキストあたりの最大値）。

次の図に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

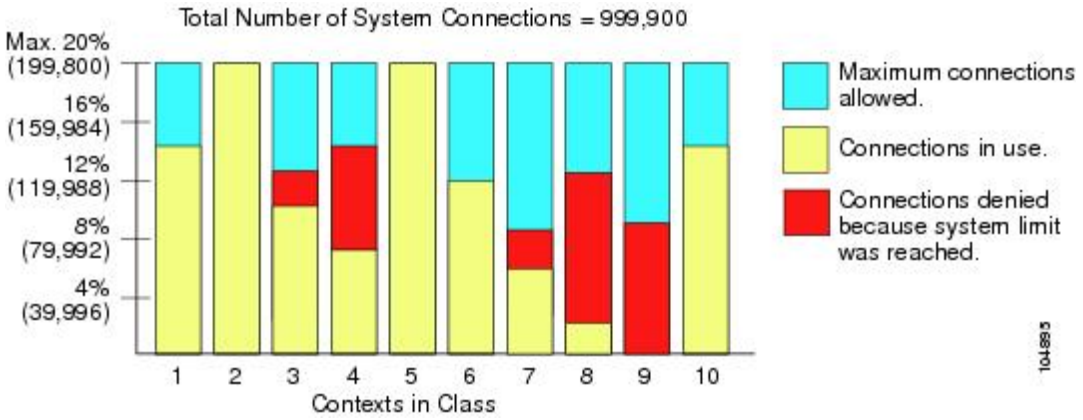
図 *5:* リソース クラス



オーバーサブスクライブ リソースの使用

ASA をオーバーサブスクライブするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。

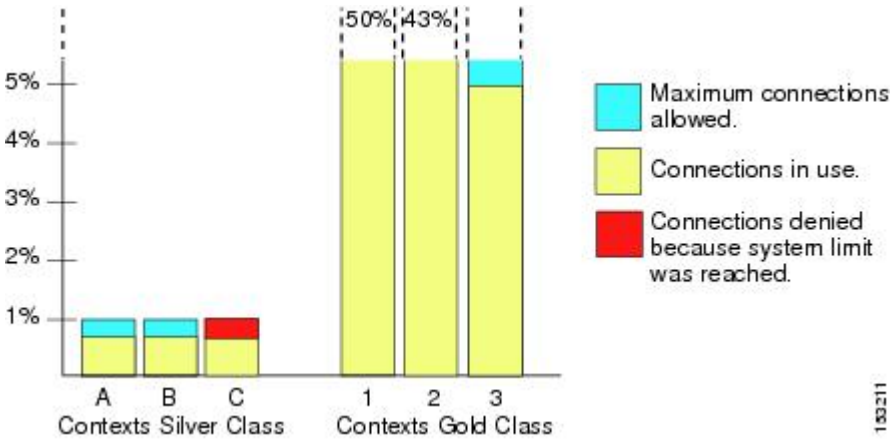
図 *6:* リソース オーバーサブスクリプション



無限リソースの使用

ASA は、パーセンテージや絶対値ではなく、クラス内の 1 つ以上のリソースに無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります無制限アクセスの設定は、ASA のオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

図 *7:* 無限リソース



MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。。

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

マルチコンテキスト モードでの MAC アドレス

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキストインターフェイスそれぞれで仮想 MAC アドレスの自動生成を有効にしてください。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成が有効になっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効な場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

VPN サポート

VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN の場合は、SSL VPN および IKEv2 プロトコルに AnyConnect 3.x 以降を使用する必要があります。 AnyConnect クライアント のイメージとカスタマイズ、およびすべてのコンテキストで共有フラッシュメモリを使用するために、コンテキストごとにフラッシュストレージをカスタマイズできます。サポートされていない機能については、マルチ コンテキスト モードのガイドライン （15 ページ） を参照してください。ASA リリースごとにサポートされる VPN 機能の詳細なリストについては、マルチ コンテキスト モードの履歴 （49 ページ） を参照してください。

（注） マルチコンテキストモードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
Firepower 1010	サポートしない

