ホスト名、リソース、ユーザ アカウントおよび SLA の設定

ここでは、セキュリティ アプライアンス上のホスト名の設定、マルチコンテキスト モードの Firewall Services Module（FWSM; ファイアウォール サービス モジュール）でのリソース クラスの定義と管理、ローカル ユーザ データベースでのユーザ アカウントの管理、およびルートトラッキングを実行するための Service Level Agreement（SLA; サービス レベル契約）のモニタリングについて説明します。

この章は次のトピックで構成されています。

[Hostname] ページ

[Hostname] ページを使用して、セキュリティ デバイスのホスト名を指定し、デフォルト ドメインを指定します。設定ファイルが展開されたあとで、他のコマンドで完全修飾ドメインを入力しない場合、デバイスではこのドメイン名が使用されます。RSA キーの生成でもこのドメイン名が使用されます。

デバイスは、このドメイン名を非修飾名に追加します。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、セキュリティアプライアンス が名前に「jupiter.example.com」と入力します。

セキュリティ アプライアンスのホスト名を設定した場合は、その名前がコマンド ライン プロンプトに表示されます。複数のデバイスへのセッションを確立する場合、ホスト名はコマンドを入力する場所の追跡に役立ちます。デフォルトのホスト名はプラットフォームによって異なります。

マルチコンテキスト モードでは、各コンテキストのドメイン名と、システム実行スペースを指定できます。システム実行スペースで指定するホスト名は、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。オプションでコンテキストに設定されているホスト名はコマンドラインに表示されませんが、バナー コマンド $(hostname) トークンでは使用できます。

ナビゲーション パス

デバイスビューでセキュリティデバイスを選択し、次にデバイスポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）] を選択します。

フィールド リファレンス

表 *1 : [Hostname]* ページ

要素	説明
ホスト名	デバイスの区別に役立つ一意のデバイス名（*PIX-510-A* など）を入力します。 （注） 管理するデバイスごとに一意のホスト名を使用することを推奨します。デバイス名には最大 63 文字の英数字（米国英語）を使用でき、次の特殊文字をすべて使用できます。` ( ) + - , . / : =
ドメイン名	オプションで、デバイスの有効なドメインネームシステム（DNS）のドメイン名（*cisco.com* など）を入力します。

マルチコンテキスト FWSM でのリソース管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

デフォルトでは、マルチコンテキスト Firewall Services Module（FWSM; ファイアウォール サービス モジュール）のすべてのセキュリティ コンテキストは、コンテキストごとの最大制限が設定されている場合を除き、FWSM のリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

（注） FWSM はコンテキストあたりの帯域幅を制限しませんが、FWSM が含まれているスイッチは VLAN あたりの帯域幅を制限できます。詳細については、スイッチのマニュアルを参照してください。

FWSM は、リソース クラスにコンテキストを割り当てることで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。クラスを作成する場合、FWSM はクラスに割り当てられている各コンテキストのリソースの一部を確保しませ

ん。代わりに、FWSMはコンテキストの最大制限を設定します。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。

すべてのリソースの制限は、デバイスで使用可能な合計に対するパーセンテージとして設定できます。また、個々のリソースの制限をパーセンテージまたは絶対値として設定できます。

すべてのコンテキストにリソースの100%を超えて割り当てることで、FWSMをオーバーサブスクライブできます。たとえば、接続をコンテキストあたり20%に制限するクラスを設定してから、10個のコンテキストをクラスに割り当てて、合計が200%になるようにできます。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。

FWSMでは、パーセンテージや絶対値の代わりに、クラス内の1つ以上のリソースへの無制限アクセスを割り当てることもできます。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、およびCがクラス「Onepercent」に割り当てられているとします。このクラスでは、各クラスメンバーを1秒あたりのシステム検査の1%に制限すると、合計で3%になりますが、現在3つのコンテキストで合計2%しか使用していません。一方、クラス「Nolimit」では、検査へのアクセスが制限されていません。Nolimitのコンテキストは、「未割り当て」検査の97%より多くを使用できます。コンテキストA、B、およびCが合計限度である3%に到達しないことになるとしても、コンテキストA、B、およびCが現在使用していない1%を合わせて使用できるからです。無制限アクセスの設定はFWSM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。

