CHAPTER 25

show asp drop コマンド～ show curpriv コマンド

show asp drop

アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

シンタックスの説明

flow [*flow_drop_reason*]	（オプション）ドロップされたフロー（接続）を表示します。*flow_drop_reason* 引数を使用して、特定の理由を指定できます。*flow_drop_reason* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
frame [***frame_drop_reason***]	（オプション）ドロップされたパケットを表示します。*frame_drop_reason* 引数を使用して、特定の理由を指定できます。*frame_drop_reason* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	他のドロップ理由が追加されました。

使用上のガイドライン

show asp drop コマンドは、アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。この情報はデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

表 25-2 はドロップされたフローの *flow_drop_reason* 引数に有効な値を一覧表示しています。表 25-1 はドロップされたフレームの *frame_drop_reason* 引数に有効な値を一覧表示しています。

表 25-1　フレーム ドロップの理由

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
acl-drop	アクセス規則によってフローが拒否されます。	パケットがセキュリティ アプライアンスに拒否された場合、このカウンタが増分します。拒否規則は、セキュリティ アプライアンスの起動時、さまざまな機能がオンまたはオフにされたとき、アクセス リストがインターフェイスに適用されたとき、またはその他の機能で作成されたデフォルトの規則の可能性があります。デフォルトの規則のドロップを除き、フローが拒否される理由は次のとおりです。 • インターフェイス上にアクセス リストが設定されている。 • アクセス リストが AAA 用に設定されていて、AAA がユーザを拒否した。 • トラフィックを通過して管理専用インターフェイスに到達した。 • IPSec がイネーブルになっているインターフェイスに、暗号化されていないトラフィックが到達した。 **推奨事項**：次のシステム ログ メッセージが参照するアクセス リストをチェックします。 **システム ログ メッセージ**：106023、106100、106004
bad-crypto	不良暗号がパケットで戻ります。	セキュリティ アプライアンスがパケットの暗号化を試みましたが、暗号化が失敗した場合、このカウンタが増分します。これは正常な状態ではなく、セキュリティ アプライアンスに関するソフトウェアまたはハードウェアに問題がある可能性を示しています。 **推奨事項**：不良暗号の表示を何度も受信する場合は、セキュリティ アプライアンスの点検が必要である可能性があります。システム メッセージ 402123 をイネーブルにして、暗号不良がハードウェアのエラーなのかソフトウェアのエラーなのかを判断してください。また、**show ipsec stats** コマンドを使用して、グローバル IPSec 統計情報にあるエラー カウンタをチェックしてください。これらのエラーを引き起こす IPSec SA が既知である場合は、**show ipsec sa detail** コマンドから出力される SA 統計情報も問題の診断に役立ちます。 **システム ログ メッセージ**：402123