モデル	ライセンス要件
Firepower 1100	標準ライセンス：2 コンテキスト オプションライセンス、最大： *Firepower 1120*：*5* *Firepower 1140*：*10* *Firepower 1150*：*25*
Firepower 2100	標準ライセンス：2 コンテキスト オプションライセンス、最大： *Firepower 2110*：*25* *Firepower 2120*：*25* *Firepower 2130*：*30* *Firepower 2140*：*40*
Cisco Secure Firewall 3100	標準ライセンス：2 コンテキスト オプションライセンス、最大： *Cisco Secure Firewall 3110*：*100* *Cisco Secure Firewall 3120*：*100* *Cisco Secure Firewall 3130*：*100* *Cisco Secure Firewall 3140*：*100*
Firepower 4100	標準ライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
Firepower 9300	標準ライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
ISA 3000	サポートしない
ASA 仮想	サポートしない

（注） 管理コンテキストに管理専用インターフェイスのみが含まれていて、通過トラフィックのデータインターフェイスが含まれていない場合は、制限に対してカウントされません。

（注） マルチコンテキストモードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードの前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするためにシステムまたは管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。

マルチ コンテキスト モードのガイドライン

フェールオーバー

アクティブ/アクティブ モード フェールオーバーは、マルチ コンテキスト モードでのみサポートされます。

IPv6

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- RIP
- OSPFv3 （OSPFv2 がサポートされます）。
- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- 仮想トンネルインターフェイス（VTI）
- スタティック ルート トラッキング

マルチ コンテキスト モードでは、次のリモート アクセス VPN の機能を現在サポートしません。

- AnyConnect 2.x 以前

- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN ロード バランシング
- カスタマイゼーション
- L2TP

その他のガイドライン

- コンテキストモード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーションファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーションファイルのサブディレクトリを作成します。Background: some models use the FAT 16 file system for internal flash memory, and if you do not use 8.3-compliant short names, or use uppercase characters, then fewer than 512 files and folders can be stored because the file system uses up slots to store long file names（see http://support.microsoft.com/kb/120138/en-us).
- ACI では、すべてのリーフで同じ MAC アドレスを使用してポリシーベースリダイレクト（PBR）ヘルスチェックが実行されます（L2 ping）。これにより、MAC フラップが発生します。MAC フラップを解決するには、インラインセットでタップモードオプションを設定します。ただし、Threat Defense ハイアベイラビリティが設定されている場合は、フェールオーバー中の接続処理のために MAC 学習を有効にする必要があります。したがって、インラインセット インターフェイスを使用する HA ペアの Threat Defense を含む ACI 環境では、パケット損失を回避するために、スタンドアロンかクラスタで Threat Defense を展開します。

マルチ コンテキスト モードのデフォルト

- デフォルトで、ASA はシングル コンテキスト モードになります。
- デフォルト クラス （9 ページ） を参照してください。

マルチ コンテキストの設定

手順

ステップ 1 マルチ コンテキスト モードの有効化または無効化 （17 ページ）。

ステップ 2 （オプション）リソース管理用のクラスの設定 （19 ページ）。

（注） VPN のサポートのために、リソース クラスの VPN リソースを設定する必要があります。デフォルト クラスは VPN を許可しません。

ステップ 3 システム実行スペースでインターフェイスを設定します。

- Firepower 1100、アプライアンスモードの Firepower 2100、Secure Firewall 3100：基本的なインターフェイス設定。
- プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。
- Firepower 4100/9300—論理デバイス Firepower 4100/9300

ステップ 4 セキュリティ コンテキストの設定 （25 ページ）。

ステップ 5 （オプション）コンテキスト インターフェイスへの MAC アドレスの自動割り当て （29 ページ）。

ステップ 6 コンテキストのインターフェイス コンフィギュレーションを完成させます。ルーテッド モードおよびトランスペアレント モードのインターフェイス を参照してください。

マルチ コンテキスト モードの有効化または無効化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティ コンテキスト用に設定されている場合があります。シングル モードからマルチ モードに変換する必要がある場合は、この項の手順に従ってください。

マルチ コンテキスト モードの有効化

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。これらはシステム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルートディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

始める前に

スタートアップ コンフィギュレーションが実行コンフィギュレーションと異なっている場合はバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを2つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。コンフィギュレーションまたはその他のファイルのバックアップと復元を参照してください。

手順

マルチコンテキストモードに変更します。

mode multiple

例：

モードを変更して設定を変換し、システムをリロードするように求められます。

（注） SSH 接続を再確立する前に、管理コンテキストで RSA キーペアを再生成する必要があります。コンソールから、**crypto key generate rsa modulus** コマンドを入力します。詳細については、SSH アクセスの設定 を参照してください。