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対して2%の制限があり、その他の制限はないクラスを作成する場合、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。反対に、すべてのリソースに対して2%の制限があるクラスを作成する場合、クラスはデフォルト クラスの設定を使用しません。

初期設定時に、デフォルトクラスは、デフォルトでコンテキストあたり許可される最大値に設定される次の制限を除き、すべてのコンテキストに対してリソースへの無制限アクセスを提供します。

- Telnet セッション：5 セッション
- SSH セッション：5 セッション
- IPSec セッション：5 セッション
- MAC アドレス：65,535 エントリ

デフォルト クラスは編集できます。

関連項目

- [Resources] ページ （4 ページ）
- [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）

[Resources] ページ

[Resources] ページを使用して、リソース管理クラスを設定および管理します。

このページのテーブルには、現在定義されているすべてのリソースクラスがリストされます。テーブルの下のボタンを使用して、このリストを管理します。

- [Add Row]：新規クラスを定義してセキュリティ コンテキストに割り当てることのできる [Add Resource] ダイアログボックスを開きます。詳細については、[Add Resource]/[Edit Resource] ダイアログボックス （4 ページ）を参照してください。
- [Edit Row]：現在選択されている行で [Edit Resource] ダイアログボックスを開いて、クラスとそのコンテキスト割り当てを編集できるようにします。詳細については、[Add Resource]/[Edit Resource] ダイアログボックス （4 ページ）を参照してください。
- [Delete Row]：現在選択されている行を削除します。確認が必要な場合があります。

ナビゲーション パス

デバイスビューで、マルチコンテキストモードの ASA または FWSM のシステムコンテキストを選択し、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [リソース（Resources）]** を選択します。

関連項目

- マルチコンテキスト FWSM でのリソース管理 （2 ページ）

[Add Resource]/[Edit Resource] ダイアログボックス

[リソースの追加（Add Resources）]/[リソースの編集（Edit Resource）] ダイアログボックスを使用して、FWSM セキュリティコンテキストのリソースクラスと割り当てを追加または編集します。

タイトルを除き、両方のダイアログボックスは同じです。次の説明は両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Resource]/[Edit Resource] ダイアログボックスには、[Resources] ページ （4 ページ）からアクセスできます。

関連項目

- マルチコンテキスト FWSM でのリソース管理 （2 ページ）

フィールド リファレンス

表 *2 : [Add Resource]/[Edit Resource]* ダイアログボックス

要素	説明
クラス名（Class Name）	このクラスの名前を入力します。最大 20 文字の英数字を入力でき、次の特殊文字をすべて使用できます。` ( ) + - , . / : =
[Limits] タブ	
（注）	次の制限については、特定の制限に値を指定しない場合に、制限がデフォルト クラスから継承されます。デフォルト クラスでその制限が設定されていない場合、制限はシステム制限を継承します。また、入力した値は、関連する [パーセント（percent）] ボックスもオンになっていない限り *1* 秒あたりのレートと見なされます（オンになっている場合、値は合計リソースに対するパーセンテージです）。
TCP or UDP Connections	1 つのホストと他の複数のホスト間の接続を含め、任意の 2 つのホスト間の TCP または UDP 接続に対するレート制限を設定します。0（システム制限）～ 102400 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
Inspections (Fixups)	アプリケーション インスペクションのレート制限を設定します。1 秒あたり 0（システム制限）～ 10000 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
Syslog メッセージ	システム ログ メッセージのレート制限を設定します。制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。 FWSM では、FWSM 端末またはバッファに送信されるメッセージに対して 1 秒あたり 30,000 メッセージをサポートできます。メッセージを syslog サーバに送信する場合、FWSM では 1 秒あたり 25,000 がサポートされます。

