



clear lisp eid コマンド ~ clear xlate コマンド

clear lisp eid

ASA EID テーブルをクリアするには、特権 EXEC モードで **clear lisp eid** コマンドを使用します。

```
clear lisp eid [ip_address]
```

構文の説明

<i>ip_address</i>	指定した IP アドレスを EID テーブルから削除します。
-------------------	--------------------------------

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は EID と サイト ID を 相 関 付 け る EID テーブルを維持します。**clear lisp eid** コマンドは、テーブルの EID エントリをクリアします。

クラスタフローモビリティの LISP インспекションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタメンバーは、最初のホップルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタフローモビリティには複数の相互に関連する設定が含まれています。

1. (オプション)ホストまたはサーバの IP アドレスに基づく検査される EID の限定:最初のホップルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp, allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインспекション:ASA は、最初のホップルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフローモビリティを有効にするサービスポリシー:ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フローモビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID:ASA は各クラスタユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フローモビリティを有効にするクラスタレベルの設定:クラスタレベルでもフローモビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フローモビリティカウンタをクリアします。
cluster flow-mobility lisp	サービスポリシーのフローモビリティを有効にします。
flow-mobility lisp	クラスタのフローモビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタシャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フローモビリティカウンタを表示します。

コマンド	説明
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

clear local-host

接続制限や初期接続制限など、クライアントごとの実行時状態を再初期化するには、特権 EXEC モードで **clear local-host** コマンドを使用します。

```
clear local-host [ip_address] [all] [zone [zone_name]]
```

構文の説明

all	(任意)to-the-box トラフィックを含む、すべての接続をクリアします。 all キーワードを指定しない場合は、through-the-box トラフィックだけがクリアされます。
<i>ip_address</i>	(任意)ローカルホストの IP アドレスを指定します。
zone [zone_name]	(オプション)ゾーン接続を指定します。

デフォルト

すべての through-the-box 実行時状態をクリアします。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	zone キーワードが追加されました。

使用上のガイドライン

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が継続されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear local-host** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。さらにきめ細かく接続をクリアするための **clear conn** コマンドや、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを代わりに使用することもできます。

clear local-host コマンドは、ホストライセンス制限からホストを解放します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

例

次に、10.1.1.15 のホストの実行時状態および関連する接続をクリアする例を示します。

```
ciscoasa# clear local-host 10.1.1.15
```

関連コマンド

コマンド	説明
clear conn	あらゆる状態の接続を切断します。
clear xlate	ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ログイング バッファをクリアするには、特権 EXEC モードで **clear logging asdm** コマンドを使用します。

clear logging asdm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、 clear pdm logging コマンドから clear asdm log コマンドに変更されました。

使用上のガイドライン

ASDM システム ログ メッセージは、ASA のシステム ログ メッセージとは別のバッファに格納されます。ASDM ログイング バッファをクリアすると、ASDM システム ログ メッセージだけがクリアされます。ASA のシステム ログ メッセージはクリアされません。ASDM システム ログ メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次に、ASDM ログイング バッファをクリアする例を示します。

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ログイング バッファの内容を表示します。

clear logging buffer

ログバッファをクリアするには、特権 EXEC モードで **clear logging buffer** コマンドを使用します。

clear logging buffer

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
ciscoasa# clear logging buffer
```

関連コマンド

コマンド	説明
logging buffered	ログ バッファを設定します。
show logging	ロギング情報を表示します。

clear logging counter

ログに記録されたカウンタと統計情報をクリアするには、特権 EXEC モードで **clear logging counter** コマンドを使用します。

clear logging counter { all | console | monitor | buffer | trap | asdm | mail }

構文の説明

counter 指定されたロギングの宛先に対するカウンタと統計情報をクリアします。すべてのロギングの宛先に対する統計情報をクリアするには、**all** を指定します。オプションで、**console**、**monitor**、**buffer**、**trap**、**asdm**、**mail** の統計情報をクリアする宛先を指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

show logging コマンドは、ASA で設定された各ロギングカテゴリについてログに記録されたメッセージの統計情報を提供します。これらの統計情報/カウンタをクリアするには、**clear logging counter** コマンドを使用します。

例

次の例では、ログに記録されたメッセージのカウンタをクリアする方法について示します。

```
ciscoasa# clear logging counter all
```

関連コマンド

コマンド	説明
show logging	ロギング情報を表示します。

clear logging queue bufferwrap

保存されたログバッファ (ASDM、内部、FTP、およびフラッシュ) をクリアするには、特権 EXEC モードで **clear logging queue bufferwrap** コマンドを使用します。

clear logging queue bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、保存されているログバッファの内容をクリアする例を示します。

```
ciscoasa# clear logging queue bufferwrap
```

関連コマンド

コマンド	説明
logging buffered	ログバッファを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリをクリアするには、特権 EXEC モードで **clear mac-address-table** コマンドを使用します。

```
clear mac-address-table [interface_name]
```

構文の説明

interface_name (任意) 選択したインターフェイスの MAC アドレス テーブル エントリをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ダイナミック MAC アドレス テーブルのエントリをクリアする例を示します。

```
ciscoasa# clear mac-address-table
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory appcache-threshold

memory appcache-threshold のヒットカウントをクリアするには、特権 EXEC モードで **clear memory appcache-threshold** コマンドを使用します。

clear memory appcache-threshold

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーター	トランス パレント	シングル	マルチ	
				コンテ キ スト	シ ス テ ム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

アプリケーション キャッシュのしきい値に達するたびに、カウンタは 1 ずつ増加します。**clear memory appcache-threshold** コマンドは、メモリ アプリケーション キャッシュのしきい値のヒットカウントをクリアし、0 にリセットします。

例

次に、memory appcache-threshold のヒットカウントをクリアする例を示します。

```
ciscoasa# clear memory appcache-threshold
```

関連コマンド

コマンド	説明
memory appcache-threshold enable	特定のメモリしきい値に達した後のアプリケーション キャッシュの割り当てを制限するには、memory appcache-threshold を有効にします。
show memory appcache-threshold	メモリ appcache しきい値のステータスとヒット数を表示します。

clear memory delayed-free-poisoner

delayed free-memory poisoner ツールのキューと統計情報をクリアするには、特権 EXEC モードで **clear memory delayed-free-poisoner** コマンドを使用します。

clear memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドは、delayed free-memory poisoner ツールのキューで保持されているすべてのメモリを検証なしでシステムに戻し、関連する統計情報カウンタをクリアします。

例

次に、delayed free-memory poisoner ツールのキューと統計情報をクリアする例を示します。

```
ciscoasa# clear memory delayed-free-poisoner
```

関連コマンド

コマンド	説明
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキューを検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファをクリアするには、特権 EXEC モードで **clear memory profile** コマンドを使用します。

clear memory profile [peak]

構文の説明

peak (任意) ピーク メモリ バッファの内容をクリアします。

デフォルト

デフォルトでは、現在「使用されている」プロファイル バッファをクリアします。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドラ イン

clear memory profile コマンドは、プロファイリング機能によって保持されているメモリ バッファを解放します。したがって、プロファイリングは、クリアされる前に停止している必要があります。

例

次に、プロファイリング機能によって保持されているメモリ バッファをクリアする例を示します。

```
ciscoasa# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況(メモリ プロファイリング)のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	ASA のメモリ使用状況(プロファイリング)に関する情報を表示します。

clear mfib counters

MFIB ルータ パケット カウンタをクリアするには、特権 EXEC モードで **clear mfib counters** コマンドを使用します。

clear mfib counters [*group* [*source*]]

構文の説明

<i>group</i>	(任意) マルチキャスト グループの IP アドレスです。
<i>source</i>	(任意) マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタがクリアされます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべての MFIB ルータ パケット カウンタをクリアする例を示します。