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
bad-ipsec-natt	不良 IPSEC NATT パケット。	セキュリティ アプライアンスが IPSec 接続上で NAT-T とネゴシエートしたパケットを受信したが、パケットのアドレスが NAT-T UDP の宛先ポートである 4500 になっていない、またはパケットのペイロード長が無効である場合、このカウンタが増分します。 **推奨事項**：ネットワーク トラフィックを分析し、NAT-T トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。
bad-ipsec-prot	AH または ESP ではない IPSEC。	セキュリティ アプライアンスが IPSec 接続上で AH または ESP プロトコル パケットではないパケットを受信した場合、このカウンタが増分します。これは正常な状態ではありません。 **推奨事項**：AH または ESP ではない IPSec 表示が何度もセキュリティ アプライアンスに表示される場合は、ネットワーク トラフィックを分析し、トラフィックの送信元を特定します。 **システム ログ メッセージ**：402115
bad-ipsec-udp	不良 IPSEC UDP パケット。	セキュリティ アプライアンスが、IPSec over UDP とネゴシエート済みの IPSec 接続上でパケットを受信したが、このパケットのペイロード長が無効だった場合、このカウンタが増分します。 **推奨事項**：ネットワーク トラフィックを分析し、NAT-T トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。
bad-tcp-cksum	不良 TCP チェックサム。	セキュリティ アプライアンスが、算出された TCP チェックサムと TCP ヘッダーに記録されているチェックサムが一致しない TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。不適切な TCP チェックサムを持つパケットを許可するには、**checksum-verification** 機能をディセーブルにします。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
bad-tcp-flags	不良 TCP フラグ。	セキュリティ アプライアンスが、TCP ヘッダー内の TCP フラグが無効な TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。たとえば、SYN フラグと FIN TCP フラグの両方がセットされているパケットは、ドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
conn-limit	接続制限値に到達しました。	この理由は、接続制限値またはホスト接続制限値を超えたためにパケットがドロップされたことによるものです。このパケットが、接続制限値により TCP 接続設定フェーズ中にドロップされた TCP パケットの場合は、ドロップ理由「TCP connection limit reached（TCP 接続制限値に到達しました。）」も報告されます。 **推奨事項**：カウンタが急速に増分する場合は、システム メッセージをチェックし、どのホストが接続制限値に到達したのかを判断します。トラフィックが正常な場合、またはホストが攻撃を受けている場合は、接続制限値を増分する必要があることもあります。 **システム ログ メッセージ**：201011
ctm-error	CTM がエラーを返しました。	セキュリティ アプライアンスがパケットの暗号化を試みましたが、暗号化が失敗した場合、このカウンタが増分します。これは正常な状態ではなく、セキュリティ アプライアンスに関するソフトウェアまたはハードウェアに問題がある可能性を示しています。 **推奨事項**：不良暗号の表示を何度も受信する場合は、セキュリティ アプライアンスの点検が必要である可能性があります。システム メッセージ 402123 をイネーブルにして、暗号不良がハードウェアのエラーなのかソフトウェアのエラーなのかを判断してください。また、**show ipsec stats** コマンドを使用して、グローバル IPSec 統計情報にあるエラー カウンタをチェックしてください。これらのエラーを引き起こす IPSec SA が既知である場合は、**show ipsec sa detail** コマンドから出力される SA 統計情報も問題の診断に役立ちます。 **システム ログ メッセージ**：402123