要素	説明
接続（Connections）	同時の TCP または UDP 接続の絶対制限を設定します。0（システム制限）～ 999900 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。 （注） 同時接続に対して、FWSM は接続を受け入れる 2 つの Network Processor（NP; ネットワーク プロセッサ）それぞれに制限の半分を割り当てます。通常、接続は NP 間に均等に分割されます。ただし、状況によっては、接続が均等に分割されず、一方の NP で最大制限に達する前にもう一方の NP で最大接続制限に達することがあります。この場合、許可される最大接続数は設定した制限を下回ります。NP 分散は、分散アルゴリズムに基づいてスイッチによって制御されます。このアルゴリズムは、スイッチ上で調整することも、不均衡の原因となった接続限度を引き上げて調整することもできます。
ホスト（Hosts）	FWSM を介して同時に接続できるホストの制限を設定します。0（システム制限）～262144 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
IPsec Sessions	IPsec セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 10 で、すべてのコンテキスト間で分割されます。
SSH セッション	SSH セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 100 で、すべてのコンテキスト間で分割されます。
Telnet セッション	同時 Telnet セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 100 で、すべてのコンテキスト間で分割されます。
NAT Translations	同時アドレス変換の制限を設定します。0（システム制限）～ 266144 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100 % を超える値を割り当てることができます。

要素	説明
MAC アドレス	（トランスペアレントモードのみ）MAC アドレステーブルで許可される同時 MAC アドレス エントリの制限を設定します。0（システム制限）～65535 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
ASDM	ASDM 管理セッションの制限を設定します（デフォルトは 5 です）。1 ～ 5 の整数を入力して制限を絶対値で設定するか、3.0 ～ 15.0 のパーセンテージを入力できます。同時セッションの最大数は 80 で、すべてのコンテキスト間で分割されます。 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、80 ASDM セッションのシステム制限は、すべてのコンテキスト間で分割される 160 HTTPS セッションの制限を表します。
Other VPN	サイトツーサイト VPN セッションに対する制限を設定します。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。
Other VPN Burst	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 セッションの数を設定します。たとえば、使用するモデルで 5000 セッションがサポートされており、vpn other で割り当てたセッション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 other vpn burst に使用可能です。other vpn 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 other vpn burst 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がバーストプールを先着順に使用できます。
（注） AnyConnect VPN および AnyConnect VPN Burst の最大値は、ASA ライセンスによって異なります。Cisco Security Manager は、AnyConnect VPN および AnyConnect VPN Burst に入力された値を検証できません。そのため、ユーザーは、AnyConnect VPN および AnyConnect VPN Burst の値が最大値以内であることを確認する必要があります。そうでない場合、展開エラーが発生します。最大値を把握するには、ASA に Telnet 接続して、show version コマンドを実行します。合計 VPN ピアの値は、最大値に対応します。	
AnyConnect VPN	Secure Client 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。

要素	説明
AnyConnect VPN Burst	Secure Client 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 Secure Client 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、Secure Client 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 AnyConnect Burst に使用可能です。Secure Client 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 AnyConnect Burst 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がバーストプールを先着順に使用できます。
ストレージ	バージョン 4.12 以降、Security Manager では、ストレージサイズを入力するか、デフォルトを選択できます。この機能は、ASA バージョン 9.6(2) 以降で使用できます。制限は MB 単位で設定されます。このストレージに複数のディスクを含めることはできないため、デフォルトの上限は設定されたディスクの 100% です。
All Resources Limit	すべてのリソースの制限を設定します。特定のリソースの制限も設定した場合は、その制限によって、すべてのリソースに対してここで設定した制限が上書きされます。制限をパーセンテージで設定できます。または値を **0** に設定することで無制限として設定できます（[パーセント（percent）] がオンになっていない場合）。他の絶対値は設定できません。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。
[Contexts] タブ	
Available Contexts	クラス割り当てに使用可能なすべてのコンテキストがリストされます。クラスがすでに割り当てられているコンテキストは表示されません。 1 つ以上のコンテキストを選択し、[>>] ボタンをクリックしてコンテキストを [Selected Contexts] リストに追加します。
Selected Contexts	このクラスに割り当てられているすべてのコンテキストがリストされます。 1 つ以上のコンテキストを選択し、[<<] ボタンをクリックしてコンテキストを [Available Contexts] リストに戻します。