```
ciscoasa# clear mfib counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウント データを表示します。

clear module

ASA 上の SSM に関する情報、ASA 5505 上の SSC に関する情報、ASA 5585-X にインストールされた SSP に関する情報、ASA 5585-X にインストールされた IPS SSP に関する情報、ASA サービス モジュールに関する情報、およびシステム情報をクリアするには、特権 EXEC モードで **clear module** コマンドを使用します。

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

構文の説明

all	(デフォルト)すべての SSM 情報をクリアします。
console	(オプション)モジュールのコンソール ログ情報をクリアします。
details	(オプション)SSM(たとえば ASA-SSM-x0 など)のリモート管理コンフィギュレーションを含め、追加情報をクリアします。
log	(オプション)モジュールのログ情報をクリアします。
<i>mod_id</i>	IPS などのソフトウェア モジュールで使用されるモジュール名をクリアします。
recover	(オプション)SSM について、 hw-module module recover コマンドの設定をクリアします。 (注) recover キーワードが有効になるのは、 hw-module module recover コマンドに configure キーワードを使用して SSM のリカバリ コンフィギュレーションを作成した場合のみです。 (オプション)ASA 5512-X、5515-X、5525-X、5545-X、または 5555-X にインストールされた IPS モジュールについて、 sw-module module mod_id recover configure image image_location コマンドの設定をクリアします。
<i>slot</i>	モジュールのスロット番号を指定します。0 または 1 のいずれかになります。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。
	8.2(1)	SSC のサポートが追加されました。
	8.2(5)	ASA 5585-X と ASA 5585-X 上の IPS SSP のサポートが追加されました。
	8.4(2)	デュアル SSP インストールのサポートが追加されました。
	8.5(1)	ASASM のサポートが追加されました。
	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のサポートが追加されました。

使用上のガイドライン このコマンドは、SSC、SSM、ASASM、IPS SSP、デバイス インターフェイス、および組み込みインターフェイスに関する情報をクリアします。

例 次に、SSM のリカバリ設定をクリアする例を示します。

```
ciscoasa# clear module 1 recover
```

関連コマンド	コマンド	説明
	hw-module module recover	リカバリ イメージを TFTP サーバからロードして、SSM を回復します。
	hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
	hw-module module reload	SSM ソフトウェアをリロードします。
	hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
	show module	SSM 情報を表示します。

clear nac-policy

NAC ポリシーの使用状況の統計情報をリセットするには、グローバル コンフィギュレーション モードで **clear nac-policy** コマンドを使用します。

clear nac-policy [*nac-policy-name*]

構文の説明	<i>nac-policy-name</i> (任意)使用状況の統計情報をリセットする NAC ポリシーの名前。
--------------	--

デフォルト	名前を指定しない場合、CLI は、すべての NAC ポリシーに関する使用状況の統計情報をリセットします。
--------------	--

コマンドモード	次の表に、コマンドを入力できるモードを示します。
----------------	--------------------------

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルールテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
グローバル コンフィギュレー ション	• 対応	• 対応	—	—	• 対応

コマンド履歴	リリース	変更内容
	8.0(2)	このコマンドが追加されました。

例 次に、framework1 という名前の NAC ポリシーの使用状況の統計情報をリセットする例を示します。

```
ciscoasa(config)# clear nac-policy framework1
```

次に、NAC ポリシーの使用状況の統計情報をすべてリセットする例を示します。

```
ciscoasa(config)# clear nac-policy
```

関連コマンド	コマンド	説明
	show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
	show vpn-session_summary.db	IPsec、WebVPN、および NAC セッションの数を表示します。
	show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

clear nat counters

NAT ポリシー カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear nat counters** コマンドを使用します。

```
clear nat counters [src_ifc [src_ip [src_mask]] [dst_ifc [dst_ip [dst_mask]]]
```

構文の説明

<i>dst_ifc</i>	(任意)フィルタリングする宛先インターフェイスを指定します。
<i>dst_ip</i>	(任意)フィルタリングする宛先 IP アドレスを指定します。
<i>dst_mask</i>	(任意)宛先 IP アドレスのマスクを指定します。
<i>src_ifc</i>	(任意)フィルタリングする送信元インターフェイスを指定します。
<i>src_ip</i>	(オプション)フィルタリングする送信元 IP アドレスを指定します。
<i>src_mask</i>	(オプション)送信元 IP アドレスのマスクを指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
グローバル コンフィギュレ ーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0 (4)	このコマンドが追加されました。

例

次に、NAT ポリシー カウンタをクリアする例を示します。

```
ciscoasa(config)# clear nat counters
```

関連コマンド

コマンド	説明
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
nat-control	NAT 設定要件をイネーブルまたはディセーブルにします。
show nat counters	プロトコル スタック カウンタを表示します。

clear nve

NVE 送信元インターフェイス統計情報をクリアするには、特権 EXEC モードで **clear nve** コマンドを使用します。

clear nve 1

構文の説明

1 NVE インスタンスを指定します(常に 1)。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイスのステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスをクリアします。

例

次に、NVE インターフェイスの統計情報をクリアする例を示します。

```
ciscoasa# clear nve 1
```

関連コマンド

コマンド	説明
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。

clear object-group

ネットワーク オブジェクト グループのオブジェクトのヒット カウントをクリアするには、特権 EXEC モードで **clear object-group** コマンドを使用します。

clear object-group *obj-name* **counters**

構文の説明

counters	ネットワーク オブジェクト グループのカウンタを指定します。
<i>obj-name</i>	既存のネットワーク オブジェクト グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

単一のネットワーク オブジェクト グループにあるオブジェクトのヒット カウントだけをクリアするには、このコマンドを使用します。

例

次に、「Anet」という名前のネットワーク オブジェクト グループのネットワーク オブジェクト ヒット カウントをクリアする例を示します。

```
ciscoasa# clear object-group Anet counters
```

関連コマンド

コマンド	説明
show object-group	指定したオブジェクト グループがネットワーク オブジェクト グループ タイプである場合に、オブジェクト グループ情報およびヒット カウントを表示します。

clear ospf

OSPF プロセス情報をクリアするには、特権 EXEC モードで **clear ospf** コマンドを使用します。

clear ospf [*pid*] {*process* | *counters*}

構文の説明

counters	OSPF カウンタをクリアします。
<i>pid</i>	(任意)OSPF ルーティング プロセスの内部使用の ID パラメータ。有効な値は、1 ~ 65535 です。
process	OSPF ルーティング プロセスを再起動します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドをクリアするには、このコンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。



(注)

clear configure router ospf コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドをクリアしません。