例：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
```

```
***
***   change mode
```

シングルコンテキスト モードの復元

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングル モードに変更するには、次の手順を実行します。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 元の実行コンフィギュレーションのバックアップバージョンを現在のスタートアップ コンフィギュレーションにコピーします。

copy disk0:old_running.cfg startup-config

例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングル モードに設定します。

mode single

例：

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソース タイプおよび制限を記載します。**show resource types** コマンドも参照してください。

（注） 「システム制限」に「該当なし」と記述されている場合、そのリソースにはハードシステム制限がないため、リソースのパーセンテージを設定できません。

表 *1:* リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
asdm	同時接続数	最小 1 最大 5	200	ASDM 管理セッション。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。
conns	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、モデルごとにサポートされている機能のライセンスを参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。 （注） syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。
hosts	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
http	同時接続数	最小 1 最大 6	100	非 ASDM HTTPS セッション
inspects	利率	該当なし	該当なし	アプリケーション インスペクション数/秒。
mac-addresses	同時接続数	該当なし	65,535	トランスペアレントファイアウォールモードでは、MACアドレステーブルで許可される MAC アドレス数。
ルート	同時接続数	該当なし	該当なし	ダイナミック ルート。
vpn burst anyconnect	同時接続数	該当なし	モデルに応じた AnyConnect クライアントピア数から、**vpn anyconnect** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn anyconnect** でコンテキストに割り当てられた数を超えて許可される AnyConnect クライアント セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、**vpn anyconnect** で割り当てたピア数の合計が全コンテキストで4000の場合は、残りの 1000 セッションが**vpn burst anyconnect** に使用可能です。**vpn anyconnect** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst anyconnect** ではオーバーサブスクライブが可能です。バーストプールをすべてのコンテキストが、先着順に使用できます。
vpn anyconnect	同時接続数	該当なし	ご使用のモデルに使用できる AnyConnect クライアント Premium ピアについては、モデルごとにサポートされている機能のライセンスを参照してください。	AnyConnect クライアントピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえばモデルが 5000 セッションをサポートしており、**vpn other** のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは **vpn burst other** に使用できます。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。
vpn other	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、モデルごとにサポートされている機能のライセンスを参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
ikev1 in-negotiation	同時（パーセンテージのみ）	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てるには、**vpn other** リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション。
ストレージ	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限（MB 単位）。ドライブを指定するには、**storage-url** コマンドを使用します。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
syslogs	利率	該当なし	該当なし	Syslog メッセージ数/秒。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	ネットワーク アドレス変換。

手順

ステップ 1 クラス名を指定して、クラス コンフィギュレーション モードを開始します。

class *name*

例：

```
ciscoasa(config)# class gold
```

name は、最大 20 文字の文字列です。デフォルト クラスの制限値を設定するには、名前として **default** と入力します。

ステップ 2 リソース タイプのリソース制限を設定します。

limit-resource [**rate**] *resource_name number*[**%**]

例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- リソース タイプのリストについては、上記の表を参照してください。**all** を指定すると、すべてのリソースが同じ値に設定されます。特定のリソースの値も指定した場合は、その制限は **all** に対して設定された制限よりも優先されます。
- **rate** 引数を入力して、特定のリソースの毎秒レートを設定します。
- ほとんどのリソースについては、**0** を *number* に対して設定すると、そのリソースは無制限となるか、システム制限を上限とする（システム制限がある場合）ことになります。VPN のリソースについては、**0** を指定すると制限なしと設定されます。
- システム制限がないリソースの場合は、パーセンテージ（**%**）を設定できません。絶対値のみを設定できます。

- また、コンテキスト内で **quota management-session** コマンドを設定して最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

例

たとえば、conns のデフォルト クラス制限を無制限ではなく 10% に設定し、サイト ツーサイト VPN トンネル 5 本と VPN バースト用のトンネル 2 本を許可するには、次のコマンドを入力します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

コンテキストにリソース クラスが設定されている場合、チェックが行われます。VPN リモート アクセスの接続試行の前に適切なライセンスがインストールされていなければ、警告メッセージが生成されます。その場合、管理者が AnyConnect Apex ライセンスを取得する必要があります。たとえば、次のような警告が表示されます。

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義では、コンテキスト名、コンフィギュレーション ファイルの URL、コンテキストが使用できるインターフェイス、およびその他の設定値を指定します。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。トランスペアレントモードのコンテキストでは、コンテキスト間でインターフェイスを共有できないため、サブインターフェイスの使用が必要になる場合があります。管理インターフェイスの使用計画については、「インターフェイス使用率の管理 （8 ページ）」を参照してください。
  - Firepower 1100、アプライアンスモードの Firepower 2100、Secure Firewall 3100：基本的なインターフェイス設定。
  - プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。
  - Firepower 4100/9300—論理デバイス Firepower 4100/9300
- 管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