ユーザ アカウントの設定

[User Accounts] ページを使用すると、ローカル ユーザ データベースを管理できます。ローカルデータベースのユーザーアカウントを認証、許可、およびアカウンティング（AAA）機能とともに使用して、デバイス上で「どのユーザーが何を実行できるか」を指定できます。詳細については、セキュリティ デバイスでの AAA についてを参照してください。

このページのテーブルには、現在定義されているすべてのローカル ユーザ アカウントがリストされ、それぞれのユーザに関して、名前および割り当てられている権限レベルが示されます。これらのフィールドの詳細については、[Add User Account]/[Edit User Account] ダイアログボックス （9 ページ）を参照してください。

重要 Cisco Security Manager 管理対象デバイスの場合、[デバイスのプロパティ（Device Properties）] ページでパスワードを変更する場合は、[ユーザーアカウント（User Accounts）] ページでも同じように更新してください。同じように更新しないと、Cisco Security Manager とデバイス間の通信の初期フェーズは成功し、[接続のテスト（Test Connectivity）] も正常に検証されますが、展開は失敗します。これは、[ユーザーアカウント（User Accounts）] ページで設定されたパスワードが [デバイスのプロパティ（Device Properties）] ページで更新されるためです。したがって、ログイン情報の更新が [デバイスのプロパティ（Device Properties）] ページと [ユーザーアカウント（User Accounts）] ページで並行して実行されるようにすることを推奨します。

- ユーザ アカウントを追加するには、[Add Row] ボタンをクリックします。
- アカウントの設定を編集するには、そのアカウント設定を選択し、[Edit Row] ボタンをクリックします。
- ユーザ アカウントを削除するには、そのアカウントを選択して [Delete Row] ボタンをクリックします。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ローカル データベース
- AAA の準備

[Add User Account]/[Edit User Account] ダイアログボックス

[Add User Account] および [Edit User Account] ダイアログボックスを使用して、ローカル ユーザ アカウントを追加するか、または既存のユーザ アカウントを編集します。

ナビゲーション パス

[Add User Account] および [Edit User Account] ダイアログボックスには、ユーザ アカウントの設定 （8 ページ）で説明しているように、[User Accounts] ページからアクセスできます。

フィールド リファレンス

表 *3 : [Add User Account]/[Edit User Account]* ダイアログボックス

要素	説明
[ユーザー名 （Username）]	ユーザアカウントの名前を入力します。4 文字以上である必要があります。最大値は 64 文字です。エントリは、大文字と小文字が区別されます。
パスワード	
[暗号化されたパスワード（Password as encrypted）]	[プレーンテキスト （Plain Text）] または [暗号化 （Encrypted）] を選択します。
[パスワード暗号化タイプ（Password encrypt type）]	[MD5] または [PBKDF2] を選択します。
パスワード	このユーザーアカウント固有のパスワードを入力します。エントリは、大文字と小文字が区別されます。 （注） セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。 （注） プレーンテキストパスワードの場合： • MD5 パスワードの長さは 3 ～ 32 文字にする必要があります。 • PBKDF2 パスワードの長さは、33 ～ 127 文字にする必要があります。展開の失敗を避けるために、PBKDF2 パスワードに正しい `sha` キー値が使用されていることを確認します。
確認 （Confirm）	確認のためにユーザ パスワードを再入力します。
特権レベル	ユーザの権限レベルを選択します。ローカル コマンド認可を定義します。範囲は、0（最低）～15（最高）です。デフォルトの特権レベルは 2 です。