例

次に、OSPF ネイバー カウンタをクリアする例を示します。

```
ciscoasa# clear ospf counters
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべてのグローバルルータ コマンドをクリアします。

clear pclu

PC 論理更新統計情報をクリアするには、特権 EXEC モードで **clear pclu** コマンドを使用します。

clear pclu

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、PC 情報をクリアする例を示します。

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

電話プロキシ データベース内のセキュア フォン エントリをクリアするには、特権 EXEC モードで **clear phone-proxy secure-phones** コマンドを使用します。

clear phone-proxy secure-phones [*mac_address* | **noconfirm**]

構文の説明

mac_address	電話プロキシ データベースから、指定した MAC アドレスを持つ IP フォンを削除します。
noconfirm	確認プロンプトなしで、電話プロキシ データベース内のすべてのセキュア フォン エントリを削除します。 noconfirm キーワードを指定しない場合は、すべてのセキュア フォン エントリを削除するかどうかを確認するプロンプトが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に (**timeout secure-phones** コマンドを介して) 削除されます。または、**clear phone-proxy secure-phones** コマンドを使用すると、設定済みのタイムアウトが経過する前に電話プロキシ データベースをクリアできます。

例

次に、電話プロキシ データベース内のセキュア エントリをクリアする例を示します。

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

関連コマンド

コマンド	説明
timeout secure-phones	アイドル タイムアウトを設定します。この時間を経過すると、電話プロキシ データベースからセキュア フォン エントリが削除されます。

clear pim counters

PIM トラフィック カウンタをクリアするには、特権 EXEC モードで **clear pim counters** コマンドを使用します。

clear pim counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、トラフィック カウンタだけをクリアします。PIM トポロジ テーブルをクリアするには、**clear pim topology** コマンドを使用します。

例

次に、PIM トラフィック カウンタをクリアする例を示します。

```
ciscoasa# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim topology	PIM トポロジ テーブルをクリアします。
show pim traffic	PIM トラフィック カウンタを表示します。

clear pim group-map

グループからのランデブーポイント(RP)へのマッピングエントリをRPマッピングキャッシュから削除するには、**clear pim group-map** コマンドを使用します。

clear pim group-map [*rp-address*]

構文の説明

rp-address ランデブーポイントのマッピングアドレス。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが導入されました。

例

次に、RPアドレス 23.23.23.2 のグループから RP へのマッピングのエントリを削除する例を示します。

```
ciscoasa(config)# sh pim group-map
Group Range          Proto Client Groups RP address      Info
-----
224.0.1.39/32*      DM    static 0        0.0.0.0
224.0.1.40/32*      DM    static 0        0.0.0.0
224.0.0.0/24*       L-Localstatic 1    0.0.0.0
232.0.0.0/8*        SSM   config 0        0.0.0.0
224.0.0.0/4*        SM    config 0        9.9.9.9          RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0        23.23.23.2      RPF: Gi0/3,23.23.23.2

ciscoasa(config)# clear pim group-map 23.23.23.2
ciscoasa(config)# sh pim group-map
Group Range          Proto Client Groups RP address      Info
-----
224.0.1.39/32*      DM    static 0        0.0.0.0
224.0.1.40/32*      DM    static 0        0.0.0.0
224.0.0.0/24*       L-Localstatic 1    0.0.0.0
232.0.0.0/8*        SSM   config 0        0.0.0.0
224.0.0.0/4*        SM    config 0        9.9.9.9          RPF: ,0.0.0.0
224.0.0.0/4         SM    static 0        0.0.0.0          RPF: ,0.0.0.0
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim reset

リセットによって MRIB 同期を強制するには、特権 EXEC モードで **clear pim reset** コマンドを使用します。

clear pim reset

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トポロジテーブルのすべての情報がクリアされ、MRIB 接続がリセットされます。このコマンドは、PIM トポロジテーブルと MRIB データベース間の状態を同期するために使用できます。

例

次に、トポロジテーブルをクリアし、MRIB 接続をリセットする例を示します。

```
ciscoasa# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジテーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim topology

PIM トポロジ テーブルをクリアするには、特権 EXEC モードで **clear pim topology** コマンドを使用します。

clear pim topology [*group*]

構文の説明

group (任意) トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

オプションの *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリがクリアされます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスぺアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートをクリアします。IGMP ローカルメンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけがクリアされます。

例

次に、PIM トポロジ テーブルをクリアする例を示します。

```
ciscoasa# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear priority-queue statistics

任意のインターフェイスまたは設定されたすべてのインターフェイスのプライオリティ キュー統計情報カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear priority-queue statistics** コマンドを使用します。

clear priority-queue statistics [*interface-name*]

構文の説明

interface-name (任意) ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティ キュー統計情報をクリアします。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—
グローバル コンフィギュレー ション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードで **clear priority-queue statistics** コマンドを使用して、「test」という名前のインターフェイスのプライオリティ キュー統計情報を削除する例を示します。

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure priority queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。

コマンド	説明
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear process

ASA 上で実行されている特定のプロセスの統計情報をクリアするには、特権 EXEC モードで **clear process** コマンドを使用します。

clear process [cpu-hog | internals]

構文の説明

cpu-hog	高 CPU 負荷統計情報をクリアします。
internals	プロセス内部統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、高 CPU 負荷統計情報をクリアする例を示します。

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

関連コマンド

コマンド	説明
cpu hog granular-detection	リアルタイム高 CPU 負荷検出情報をトリガーします。
show processes	ASA で動作しているプロセスのリストを表示します。

clear resource usage

リソース使用状況の統計情報をクリアするには、特権 EXEC モードで **clear resource usage** コマンドを使用します。

```
clear resource usage [context context_name | all | summary | system] [resource {[rate]
resource_name | all}]
```

構文の説明

context <i>context_name</i>	(マルチ モードのみ) 統計情報をクリアするコンテキスト名を指定します。すべてのコンテキストを対象にする場合は、 all (デフォルト) を指定します。
resource [rate] <i>resource_name</i>	<p>特定のリソースの使用状況をクリアします。すべてのリソースを対象にするには、all (デフォルト) を指定します。リソース使用状況のレートをクリアする場合は、rate を指定します。比率で測定されるリソースには、conns、inspects、および syslogs があります。これらのリソース タイプを指定する場合は、rate キーワードを指定する必要があります。</p> <p>conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、rate キーワードのみを使用します。</p> <p>リソースには、次のタイプがあります。</p> <ul style="list-style-type: none"> • asdm: ASDM 管理セッション。 • conns: 1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • inspects: アプリケーション インспекション。 • hosts: ASA を通じて接続可能なホスト。 • mac-addresses: トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • ssh: SSH セッション。 • syslogs: syslogs メッセージ。 • telnet: Telnet セッション。 • (マルチ モードのみ) VPN Other: サイト間 VPN セッション。 • (マルチ モードのみ) VPN Burst Other: サイト間 VPN バーストセッション。 • xlates: NAT 変換。
summary	(マルチ モードのみ) 結合されたコンテキスト統計情報をクリアします。
system	(マルチ モードのみ) システム全体 (グローバル) の使用状況の統計情報をクリアします。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** で、これにより、すべてのコンテキストのリソース使用状況がクリアされます。シングル モードの場合、コンテキスト名は無視され、すべてのリソース統計情報がクリアされます。

デフォルトのリソース名は **all** で、これにより、すべてのリソース タイプがクリアされます。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、すべてのコンテキストの、すべてのリソース使用状況の統計情報(システム全体の使用状況の統計情報は除く)をクリアする例を示します。

```
ciscoasa# clear resource usage
```

次に、システム全体の使用状況の統計情報をクリアする例を示します。

```
ciscoasa# clear resource usage system
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	ASA のリソース使用状況を表示します。

clear route all

ダイナミックに学習されたルートをコンフィギュレーションから削除するには、特権 EXEC モードで **clear route all** コマンドを使用します。

clear route all

デフォルト デフォルトの動作や値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴	リリース	変更内容
	9.2(1)	このコマンドが追加されました。