  ```
  ciscoasa(config)# admin-context name
  ```

  このコンテキストはコンフィギュレーション内にまだ存在しませんが、続いて **context** *name* コマンドを入力して管理コンテキスト コンフィギュレーションに進むことができます。

手順

ステップ 1 コンテキストを追加または変更します。

context *name*

例：

```
ciscoasa(config)# context admin
```

name は最大 32 文字の文字列です。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。

（注） 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 2 （任意） このコンテキストの説明を追加します。

description *text*

例：

```
ciscoasa(config-ctx)# description Admin Context
```

ステップ 3 コンテキストで使用できるインターフェイスを指定します。

インターフェイスを割り当てるには：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

1 つまたは複数のサブインターフェイスを割り当てるには：

allocate-interface *interface_id***.***subinterface* [**-***interface_id***.***subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**]

例：

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

（注） インターフェイス タイプとポート番号の間にスペースを含めないでください。

- これらのコマンドを複数回入力して複数の範囲を指定します。このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスを含むコンテキスト コマンドはいずれも実行コンフィギュレーションから削除されます。
- ルーテッドモードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレントモードでは、インターフェイスを共有できません。
- *mapped_name* は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス IDがコンテキスト内で使用されます。セキュリティ目的で、コンテキストがどのインターフェイスを使用しているかをコンテキスト管理者には知らせないようにすることができます。マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。**int0**、**inta**、**int_0**。
- サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。
  - マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。**int0-int10**。たとえば、gig0/1.1-gig0/1.5 **happy**1-**sad**5 と入力した場合、このコマンドは失敗します。
  - マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次のように、両方の範囲に 100 個のインターフェイス

が含まれている場合：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。たとえば、gig0/0.**100**-gig0/0.**199** int**1**-int**15** と入力した場合、コマンドは失敗します。

- マッピング名を設定している場合に **show interface** コマンドで実際のインターフェイス ID を参照するには、**visible** を指定します。デフォルトの **invisible** キーワードでは、マッピング名だけが表示されます。

ステップ 4 システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別します。

config-url *url*

例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

ステップ 5 （任意）各コンテキストでフラッシュメモリを使用して AnyConnect クライアントなどの VPN パッケージを保存できるだけでなく、AnyConnect クライアント およびクライアントレス SSL VPN ポータルのカスタマイズ用のストレージも提供できます。たとえば、マルチコンテキストモードを使用してダイナミック アクセス ポリシーに AnyConnect クライアント プロファイルを設定する場合、コンテキスト固有のプライベートストレージを計画する必要があります。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。**注**：**mkdir** コマンドを使用して、指定したディスク上にターゲットディレクトリがすでに存在することを確認してください。

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

例：

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

private 記憶域は、コンテキストごとに 1 つ指定できます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。ディスク番号を指定しない場合、デフォルトで disk0 に設定されます。ASA は指定された *path* にサブディレクトリを作成し、コンテキストに基づく名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを **disk1:/private-storage/contextA/** に作成します。オプションで、ファイル システムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、*context_label* を使用します。たとえば、*context_label* を **context** として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。コンテキストごとに許容するディスク容量を制御する方法については、リソース管理用のクラスの設定（19 ページ）を参照してください。

指定できる読み取り専用の **shared** 記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成できます。AnyConnect クライアント パッケージなど、すべてのコンテキストで共有できる共通の大きなファイルの重複を減らすために、共有のストレージスペースを使用で

きます。この記憶域は複数のコンテキストで共有されるため、ASAは記憶域にはコンテキストのサブディレクトリを作成しません。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

ステップ 6 （任意） コンテキストをリソース クラスに割り当てます。

member *class_name*

例：