接続を維持するためのサービス レベル契約（SLA）のモニタリング

サービスレベル契約をモニタリングしてルートトラッキングを実行するように、バージョン 7.2 以降を実行している ASA または PIX デバイスを設定できます。別のネットワーク上のデバイスへの接続性をモニタリングすることによって、プライマリ ルートの可用性をトラッキングし、プライマリ ルートに障害が発生した場合のバックアップ ルートを準備することができます。たとえば、インターネット サービス プロバイダー（ISP）ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。この方法はデュアル ISP と呼ばれ、セキュリティ アプライアンスにハイ アベイラビリティをもたらします。ハイ アベイラビリティは、カスタマーに必要なサービスを提供するための重要な要素となります。

ルートが有効かどうかを本質的に判断するメカニズムは、ルート トラッキング以外には存在しません。ネクスト ホップ ゲートウェイが使用できなくなった場合にも、スタティック ルートはルーティング テーブル内に残ります。セキュリティ アプライアンス上の関連付けられたインターフェイスがダウンした場合にのみ削除されます。

セキュリティ アプライアンスは、SLA モニタのポリシー オブジェクトで定義したモニタリング対象にルートを関連付けることによって、ルート トラッキングを実行します。対象のモニタリングは、オブジェクトで設定されたパラメータに従い、ICMP エコー要求を使用して行われます。指定された時間内にエコー応答が受信されない場合、SLA モニタはダウンしていると見なされ、関連付けられたルートがルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージング アウトしません）。

関連項目

- スタティック ルートの設定
- ファイアウォール デバイスのインターフェイスの設定
- ポリシー オブジェクトの作成

ここでは、次の内容について説明します。

- サービス レベル契約の作成 （11 ページ）

サービス レベル契約の作成

次の手順では、SLA モニタ オブジェクトを設定し、ASA または PIX の設定で、それらのオブジェクトをルートおよびインターフェイスに関連付ける方法について説明します。

関連項目

- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （11 ページ）
- スタティック ルートの設定
- ファイアウォール デバイスのインターフェイスの設定
- ポリシー オブジェクトの作成

ステップ 1 SLA モニタ ポリシー オブジェクトを作成します。

a) **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開き（Policy Object Managerを参照）、コンテンツテーブルから [SLAモニター（SLA Monitors）] を選択します。

ヒント SLA モニタ オブジェクトは、このオブジェクト タイプを使用するポリシーを定義する際に作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

b) 作業領域を右クリックして [新しいオブジェクト（New Object）] を選択し、[SLAモニターを追加（Add SLA Monitor）] ダイアログボックスを開きます。詳細については、 SLA モニタ オブジェクトの設定 （13 ページ）を参照してください。

c) モニタリング オプションはほとんどの接続に適しているため、設定する必要があるのは次の項目のみです。

- [Name]：オブジェクトの名前。
- [SLA Monitor ID]：モニタリング プロセスを識別する番号。この番号は 1 つのデバイス設定内で一意である必要があります。
- [Monitored Address]：モニタリング対象のアドレス。モニタリング対象を選択する場合は、その対象が ICMP エコー要求（ping）に応答できることを確認してください。対象には任意のネットワーク アドレスを選択できますが、次のどれを使用するか検討する必要があります。
- ISP ゲートウェイ アドレス。
- ネクスト ホップ ゲートウェイ アドレス（ISP ゲートウェイの可用性を確認する場合）。
- セキュリティ アプライアンスが通信する必要のある、AAA サーバなどのターゲット ネットワーク上のサーバ。
- 宛先ネットワーク上の永続的なネットワーク デバイス（夜間にシャットダウンされるデスクトップ コンピュータやノートブック コンピュータは適切ではありません）。
- [Interface]：ICMP メッセージのソースとなるインターフェイスを識別する、インターフェイス名またはインターフェイス ロール。デバイスでは、監視対象のアドレスに対して、このインターフェイスの IP アドレスから ping が行われます。

d) [OK] をクリックしてオブジェクトを保存します。

ステップ 2 このオブジェクトを使用してルートをモニタリングするように、ASA/PIX ポリシーを設定します。SLA をモニタリングするために、次のポリシーを設定できます。