使用上のガイドライン 欠落したルートを回復するには、**clear route all** コマンドを使用します。このコマンドを実行すると、グローバル RIB からのすべてのルートが削除されます。すべてのルート(ダイナミックまたはスタティック)がそれぞれのモジュール(プロトコル)によってグローバル RIB にプッシュされます。

一方、最適なルートがグローバル RIB にインストールされている場合は、同じルートがピアと NP テーブルに再配布されます。このプロセスは、複数のスレッドで順番に実行されます。このサイクルが完了するまでにかかる時間は、グローバル RIB のルートの数によって異なります。

したがって、**clear route all** コマンドを連続して使用する場合は、最小時間間隔を 30 秒、最大時間間隔を 120 秒にしてください。推奨される時間間隔に従わずにこのコマンドを複数回実行すると、配布されたルートが削除され、RIB からのルートが失われる可能性があります。

例 次に、ダイナミックに学習されたルートを削除する例を示します。

```
ciscoasa# clear route all
```

関連コマンド	コマンド	説明
	clear route network <mask>	指定された宛先ルートを除外します。
	show route	ルート情報を表示します。
	show running-config route	設定されているルートを表示します。

clear route management-only

指定された宛先ルートを削除するには、特権 EXEC モードで **clear route network <mask>** コマンドを使用します。管理専用キーワードによって IPv4 管理ルーティングテーブルのみがクリアされます。

clear route management-only [ip_address ip_mask]

構文の説明

<i>ip_address</i>	除外する宛先 IP アドレスおよびサブネット マスクを指定します。
<i>ip_mask</i>	
management-only	IPv4 管理ルーティング テーブルをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.5(1)	管理 VRF インターフェイスのサポートが追加されました。

例

次に、ダイナミックに学習されたルートを削除する例を示します。

```
ciscoasa# clear route 10.118.86.3
```

関連コマンド

コマンド	説明
clear route all	すべてのルートを除外し、リフレッシュします。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの動作データまたは統計情報(存在する場合)をクリアするには、特権 EXEC モードで **clear service-policy** コマンドを使用します。

clear service-policy [*global* | *interface intf*] [*user-statistics*]

構文の説明

global	(任意) グローバル サービス ポリシーの統計情報をクリアします。
interface <i>intf</i>	(任意) 特定のインターフェイスのサービス ポリシーの統計情報をクリアします。
user-statistics	<p>(オプション) ユーザ統計情報のグローバル カウンタはクリアしますが、ユーザごとの統計情報はクリアしません。ユーザごとまたはユーザ グループごとの統計情報は、show user-identity statistics コマンドを使用して引き続き確認できます。</p> <p>user-statistics コマンドに accounting キーワードを指定すると、送信パケット、受信パケット、および送信ドロップ パケットのすべてのグローバル カウンタがクリアされます。user-statistics コマンドに scanning キーワードを指定すると、送信ドロップ パケットのグローバル カウンタがクリアされます。</p> <p>ASA でこれらのユーザ統計情報を収集するには、ユーザ統計情報を収集するようにポリシー マップを設定する必要があります。このガイドの user-statistics コマンドを参照してください。</p>

デフォルト

デフォルトでは、このコマンドは、すべてのイネーブルなサービス ポリシーのすべての統計情報をクリアします。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

一部のインスペクション エンジンでは、統計情報を選択してクリアできます。**clear service-policy inspect** コマンドを参照してください。

例

次に、外部インターフェイスのサービス ポリシー統計情報をクリアする方法の例を示します。

```
ciscoasa# clear service-policy interface outside
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	GTP インспекション エンジンのサービス ポリシーの統計情報をクリアします。
clear service-policy inspect radius-accounting	RADIUS アカウンティング インспекション エンジンのサービス ポリシーの統計情報をクリアします。
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

GTP インспекション統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect gtp** コマンドを使用します。

```
clear service-policy inspect gtp {pdp-context {all | apn ap_name | imsi IMSI_value | ms-addr IP_address | tid tunnel_ID | version version_num} | requests [name | map name | version version_num] | statistics [gsn IP_address | IP_address]}
```

構文の説明。

<p>pdp-context {all apn ap_name imsi IMSI_value ms-addr IP_address tid tunnel_ID version version_num}</p>	<p>パケットデータプロトコル(PDP)またはベアラークontext情報をクリアします。次のキーワードを使用して、クリアするコンテキストを指定できます。</p> <ul style="list-style-type: none"> • all:すべてのコンテキストをクリアします。 • apn ap_name:指定されたアクセスポイントの名前のコンテキストをクリアします。 • imsi IMSI_value:指定された IMSI 16 進数のコンテキストをクリアします。 • ms-addr IP_address:指定されたモバイルサブスクライバ(MS)の IP アドレスのコンテキストをクリアします。 • tid tunnel_ID:指定された GTP トンネル ID(16 進数)のコンテキストをクリアします。 • version version_num:指定された GTP バージョン(0 ~ 255)のコンテキストをクリアします。
<p>requests [name map name version version_num]</p>	<p>GTP 要求をクリアします。次のパラメータを使用して、クリアする要求を任意で制限できます。</p> <ul style="list-style-type: none"> • name:指定された GTP インспекションポリシーマップに関連付けられている要求をクリアします。このオプションは、9.5(1)以降では使用できません。 • map name: (9.5(1)+)指定された GTP インспекションポリシーマップに関連付けられている要求をクリアします。 • version version_num: (9.5(1)+)指定された GTP バージョン(0 ~ 255)の要求をクリアします。
<p>statistics [gsn IP_address IP_address]</p>	<p>inspect gtp コマンドの GTP 統計情報をクリアします。</p> <p>gsn キーワードにエンドポイントのアドレスを指定すると、特定のエンドポイントの統計情報をクリアできます。9.5(1)以降はアドレスのみを指定し、gsn キーワードは含めないでください。</p>

デフォルト

デフォルトの動作や値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	次の点に変更されました。 <ul style="list-style-type: none"> • statistics オプションの gsn キーワードが削除されました。エンドポイントの統計情報をクリアするには、そのエンドポイントの IP アドレスのみを指定します。 • requests オプションに version キーワードが追加されました。requests オプションの後ろにマップ名を直接入力する機能に代わり、map キーワードがポリシー マップ名に追加されました。 • IPv6 アドレスのサポート。

使用上のガイドライン

GTP インспекションから統計情報をクリアするには、このコマンドを使用します。統計情報を表示するには、このコマンドの **show** バージョンを使用します。

例

次に、GTP 統計情報をクリアする例を示します。

```
ciscoasa# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
inspect gtp	GTP インспекションをイネーブルにします。
show service-policy inspect gtp	GTP 統計情報を表示します。

clear service-policy inspect m3ua

M3UA インスペクション統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect m3ua** コマンドを使用します。

```
clear service-policy inspect m3ua {drops | endpoint [ip_address] | session [assocID
hex_number]}
```

構文の説明

drops	M3UA ドロップの統計情報をクリアします。
endpoint [ip_address]	M3UA エンドポイントの統計情報をクリアします。必要に応じて、エンドポイントの IP アドレスを指定して、そのエンドポイントの統計情報のみをクリアできます。
session [assocID hex_number]	<p>厳密なアプリケーション サーバ プロセス (ASP) 状態検証をイネーブルにした場合に追跡される、すべての M3UA セッションをクリアします。</p> <p>特定のセクションをクリアするには、assocID キーワードと 16 進数のセッション番号を追加します。現在のセッションとそのアソシエーション ID を表示するには、show service-policy inspect m3ua session コマンドを使用します。</p>