```
ciscoasa(config-ctx)# member gold
```

クラスを指定しない場合、コンテキストはデフォルト クラスに属します。コンテキストは1つのリソース クラスにだけ割り当てることができます。

ステップ 7 （任意）アクティブ/アクティブ フェールオーバーのフェールオーバー グループにコンテキストを割り当てます。

join-failover-group {**1** | **2**}

例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

デフォルトでは、コンテキストはグループ 1 にあります。管理コンテキストは常にグループ 1 に置く必要があります。

ステップ 8 （任意） このコンテキストに対してクラウド Web セキュリティを有効にします。

scansafe [**license** *key*]

例：

```
ciscoasa(config-ctx)# scansafe
```

license を指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASAは、要求がどの組織からのものかを示すために、認証キーをクラウド Web セキュリティ プロキシ サーバーに送信します。認証キーは 16 バイトの 16 進数です。

ScanSafeの詳細については、ファイアウォールのコンフィギュレーション ガイドを参照してください。

例

次の例では、管理コンテキストを「administrator」と設定し、「administrator」というコンテキストを内部フラッシュ メモリに作成してから、2 つのコンテキストを FTP サーバから追加します。

```
ciscoasa(config)# admin-context admin
```

```
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

この項では、MACアドレスの自動生成の設定方法について説明します。MACアドレスは、コンテキスト内でパケットを分類するために使用されます。

始める前に

- コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規MACアドレスが生成されます。コンテキストインターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。

手順

プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てます。

mac-address auto [**prefix** *prefix*]

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

プレフィックスを入力しない場合は、ASAによって、インターフェイスの最後の2バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コンテキストとシステム実行スペースの切り替え

システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーション モードで編集される実行コンフィギュレーション、つまり **copy** コマンドや **write** コマンドで使用される実行コンフィギュレーションは、ユーザーのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

手順

ステップ 1 コンテキストに変更します。

changeto context *name*

プロンプトが ciscoasa/*name*# に変化します。

ステップ 2 システム実行スペースに変更します。

changeto system

プロンプトが ciscoasa# に変化します。

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。

セキュリティ コンテキストの削除

現在の管理コンテキストは削除できません。ただし、**clear context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

（注） フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラーメッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 単一のコンテキストを削除します。

no context *name*

すべてのコンテキスト コマンドを削除することもできます。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

ステップ 2 すべてのコンテキスト（管理コンテキストを含む）を削除します。

clear context

コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。

始める前に

- コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。

- この手順はシステム実行スペースで実行します。

手順

管理コンテキストを設定します。

admin-context *context_name*

例：

```
ciscoasa(config)# admin-context administrator
```

Telnet、SSH、HTTPS など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

この項では、コンテキスト URL を変更する方法について説明します。

始める前に

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。
- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
  - コンフィギュレーションが同じ場合、変更は発生しません。
  - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバーが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。

- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。
- この手順はシステム実行スペースで実行します。

手順

ステップ 1 （オプション、マージを実行しない場合）コンテキストに変更して、コンフィギュレーションをクリアします。

changeto context *name*

clear configure all

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

マージを実行する場合は、ステップ 2 にスキップします。

ステップ 2 システム実行スペースに変更します。

changeto system

例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

ステップ 3 変更するコンテキストのコンテキスト コンフィギュレーション モードを開始します。

context *name*

例：

```
ciscoasa(config)# context ctx1
```

ステップ 4 新しい URL を入力します。システムは、動作中になるように、ただちにコンテキストをロードします。

config-url *new_url*

例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップ コンフィギュレーションをインポートする。

  このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどの属性の大部分がクリアされます。

- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。

  このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

コンフィギュレーションのクリアによるリロード

手順

ステップ 1 リロードするコンテキストに変更します。

changeto context *name*

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

ステップ 2 実行コンフィギュレーションをクリアします。

clear configure all

このコマンドを実行するとすべての接続がクリアされます。

ステップ 3 コンフィギュレーションをリロードします。

copy startup-config running-config

例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA は、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の手順を実行してください。

手順

ステップ 1 セキュリティ コンテキストの削除 （30 ページ）。

ステップ 2 セキュリティ コンテキストの設定 （25 ページ）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報を表示およびモニタリングする方法について説明します。