- **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [静的ルート（Static Route）]**：スタティックルートを定義するとき、そのルートに対するルートトラッキングを実行する SLA モニタオブジェクトを選択できます。詳細については、スタティック ルートの設定および[Add Static Route]/[Edit Static Route] ダイアログボックスを参照してください。
- [インターフェイス（Interfaces）]：DHCP または PPPoE を使用するインターフェイスを定義するとき、DHCP または PPPoE の学習されたデフォルトルートがトラッキングされるように設定できます。詳細については、デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降）を参照してください。

SLA モニタ オブジェクトの設定

[Add SLA Monitor] と [Edit SLA Monitor] ダイアログボックスを使用すると、SLA モニタ オブジェクトを作成、編集およびコピーできます。各 SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティング テーブルから削除され、バックアップ ルートに置き換えられます。

SLA モニターは、PIX/ASA バージョン 7.2 以降を実行するセキュリティアプライアンスにのみ設定できます。SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージングアウトしません）。

SLA モニタ オブジェクトの設定と使用の詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （11 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SLAモニター（SLA Monitors）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （11 ページ）
- Policy Object Manager

フィールド リファレンス

表 4 : [SLA Monitor] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。

要素	説明
説明	（任意）オブジェクトの説明。
SLA Monitor ID	SLA 操作の ID 番号。値の範囲は 1 ～ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。
Monitored Address	SLA 操作によって可用性をモニタリングされる IP アドレス。モニタリングするアドレスの選択に関する推奨事項については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （11 ページ）を参照してください。
インターフェイス	可用性をテストするためにモニタリング対象のアドレスに対して送信される、すべての ICMP エコー要求の送信元インターフェイス。インターフェイスやインターフェイス ロールの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択するか新しいインターフェイス ロールを作成します。
周波数（Frequency）	ICMP エコー要求の送信頻度（秒単位）。値の範囲は 1 ～ 604800 秒（7 日）です。デフォルトは 60 秒です。 （注） 頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。
[しきい値（Threshold）]	上昇しきい値が宣言されるまでに、ICMP エコー要求のあとに経過する必要のある時間（ミリ秒単位）。値の範囲は 0 ～ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。 しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であるかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。 （注） しきい値はタイムアウト値を超過しないようにします。
時間切れ（Time out）	SLA 操作が ICMP エコー要求への応答を待機する時間（ミリ秒単位）。値の範囲は 0 ～ 604800000 ミリ秒（7 日）です。デフォルトは 5000 ミリ秒です。 モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。 （注） タイムアウト値は頻度値を超過できません。2 つの数値を比較するには、頻度値をミリ秒に換算してください。

要素	説明
Request Data Size	ICMP 要求パケット ペイロードのサイズ（バイト単位）。値の範囲は 0 ～ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit（PMTU）で許可される最大値を超える値を設定しないでください。 場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTUが小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリ パスが使用されます。
ToS	ICMP 要求パケットの IP ヘッダー内に定義されたタイプ オブ サービス（ToS）。値の範囲は 0 ～ 255 です。デフォルトは 0 です。 このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシー ルーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセス レートなどの機能によって使用される場合もあります。
パケット数	送信されたパケットの数。値の範囲は 1 ～ 100 です。デフォルトは 1 パケットです。 **ヒント** パケット損失によって、セキュリティ アプライアンスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

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