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。
9.7(1)	session キーワードが追加されました。

使用上のガイドライン

M3UA インスペクションから統計情報またはセッションをクリアするには、このコマンドを使用します。統計情報とセッションを表示するには、このコマンドの **show** バージョンを使用します。

例

次に、M3UA エンドポイントの統計情報をクリアする例を示します。

```
ciscoasa# clear service-policy inspect m3ua endpoint
```

次に、特定の M3UA セッションをクリアする例を示します。

```
ciscoasa(config)# show service-policy inspect m3ua session
1 in use, 1 most used
Flags: d - double exchange      , s - single exchange
AssocID: c0bbe629 in Down state, idle:0:00:06, timeout:0:30:00, s
ciscoasa(config)# clear service-policy inspect m3ua session assocID c0bbe629
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インспекションをイネーブルにします。
show service-policy inspect m3ua	M3UA 統計情報を表示します。
strict-asp-state	厳密な M3UA ASP 状態検証をイネーブルにします。

clear service-policy inspect radius-accounting

RADIUS アカウンティング ユーザをクリアするには、特権 EXEC モードで **clear service-policy inspect radius-accounting** コマンドを使用します。

```
clear service-policy inspect radius-accounting users {all | ip_address | policy_map}
```

構文の説明

all	すべてのユーザをクリアします。
<i>ip_address</i>	この IP アドレスのユーザをクリアします。
<i>policy_map</i>	このポリシー マップに関連付けられているユーザをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、すべての RADIUS アカウンティング ユーザをクリアする例を示します。

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear session

コンフィギュレーション セッションの内容を削除したり、そのアクセス フラグをリセットしたりするには、グローバル コンフィギュレーション モードで **clear session** コマンドを使用します。

clear session *session_name* {**access** | **configuration**}

構文の説明

session_name	既存のコンフィギュレーション セッションの名前。現在のセッションのリストを表示するには、 show configuration session コマンドを使用します。
access	アクセス フラグをクリアします。このフラグは、セッションが編集モードであることを示します。編集セッションが破棄されたことを知っていて、変更を完了するにはセッションを開始する必要がある場合に限り、このフラグをクリアします。
configuration	セッションを削除することなく、セッション内で加えた設定変更をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL やその他のオブジェクトを編集するために隔離されたセッションを作成する、**configure session** コマンドとともに使用します。

このコマンドの主な用途は、アクセス フラグをリセットすることです。セッションを開くと、このフラグにより、セッションが編集モードであることが示されます。その後、セッションをクリーンに終了することなく ASA への接続を解除した場合、フラグは設定されたままになり、そのためにセッションを再度開くことができなくなることがあります。実際には誰もセッションを編集していないことが確実にわかっている場合は、フラグをリセットしてアクセスし直すことができます。

また、このコマンドを使用すると、セッションを削除しないで、変更のセッションを空にすることもできます。作成したセッションが不要になり、セッションで定義した変更をコミットしない場合は、**clear configuration session** コマンドを使用して、セッションおよびセッションに含まれている変更を削除します。

例

次に、my-session のアクセス フラグをリセットする例を示します。

```
ciscoasa(config)# clear session my-session access
```

関連コマンド

コマンド	説明
clear configuration session	コンフィギュレーション セッションとその内容を削除します。
configure session	セッションを作成するか、開きます。
show configuration session	現在の各セッションで行われた変更を表示します。

clear shared license

共有ライセンス統計情報、共有ライセンス クライアント統計情報、および共有ライセンス バックアップ サーバ統計情報を 0 にリセットするには、特権 EXEC モードで **clear shared license** コマンドを使用します。

clear shared license [**all** | **backup** | **client** [*hostname*]]

構文の説明

all	(任意)すべての統計情報をクリアします。これがデフォルト設定です。
backup	(任意)バックアップ サーバの統計情報をクリアします。
client	(任意)すべての参加ユニットの統計情報をクリアします。
<i>hostname</i>	(任意)特定の参加ユニットの統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

共有ライセンス カウンタには統計データとエラー データが含まれます。

例

次に、すべての共有ライセンス カウンタをリセットする例を示します。

```
ciscoasa# clear shared license all
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。

コマンド	説明
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

clear shun

現在イネーブルであるすべての shun をディセーブルにして、shun 統計情報をクリアするには、特権 EXEC モードで **clear shun** コマンドを使用します。

clear shun [*statistics*]

構文の説明

statistics (任意) インターフェイス カウンタだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、現在イネーブルになっているすべての shun をディセーブルにして、shun 統計情報をクリアする例を示します。

```
ciscoasa(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。
show shun	回避についての情報を表示します。

clear snmp-server statistics

SNMP サーバ統計情報(SNMP パケットの入力カウンタと出力カウンタ)をクリアするには、特権 EXEC モードで **clear snmp-server statistics** コマンドを使用します。

clear snmp-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルータッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP サーバ統計情報をクリアする例を示します。

```
ciscoasa# clear snmp-server statistics
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show snmp-server statistics	SNMP サーバ コンフィギュレーション情報を表示します。

clear ssl

デバッグ目的で SSL 情報をクリアするには、特権 EXEC モードで **clear ssl** コマンドを使用します。

```
clear ssl {cache [all] | errors | mib | objects}
```

構文の説明

<i>all</i>	SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアします。
<i>cache</i>	SSL セッション キャッシュ内の期限切れセッションをクリアします。
<i>errors</i>	ssl エラーをクリアします。
<i>mib</i>	SSL MIB 統計情報をクリアします。
<i>objects</i>	SSL オブジェクト統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

AnyConnect 機能に影響するため、DTLS キャッシュがクリアされることはありません。

例

次に、SSL キャッシュをクリアし、SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアする例を示します。

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DTLS caches are not cleared

ciscoasa# clear ssl cache all
```

```
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

メモリからコンフィギュレーション エラー メッセージをクリアするには、特権 EXEC モードで **clear startup-config errors** コマンドを使用します。

clear startup-config errors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示するには、**show startup-config errors** コマンドを使用します。

例

次に、メモリからすべてのコンフィギュレーション エラーをクリアする例を示します。

```
ciscoasa# clear startup-config errors
```

関連コマンド

コマンド	説明
show startup-config errors	ASA がスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示します。

clear sunrpc-server active

Sun RPC アプリケーション インспекションによって開けられたピンホールをクリアするには、特権 EXEC モードで **clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

デフォルト デフォルトの動作や値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。

使用上のガイドライン Sun RPC アプリケーション インспекションによって開けられた、NFS や NIS などのサービストラフィックが ASA を通過できるようにするピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

例 次に、SunRPC サービス テーブルをクリアする例を示します。

```
ciscoasa# clear sunrpc-server
```

関連コマンド	コマンド	説明
	clear configure sunrpc-server	ASA からの Sun リモートプロセッサ コール サービスをクリアします。
	inspect sunrpc	Sun RPC アプリケーション インспекションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
	show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。
	show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear terminal

現在の CLI セッションの端末設定をクリアして、デフォルトを使用するには、特権 EXEC モードで **clear terminal** コマンドを使用します。

```
clear terminal {interactive | pager [[lines] number]}
```

構文の説明

interactive	インタラクティブなヘルプの設定をクリアします(CLIで?を入力したときの)。デフォルトではイネーブルになっています。
pager [[lines] number]	「---more---」プロンプトが表示されるまでの1ページあたりの行数の設定をクリアします。デフォルトは24です。