コンテキスト情報の表示

システム実行スペースから、名前、割り当てられているインターフェイス、コンフィギュレーション ファイル URL を含むコンテキストのリストを表示できます。

手順

すべてのコンテキストの表示：

show context [*name* | **detail**| **count**]

特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。

detail オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

count オプションを指定すると、コンテキストの合計数が表示されます。

例

次に、**show context** コマンドの出力例を示します。この出力例は、3 個のコンテキストを示しています。

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
```

```
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

次の表は、各フィールドの説明を示しています。

表 *2 : show context* のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
インターフェイス	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

detail の出力の詳細については、コマンド リファレンスを参照してください。

次に、**show context count** コマンドの出力例を示します。

```
ciscoasa# show context count
Total active contexts: 2
```

リソースの割り当ての表示

システム実行スペースから、すべてのクラスおよびクラス メンバーに渡るリソースごとの割り当て状況を表示できます。

手順

リソース割り当てを表示します。

show resource allocation [**detail**]

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況の詳細については、リソースの使用状況の表示（40ページ）を参照してください。

detail 引数を指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

例

次の出力例には、各リソースの合計割り当て量が絶対値および使用可能なシステム リソースの割合として示されています。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 AnyConnect                  1000           10%
 AnyConnectBurst              200           2%
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

次の表は、各フィールドの説明を示しています。

表 *3 : show resource allocation* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASAはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	リソースにハードウェア システム制限がある場合に、コンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A
```

```
SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%

Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%

Routes            default          all       C  unlimited                N/A
                  gold               1       D  unlimited          5      N/A
                  silver             1      CA         10         10      N/A
                  bronze             0      CA          5                 N/A
                  All Contexts:      3                             20      N/A

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040     N/A
                  bronze             0      CA      11520
                  All Contexts:      3                          23040     N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535    100.00%
                  silver             1      CA       6553       6553      9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                         137623    209.99%
```

次の表は、各フィールドの説明を示しています。

表 *4 : show resource allocation detail* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
クラス	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。

フィールド	説明
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「C」または「D」を「A」に組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	クラス内のコンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムの表示は N/A になります。

リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。

手順

コンテキストごとのリソース使用状況を表示します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- デフォルトでは、**all**（すべての）コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。
- 指定したリソースの上位 **n** 人のユーザーとなっているコンテキストを表示するには、*top n* キーワードを入力します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。
- **summary** オプションを指定すると、すべてのコンテキストの使用状況が組み合されて表示されます。
- **system** オプションでは、すべてのコンテキストの使用状況が組み合されて表示されますが、組み合されたコンテキスト制限ではなく、リソースに対するシステムの制限が表示されます。
- **resource** *resource_name* で使用可能なリソース名については、リソース管理用のクラスの設定 （19 ページ） を参照してください。**show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。
- **detail** オプションを指定すると、管理できないリソースを含むすべてのリソースの使用状況が表示されます。たとえば、TCP 代行受信の数を表示できます。
- **counter** *counter_name* には、次のいずれかのキーワードを指定します。
  - **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。
  - **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。
  - **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。
  - **all**：（デフォルト）すべての統計情報を表示します。
- *count_threshold* は、表示するリソースの下限を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。
- すべてのリソースを表示するには、*count_threshold* を **0** に設定します。

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
AnyConnect                  2           25      1000           0 Summary
AnyConnectBurst             0            0      200            0 Summary
Other VPN Sessions          0           10      10           740 Summary
Other VPN Burst             0           10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage summary** コマンドの出力例を示します。このコマンドでは、25 コンテキストの制限が示されます。Telnet 接続および SSH 接続のコンテキストの限界がコンテキストごとに 5 であるため、合計の限界は 125 です。システムの限界が単に 100 であるため、システムの限界が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソース使用状況を表示しますが、組み合わせたコンテキストの限界ではなく、システムの限界を表示しています。現在使用中でないリソースを表示するには、**counter all 0** オプションを指定します。Denied の統計情報は、システム制限がある場合に、その制限によってリソースが拒否された回数を示します。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit          Denied    Context
Telnet                      0            0        100               0    System
SSH                         0            0        100               0    System
ASDM                        0            0         32               0    System
Routes                      0            0        N/A               0    System
```

```
IPSec                     0           0          5              0    System
Syslogs [rate]            1          18        N/A              0    System
Conns                     0           1     280000              0    System
Xlates                    0           0        N/A              0    System
Hosts                     0           2        N/A              0    System
Conns [rate]              1           1        N/A              0    System
Inspects [rate]           0           0        N/A              0    System
AnyConnect                2          25      10000              0    System
AnyConnectBurst           0           0        200              0    System
Other VPN Sessions        0          10        750            740    System
Other VPN Burst           0          10        750            730    System
```