コマンドデフォルト

デフォルトの端末動作は次のとおりです。

- **interactive**: 有効
- **pager**: 24 回線

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ポケットベルの設定をクリアする例を示します。

```
ciscoasa# clear terminal pager
```

関連コマンド

コマンド	説明
terminal pager	「---More---」プロンプトが表示されるまでの1ページあたりの行数を設定します。
terminal interactive	CLIに?と入力した場合にヘルプをイネーブルまたはディセーブルにします。

clear threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにしたときに統計情報をクリアするには、特権 EXEC モードで **clear threat detection rate** コマンドを使用します。

clear threat-detection rate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルールセット	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、レート統計情報をクリアする例を示します。

```
ciscoasa# clear threat-detection rate
```

関連コマンド

コマンド	説明
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベントタイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用して脅威検出のスキャンをイネーブルにした後で攻撃者と攻撃対象をクリアするには、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用します。

```
clear threat-detection scanning-threat [attacker [ip_address [mask]]] |
target [ip_address [mask]]
```

構文の説明

attacker	(任意) 攻撃者だけをクリアします。
<i>ip_address</i>	(オプション) 特定の IP アドレスをクリアします。
<i>mask</i>	(任意) サブネット マスクを設定します。
target	(任意) 攻撃対象だけをクリアします。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

現在の攻撃者および攻撃対象を表示するには、**show threat-detection scanning-threat** コマンドを使用します。

例

次に、**show threat-detection scanning-threat** コマンドで攻撃対象と攻撃者を表示し、次にすべての攻撃対象をクリアする例を示します。

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
  192.168.1.0
  192.168.1.249
Latest Attacker Host & Subnet List:
  192.168.10.234
  192.168.10.0
  192.168.10.2
  192.168.10.3
```

```

192.168.10.4
192.168.10.5
192.168.10.6
192.168.10.7
192.168.10.8
192.168.10.9
ciscoasa# clear threat-detection scanning-threat target

```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection shun

threat-detection scanning-threat コマンドを使用して脅威検出のスキャンをイネーブルにし、さらに攻撃元ホストの自動回避もイネーブルにした後で、現在回避されているホストを解放するには、特権 EXEC モードで **clear threat-detection shun** コマンドを使用します。

```
clear threat-detection shun [ip_address [mask]]
```

構文の説明

<i>ip_address</i>	(任意)特定の IP アドレスの回避を解除します。
<i>mask</i>	(任意)回避されているホストの IP アドレスのサブネット マスクを設定します。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

現在回避されているホストを表示するには、**show threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドで現在回避されているホストを表示し、ホスト 10.1.1.6 を回避状態から解放する例を示します。

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection statistics

threat-detection statistics tcp-intercept コマンドを使用して TCP 代行受信の統計情報をイネーブ
ルにした後で統計情報をクリアするには、特権 EXEC モードで **clear threat-detection**
scanning-threat コマンドを使用します。

clear threat-detection statistics [tcp-intercept]

構文の説明

tcp-intercept (任意)TCP 代行受信の統計情報をクリアします。

デフォルト

TCP 代行受信の統計情報をクリアします。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドラ イン

TCP 代行受信の統計情報を表示するには、**show threat-detection statistics top** コマンドを入力し
ます。

例

次に、**show threat-detection statistics top tcp-intercept** コマンドで TCP 代行受信の統計情報を表
示し、次にすべての統計情報をクリアする例を示します。

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
-----
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
```

```
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)

ciscoasa# clear threat-detection statistics
```

関連コマンド

コマンド	説明
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威の検出の統計情報をイネーブルにします。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、特権 EXEC モードで **clear traffic** コマンドを使用します。

clear traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear traffic コマンドは、**show traffic** コマンドで表示される送信アクティビティと受信アクティビティのカウンタをリセットします。これらのカウンタは、最後に **clear traffic** コマンドが入力されてから、または ASA がオンラインになってからの、各インターフェイスを通過したパケット数およびバイト数を示します。また、秒数は、ASA が最後にレポートされてからオンラインである継続時間を示します。

例

次に、**clear traffic** コマンドの例を示します。

```
ciscoasa# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのキャッシュされた認証および認可情報をすべて削除するには、特権 EXEC モードで **clear uauth** コマンドを使用します。

clear uauth [username]

構文の説明

username (オプション)削除するユーザ認証情報をユーザ名で指定します。

デフォルト

username 引数を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear uauth コマンドは、1 人のユーザまたはすべてのユーザの AAA 認可および認証のキャッシュを削除します。これにより、これらのユーザは、次回接続を作成するときに、再認証を強制されるようになります。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、ASA ではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません(イメージが同じ IP アドレスからであると想定されます)。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。



(注)

Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル (`show uauth` コマンドで表示できます) に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPsec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウントिंग サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、`timeout uauth` コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、`clear uauth` コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザの再認証を実行する例を示します。

```
ciscoasa(config)# clear uauth user
```

関連コマンド

コマンド	説明
<code>aaa authentication</code>	<code>aaa-server</code> コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
<code>aaa authorization</code>	<code>aaa-server</code> コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
<code>show uauth</code>	現在のユーザの認証情報と認可情報を表示します。
<code>timeout</code>	アイドル時間の最大継続期間を設定します。

clear uc-ime

Cisco Intercompany Media Engine プロキシに関する統計情報を表示するために使用されるカウンタをクリアするには、特権 EXEC モードで **clear uc-ime** コマンドを使用します。

clear uc-ime [[**mapping-service-sessions** | **signaling-sessions** | **fallback-notification**] **statistics**]

構文の説明

fallback-notification	(任意)フォールバック通知の統計情報のカウンタをクリアします。
mapping-service-sessions	(任意)マッピング サービス セッションの統計情報のカウンタをクリアします。
signaling-sessions	(任意)シグナリング セッションの統計情報のカウンタをクリアします。
statistics	(任意)クリアする Cisco Intercompany Media Engine プロキシのカウンタを設定するキーワードです。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルールテッド	トランス アレント	シングル	マルチ	
				コンテ キ スト	システ ム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

例

次に、シグナリング セッションの統計情報を表示するために使用されるカウンタをクリアする例を示します。

```
ciscoasa# clear configure signaling-sessions statistics
```

関連コマンド

コマンド	説明
clear configure uc-ime	ASA 上の Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションをクリアします。
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。

コマンド	説明
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

clear url-block block statistics

ブロック バッファ使用状況カウンタをクリアするには、特権 EXEC モードで **clear url-block block statistics** コマンドを使用します。

clear url-block block statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドラ イン

clear url-block block statistics コマンドは、ブロック バッファ使用状況カウンタ (Current number of packets held (global) カウンタは除く) をクリアします。

例

次に、URL ブロック統計情報をクリアし、クリア後のカウンタのステータスを表示する例を示します。

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block 0
-----
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバ応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド ステートメントを削除するには、特権 EXEC モードで **clear url-cache** コマンドを使用します。

clear url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから URL キャッシュ統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコルバージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコルバージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。目的のセキュリティ要求を満たす使用状況プロファイルを取得したら **url-cache** コマンドを入力してスループットを増大させます。Websense プロトコルバージョン 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、URL キャッシュ統計情報をクリアする例を示します。

```
ciscoasa# clear url-cache statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報をクリアするには、特権 EXEC モードで **clear url-server** コマンドを使用します。

clear url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーフッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次に、URL サーバの統計情報をクリアする例を示します。

```
ciscoasa# clear url-server statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。

コマンド	説明
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear user-identity active-user-database

アイデンティティ ファイアウォールのために特定のユーザのステータスをログアウトに設定するには、特権 EXEC モードで **clear user-identity active-user-database** コマンドを使用します。

```
clear user-identity active-user-database [user [domain_nickname\]use_rname] | user-group [domain_nickname\]user_group_name
```

構文の説明

<i>domain_nickname\user_group_name</i>	統計情報をクリアする対象のユーザ グループを指定します。 <i>group_name</i> には、[a-z]、[A-Z]、[0-9]、[!@#%&()-_{}.] など、あらゆる文字を使用できます。 <i>domain_NetBIOS_name\group_name</i> にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
<i>domain_nickname\use_rname</i>	統計情報をクリアする対象のユーザを指定します。 <i>user_name</i> には、[a-z]、[A-Z]、[0-9]、[!@#%&()-_{}.] など、あらゆる文字を使用できます。 <i>domain_NetBIOS_name\user_name</i> にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
user	ユーザの統計情報をクリアすることを指定します。
user-group	ユーザ グループの統計情報をクリアすることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスパレント	シングル	マルチ コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、指定したユーザ、指定したユーザ グループに属するすべてのユーザ、またはすべてのユーザのステータスをログアウトに設定します。

user-group キーワードを指定すると、指定したユーザ グループに属するすべてのユーザのステータスがログアウトに設定されます。**user-group** キーワードとともに *domain_nickname* 引数を指定しない場合、デフォルト ドメイン内の *user_group_name* というグループに属するユーザのステータスがログアウトに設定されます。

user キーワードを指定すると、指定したユーザのステータスがログアウトに設定されます。**user** キーワードとともに *domain_nickname* 引数を指定しない場合、デフォルト ドメイン内の *user_name* というユーザのステータスがログアウトに設定されます。

user キーワードも **user-group** キーワードも指定しない場合、すべてのユーザのステータスがログアウトに設定されます。

例

次に、SAMPLE ドメインのユーザ グループ **users1** に属するすべてのユーザのステータスをログアウトに設定する例を示します。

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティファイアウォール機能の設定をクリアします。
show user-identity user active	アイデンティティファイアウォールのアクティブ ユーザを表示します。

clear user-identity ad-agent statistics

アイデンティティ ファイアウォールの AD エージェント統計情報をクリアするには、特権 EXEC モードで **clear user-identity ad-agent statistics** コマンドを使用します。

clear user-identity ad-agent statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報を保持します。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

AD エージェントの統計データをクリアするには、**clear user-identity ad-agent statistics** コマンドを使用します。

例

次に、アイデンティティ ファイアウォールの AD エージェント統計情報をクリアする例を示します。

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics
```

```
Primary AD Agent          Total  Last Activity
-----
Input packets:           0  N/A
Output packets:         0  N/A
Send updates:           0  N/A
```

```

Recv updates:                0  N/A
Keepalive failed:            0  N/A
Send update failed:          0  N/A
Query failed:                 0  N/A

```

```

Secondary AD Agent           Total  Last Activity
-----
Input packets:               0  N/A
Output packets:              0  N/A
Send updates:                 0  N/A
Recv updates:                 0  N/A
Keepalive failed:            0  N/A
Send update failed:          0  N/A
Query failed:                 0  N/A

```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティファイアウォール機能の設定をクリアします。
show user-identity ad-agent [statistics]	アイデンティティファイアウォールの AD エージェントに関する統計情報を表示します。

clear user-identity statistics

アイデンティティ ファイアウォールに関する統計情報を表示するために使用されるカウンタをクリアするには、特権 EXEC モードで **clear user-identity statistics** コマンドを使用します。

clear user-identity statistics [**user** *domain_nickname\use_rname*] | **user-group** *domain_nickname\user_group_name*]

構文の説明

<i>domain_nickname\user_group_name</i>	統計情報をクリアする対象のユーザ グループを指定します。 <i>group_name</i> には、[a-z]、[A-Z]、[0-9]、[!@#%&()-_{}.] など、あらゆる文字を使用できます。 <i>domain_NetBIOS_name\group_name</i> にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
<i>domain_nickname\use_rname</i>	統計情報をクリアする対象のユーザを指定します。 <i>user_name</i> には、[a-z]、[A-Z]、[0-9]、[!@#%&()-_{}.] など、あらゆる文字を使用できます。 <i>domain_NetBIOS_name\user_name</i> にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
user	ユーザの統計情報をクリアすることを指定します。
user-group	ユーザ グループの統計情報をクリアすることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

domain_nickname が *user_group_name* よりも前に指定されていない場合、ASA はデフォルトドメイン内の *user_group_name* というグループのアイデンティティファイアウォール統計情報を削除します。

domain_nickname が *user_name* よりも前に指定されていない場合、ASA はデフォルトドメイン内の *user_name* というユーザのアイデンティティファイアウォール統計情報を削除します。

例

次に、ユーザグループの統計情報を表示するために使用されるカウンタをクリアする例を示します。

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティファイアウォール機能の設定をクリアします。
show user-identity statistics	アイデンティティファイアウォールのユーザまたはユーザグループの統計情報を表示します。

clear user-identity user-not-found

アイデンティティ ファイアウォールの ASA ローカル user-not-found データベースをクリアするには、特権 EXEC モードで **clear user-identity user-not-found** コマンドを使用します。

clear user-identity user-not-found

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Microsoft Active Directory で見つからない IP アドレスのローカル user-not-found データベースを保持します。ASA は、データベースのリスト全体ではなく、user-not-found リストの最後の 1024 パケットのみを保持します(同じ送信元 IP アドレスからの連続するパケットは 1 つのパケットとして扱われます)。

ASA 上のローカル データベースをクリアするには、**clear user-identity user-not-found** コマンドを使用します。



ヒント

Microsoft Active Directory で見つからないユーザの IP アドレスを表示するには、**show user-identity user-not-found** コマンドを使用します。

例

次に、アイデンティティ ファイアウォールのローカル user-not-found データベースをクリアする例を示します。

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティファイアウォール機能の設定をクリアします。
show user-identity user-not-found	ASA user-not-found データベースで見つからない Active Directory ユーザの IP アドレスを表示します。

clear user-identity user no-policy-activated

アイデンティティ ファイアウォール用にアクティブ化されていないユーザの ASA でローカルレコードをクリアするには、特権 EXEC モードで **clear user-identity user no-policy-activated** コマンドを使用します。

clear user-identity user no-policy-activated

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルールテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

どのセキュリティ ポリシーでもアクティブ化されていないユーザ、つまり、アクティブ化されたユーザ グループに属していないか、アクセス リストまたはサービス ポリシー コンフィギュレーションで参照されていないユーザのローカル レコードをクリアするには、**clear user-identity user no-policy-activated** を使用します。

また、**clear user-identity user no-policy-activated** コマンドは、アクティブであるもののまだアクティブ化されていないユーザの IP アドレスもクリアします。

アイデンティティ ファイアウォールのユーザ グループを作成する場合、そのグループをアクティブ化する必要があります。つまり、グループはインポート ユーザ グループ(アクセス リストまたはサービス ポリシー コンフィギュレーションでユーザ グループとして定義)またはローカル ユーザ グループ(オブジェクト グループ ユーザで定義)です。