コンテキストでの SYN 攻撃のモニタリング

ASA は TCP 代行受信を使用して SYN 攻撃を阻止します。TCP 代行受信では、SYN クッキーアルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバーのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバーへの接続を許可できます。

手順

ステップ 1 各コンテキストについて、攻撃の割合をモニタリングします。

show perfmon

ステップ 2 個々のコンテキストの TCP 代行受信で使用されるリソースの量をモニターします。

show resource usage detail

ステップ 3 システム全体の TCP 代行受信で使用されるリソースをモニターします。

show resource usage summary detail

例

次に、**show perfmon** コマンドの出力例を示します。このコマンドは、admin というコンテキストの TCP 代行受信レートを表示します。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
```

```
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s     322779/s
```

次に、**show resource usage detail** コマンドの出力例を示します。このコマンドは、個々のコンテキストの TCP 代行受信で使用されるリソース量を表示します。（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit         Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
```

```
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

次の出力例は、システム全体の TCP 代行受信で使用されるリソースを示します（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels              46           48  unlimited             0 Summary
chunk:dbgtrace               4            4  unlimited             0 Summary
chunk:fixup                 45           45  unlimited             0 Summary
chunk:global                 1            1  unlimited             0 Summary
chunk:hole                   3            3  unlimited             0 Summary
chunk:ip-users              24           24  unlimited             0 Summary
chunk:udp-ctrl-blk           1            1  unlimited             0 Summary
chunk:list-elem           1059         1059  unlimited             0 Summary
chunk:list-hdr              10           11  unlimited             0 Summary
chunk:nat                    1            1  unlimited             0 Summary
chunk:route                  5            5  unlimited             0 Summary
chunk:static                 2            2  unlimited             0 Summary
block:16384                510          885  unlimited             0 Summary
block:2048                  32           35  unlimited             0 Summary
tcp-intercept-rate      341306       811579  unlimited             0 Summary
globals                      1            1  unlimited             0 Summary
np-statics                   6            6  unlimited             0 Summary
statics                      2            2        N/A             0 Summary
nats                         1            1        N/A             0 Summary
ace-rules                    3            3        N/A             0 Summary
console-access-rul           4            4        N/A             0 Summary
fixup-rules                 43           44        N/A             0 Summary
```

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。

システム設定での MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

始める前に

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順

システム実行スペースから割り当てられた MAC アドレスを表示します。

show running-config all context [*name*]

割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。**mac-address auto** コマンドは、グローバル コンフィギュレーション モードに限りユーザー設定可能ですが、コンテキスト コンフィギュレーション モードでは、このコマンドは読み取り専用エントリとして、割り当てられたMACアドレスとともに表示されます。コンテキスト内で**nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
```

```
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順

コンテキスト内で各インターフェイスに使用されている MAC アドレスを表示します。

/context# show interface | include (Interface)|(MAC)