例

次に、アクティブ化されていないユーザの ASA 上でローカル レコードをクリアする例を示します。

```
ciscoasa# clear user-identity user no-policy-activated
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティファイアウォール機能の設定をクリアします。
show user-identity group	アイデンティティファイアウォールのアクティブ化されたユーザグループのリストを表示します。

clear vpn cluster stats internal

VPN クラスタリングの内部カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで次のコマンドを使用します。

clear vpn cluster stats internal

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
グローバル コンフィギュレー ション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

関連コマンド

コマンド	説明
show vpn cluster stats internal	すべての VPN クラスタ カウンタを表示します。

clear vpn-sessiondb statistics

すべての統計情報、特定のセッション、特定のプロトコルなど VPN セッションに関する情報をクリアするには、特権 EXEC モードで **clear vpn-sessiondb statistics** コマンドを使用します。

```
clear vpn-sessiondb {all | anyconnect | failover | email-proxy | global | index index_number |
  ipaddress IPAddr | l2l | name username | protocol protocol | ra-ikev1-ipsec | ra-ikev2-ipsec |
  tunnel-group name | vpn-lb | webvpn}
```

構文の説明

all	すべてのセッションの統計情報をクリアします。
anyconnect	AnyConnect VPN クライアントセッションの統計情報をクリアします。
failover	フェールオーバー IPsec セッションの統計情報をクリアします。
email-proxy	(廃止)電子メールプロキシセッションの統計情報をクリアします。
global	グローバルセッションデータの統計情報をクリアします。
index <i>indexnumber</i>	インデックス番号を指定して単一のセッションの統計情報をクリアします。 show vpn-sessiondb detail コマンドの出力には、セッションごとにインデックス番号が表示されます。
ipaddress <i>IPAddr</i>	指定した IP アドレスのセッションの統計情報をクリアします。
l2l	VPN LAN-to-LAN セッションの統計情報をクリアします。
protocol <i>protocol</i>	次のプロトコルの統計情報をクリアします。 <ul style="list-style-type: none"> ikev1:IKEv1 プロトコルを使用したセッション。 ikev2:IKEv2 プロトコルを使用したセッション。 ipsec:IKEv1 または IKEv2 を使用した IPsec セッション。 ipseclan2lan:IPsec LAN-to-LAN セッション。 ipseclan2lanovernatt:IPsec LAN-to-LAN over NAT-T セッション。 ipsecovernatt:IPsec over NAT-T セッション。 ipsecovertcp:IPsec over TCP セッション。 ipsecoverudp:IPsec over UDP セッション。 l2tpOverIpSec:L2TP over IPsec セッション。 l2tpOverIpsecOverNatT:NAT-T を介した L2TP over IPsec セッション。 ospfv3:OSPFv3 over IPsec セッション。 webvpn:クライアントレス SSL VPN セッション。 imap4s:IMAP4 セッション。 pop3s:POP3 セッション。 smtps:SMTP セッション。 anyconnectParent:セッションに使用されるプロトコルに関係なく、AnyConnect クライアントセッション(AnyConnect IPsec IKEv2 セッションおよび SSL セッションを終了します)。 ssltunnel:SSL を使用した AnyConnect セッションやクライアントレス SSL VPN セッションを含めた、SSL VPN セッション。 dtlstunnel:DTLS がイネーブルになっている AnyConnect クライアントセッション。

ra-ikev1-ipsec	IPsec IKEv1 セッションおよび L2TP セッションに関する統計情報をクリアします。
ra-ikev2-ipsec	IPsec IKEv2 セッションの統計情報をクリアします。
tunnel-group groupname	指定したトンネルグループ(接続プロファイル)のセッションの統計情報をクリアします。
vpn-lb	VPN ロードバランシング管理セッションの統計情報をクリアします。
webvpn	クライアントレス SSL VPN セッションの統計情報をクリアします。

デフォルト デフォルトの動作や値はありません。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランス アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴	リリース	変更内容
	8.4(1)	このコマンドが追加されました。
	9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
	9.3(2)	ra-ikev2-ipsec キーワードが追加されました。
	9.8(1)	email-proxy オプションが廃止されました。

clear wccp

WCCP 情報をリセットするには、特権 EXEC モードで **clear wccp** コマンドを使用します。

clear wccp [**web-cache** | *service_number*]

構文の説明

web-cache	Web キャッシュ サービスを指定します。
<i>service-number</i>	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ~ 255 の範囲で指定できます。 web-cache キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、Web キャッシュ サービスの WCCP 情報をリセットする例を示します。

```
ciscoasa# clear wccp web-cache
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear webvpn sso-server statistics

WebVPN シングル サインオン (SSO) サーバの統計情報をリセットするには、特権 EXEC モードで **clear webvpn sso-server statistics** コマンドを使用します。

clear webvpn sso-server statistics *servername*

構文の説明

servername リセットする SSO サーバの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスぺアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、「保留要求」の統計情報をリセットしません。

例

次に、暗号アクセラレータ統計情報を表示する例を示します。

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear xlate

現在のダイナミック変換および接続情報をクリアするには、特権 EXEC モードで **clear xlate** コマンドを使用します。

```
clear xlate [global ip1[-ip2] [netmask mask]] [local ip1[-ip2] [netmask mask]]
           [gport port1[-port2]] [lport port1[-port2]] [interface if_name] [state state]
```

構文の説明

global ip1[-ip2]	(任意)グローバル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
gport port1[-port2]	(任意)グローバル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
interface if_name	(任意)アクティブな変換をインターフェイス別に表示します。
local ip1[-ip2]	(任意)ローカル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
lport port1[-port2]	(任意)ローカル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
netmask mask	(任意)グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state state	(任意)状態を指定して、アクティブな変換をクリアします。次の 1 つ以上の状態を入力できます。 <ul style="list-style-type: none"> • static: スタティック変換を指定します。 • portmap: PAT グローバル変換を指定します。 • norandomseq: norandomseq 設定での nat またはスタティック変換を指定します。 • identity: nat 0 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ってください。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ コンテキ スト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容をクリアします(「xlate」は変換スロットを意味します)。変換スロットは、キーの変更が行われた後でも存続できます。**clear xlate** コマンドは、コンフィギュレーション内の **global** コマンドまたは **nat** コマンドを追加、変更、または削除した後に必ず使用してください。

xlate は、NAT または PAT セッションについて記述します。これらのセッションは、**detail** オプションを指定した **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックという 2 つのタイプがあります。

スタティック xlate は、**static** コマンドを使用して作成される永続的な xlate です。**clear xlate** コマンドは、スタティック エントリ内のホストをクリアしません。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** コマンドは、スタティック変換ルールを削除しません。コンフィギュレーションから **static** コマンドを削除しても、スタティック ルールを使用する既存の接続はトラフィックを引き続き転送できます。これらの接続を無効にするには、**clear local-host** コマンドまたは **clear conn** コマンドを使用します。

ダイナミック xlate は、**nat** コマンドまたは **global** コマンドを介したトラフィック処理が必要に応じて作成される xlate です。**clear xlate** コマンドを実行すると、ダイナミック xlate および関連付けられた接続が削除されます。また、**clear local-host** コマンドまたは **clear conn** コマンドを使用して、xlate および関連する接続をクリアすることもできます。コンフィギュレーションから **nat** コマンドまたは **global** コマンドを削除した場合、ダイナミック xlate および関連する接続がアクティブのまま残る場合があります。これらの接続を削除するには、**clear xlate** コマンドを使用します。

例

次に、現在の変換および接続スロット情報をクリアする例を示します。

```
ciscoasa# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報をクリアします。
clear uauth	キャッシュされたユーザ認証および認可情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。