例

次に例を示します。

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

（注） **show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

マルチ コンテキスト モードの例

次に例を示します。

- 各コンテキストのMACアドレスを、カスタムプレフィックスを使用して自動的に設定します。
- conns のデフォルト クラス制限を、無制限ではなく 10% に設定し、VPN other セッション数を 10、バーストを 5 に設定します。
- gold リソース クラスを作成します。
- 管理コンテキストを「administrator」と設定します。
- 「administrator」というコンテキストを、デフォルトのリソース クラスの一部になるように、内部フラッシュ メモリ上に作成します。
- gold リソース クラスの一部として FTP サーバーから 2 個のコンテキストを追加します。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
```

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

マルチ コンテキスト モードの履歴

表 *5:* マルチ コンテキスト モードの履歴

機能名	プラットフォームリリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 **context**、**mode**、**class** の各コマンドが導入されました。
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 **mac-address auto** コマンドが導入されました。
リソース管理	7.2(1)	リソース管理が導入されました。 **class**、**limit-resource**、**member** の各コマンドが導入されました。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティ ポリシーを設定することができます。各コンテキストまたはシングル モード ASA を 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。 **allocate-ips** コマンドが導入されました。
MAC アドレス自動割り当ての機能強化	8.5(2)	MAC アドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバー ペアのプライマリ装置とセカンダリ装置の MAC アドレスそれぞれに異なるスキームが使用されます。MAC アドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。 **mac-address auto prefix** 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	機能情報
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	ASA 5550 の最大セキュリティ コンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。
MAC アドレスの自動割り当てのデフォルトでの有効化	8.5(1)	MACアドレスの自動割り当てが、デフォルトでイネーブルになりました。 **mac-address auto** コマンドが変更されました。
MAC アドレス プレフィックスの自動生成	8.6(1)	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）のMACアドレスの最後の2バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時またはMACアドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。**show running-config mac-address** コマンドを入力して、自動生成されたプレフィックスを表示できます。プレフィックスを変更する場合、カスタム プレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバーペアのヒットレスアップグレードを維持するため、ASAは、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックスに手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス メソッドを使用しない場合、異なるスロット番号にインストールされたASASMでは、フェールオーバーが発生した場合にMACアドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MACアドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 **mac-address auto** コマンドが変更されました。
ASASM 以外のすべてのモデル上での MAC アドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	自動MACアドレスの割り当てはASASMを除いて、デフォルトでディセーブルになりました。 **mac-address auto** 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	機能情報
セキュリティ コンテキストでのダイナミック ルーティング	9.0(1)	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。
ルーティング テーブル エントリのための新しいリソース タイプ	9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
マルチ コンテキスト モードのサイトツーサイト VPN	9.0(1)	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	9.0(1)	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ ikev1 in-negotiation が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各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	機能情報
マルチ コンテキスト モードでのリモート アクセス VPN サポート	9.5(2)	次のリモートアクセス機能をマルチコンテキストモードで使用できるようになりました。 • AnyConnect 3.x 以降（SSL VPN のみ、IKEv2 はサポートしません） • 中央集中型 AnyConnect クライアント のイメージの設定 • AnyConnect クライアント のイメージのアップグレード • AnyConnect クライアント 接続のコンテキストリソース管理 （注） マルチコンテキストモードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。 次のコマンドが導入されました。**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect**
マルチ コンテキスト モードの場合の証明書の事前入力/ユーザー名	9.6(2)	AnyConnect クライアント SSL サポートが拡張され、これまでシングルモードでのみ使用可能だった証明書の事前入力とユーザー名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更されたコマンドはありません。
リモート アクセス VPN のフラッシュ仮想化	9.6(2)	マルチ コンテキスト モードのリモート アクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザーのみに関連付けられ、該当ユーザー対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザー コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次のコマンドが導入されました。**limit-resource storage**、**storage-url**
マルチコンテキストデバイスでの AnyConnect クライアントプロファイルのサポート	9.6(2)	AnyConnect クライアントプロファイルは、マルチコンテキストデバイスでサポートされます。ASDM を使用して新しいプロファイルを追加するには、AnyConnect クライアント リリース 4.2.00748 または 4.3.03013 以降が必要です。

機能名	プラットフォームリリース	機能情報
マルチコンテキストモードの AnyConnect クライアント 接続のステートフル フェールオーバー	9.6(2)	マルチコンテキストモードでAnyConnectクライアント接続のステートフルフェールオーバーがサポートされるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN CoA（認可変更）がサポートされました。	9.6(2)	マルチコンテキストモードで、コンテキストごとにCoAを設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードで、リモート アクセス VPN のローカライズがサポートされました。	9.6(2)	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更されたコマンドはありません。
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更されたコマンド：**quota management-session**、**show quota management-session**

機能名	プラットフォームリリース	機能情報
HTTPS リソース管理	9.12(1)	リソースクラスの非ASDM HTTPSセッションの最大数を設定できるようになりました。デフォルトでは、制限はコンテキストあたり最大 6 に設定でき、すべてのコンテキスト全体では最大 100 の HTTPS セッションを使用できます。 新規/変更されたコマンド：**limit-resource http** ASDM サポートはありません。
Firepower 1140 の最大コンテキスト数が 5 から 10 に増加	9.16(1)	Firepower 1140 は、最大 10 のコンテキストをサポートするようになりました。

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。