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
dns-guard-id-not-matched	DNS Guard id が一致しません。	DNS 応答メッセージの ID が、同じ接続上で先にセキュリティ アプライアンスを通過した DNS クエリーのいずれにも一致しなかった場合、このカウンタが増分します。このカウンタは、DNS Guard 機能により増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：なし。
dns-guard-out-of-app-id	app id 以外の DNS Guard。	DNS Guard 機能が DNS メッセージの ID を保存するためのデータ構造の割り当てに失敗した場合、このカウンタが増分します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
dst-l2_lookup-fail	Dst MAC L2 検索が失敗しました。	セキュリティ アプライアンスが透過モードに設定され、セキュリティ アプライアンスがレイヤ 2 の宛先 MAC アドレスの検索に失敗した場合、このカウンタが増分します。検索に失敗すると、セキュリティ アプライアンスは宛先 MAC 探索プロセスを開始し、ARP/ICMP メッセージからホストの場所を探そうとします。 **推奨事項**：セキュリティ アプライアンスが透過モードに設定されている場合、これは正常な状態です。**show mac-address-table** コマンドを実行して、現在セキュリティ アプライアンスによって検出されているレイヤ 2 MAC アドレスの場所をリストすることもできます。 **システム ログ メッセージ**：なし。
flow-expired	期限切れのフロー。	セキュリティ アプライアンスが新しいパケットまたはキャッシュされたパケットを投入しようとしたが、そのパケットがすでに期限切れのフローに属している場合、このカウンタが増分します。また、セキュリティ アプライアンスがすでに期限切れの TCP フロー上で RST を送信しようとした場合、または AIP SSM からパケットが返されてもそのフローがすでに期限切れの場合にも増分します。このパケットはドロップされます。 **推奨事項**：有効なアプリケーションが優先されている場合、タイムアウトを増分する必要があるかどうか調べます。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
fo-standby	スタンバイ装置によってドロップされました。	スタンバイ状態のセキュリティ アプライアンスまたはコンテキストに through-the-box パケットが届き、フローが作成されると、そのパケットはドロップされ、作成されたフローは削除されます。パケットがこの方法でドロップされるたびに、このカウンタが増分します。 **推奨事項**：アクティブなセキュリティ アプライアンスまたはコンテキスト上では、このカウンタが増分することはありません。ただし、スタンバイ アプライアンスまたはセキュリティ アプライアンス上では、増分するのが普通です。 **システム ログ メッセージ**：302014、302016、302018
fragment-reassembly-failed	フラグメントの再構成が失敗しました。	このカウンタは、セキュリティ アプライアンスが一連の断片化されたパケットを 1 つのパケットに再構成できなかった場合に増分します。一連のフラグメント パケットはすべてドロップされます。これは、再構成されたパケットにメモリを配分中にエラーが発生したことが原因であると考えられます。 **推奨事項**：**show blocks** コマンドを使用して、現在のブロック メモリを監視します。 **システム ログ メッセージ**：なし。
host-move-pkt	FP ホスト移動パケット。	セキュリティ アプライアンスまたはコンテキストが透過モードに設定されていて、既知のレイヤ 2 MAC アドレスの発信元インターフェイスが異なるインターフェイス上で検出された場合、このカウンタが増分します。 **推奨事項**：これは、ホストがあるインターフェイス（たとえば LAN セグメント）から別のインターフェイスに移動したことを示しています。実際にホストが移動している場合、透過モードではこれは正常な状態です。ただし、ホストがインターフェイス間であちこち移動する場合は、ネットワーク ループが存在している可能性があります。 **システム ログ メッセージ**：412001、412002、322001
ifc-classify	仮想ファイアウォール分類が失敗しました。	パケットが共有インターフェイスに到着しましたが、特定のコンテキスト インターフェイスへの分類が失敗しました。 **推奨事項**：**global** コマンドまたは **static** コマンドを使用して、各コンテキスト インターフェイスに属している IPv4 アドレスを指定します。 **システム ログ メッセージ**：なし。
inspect-dns-id-not-matched	DNS Inspect id が一致しません。	DNS 応答メッセージの ID が、同じ接続上で先にセキュリティ アプライアンスを通過した DNS クエリーのいずれにも一致しなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-dns-invalid-domain-label	DNS Inspect 無効ドメイン ラベル。	セキュリティ アプライアンスが無効な DNS ドメイン名またはラベルを検出した場合、このカウンタが増分します。DNS ドメイン名とラベルのチェックは、RFC 1035 ごとに行われます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-dns-invalid-pak	DNS Inspect 無効パケット。	セキュリティ アプライアンスが無効な DNS パケットを検出した場合、このカウンタが増分します。たとえば、DNS パケットに DNS ヘッダーがない場合や､DNS リソース レコード数がヘッダー内のカウンタと一致しない場合などです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-dns-out-of-app-id	app id 以外の DNS Inspect。	DNS 検査エンジンが、DNS メッセージの ID を保存するためのデータ構造の割り当てに失敗した場合、このカウンタが増分します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
inspect-dns-pak-too-long	DNS Inspect パケットが長すぎます。	DNS メッセージ長が設定されている最大値を超えると、このカウンタが増分します。 **推奨事項**：アクションは不要です。DNS メッセージ長のチェックが必要でない場合は、**inspect dns maximum-length** オプションを指定せずに DNS 検査をイネーブルにします。 **システム ログ メッセージ**：410001
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect の組み込み接続が異なります。	ICMP エラー メッセージに埋め込まれたフレームが、ICMP 接続の作成時に識別された確立済みの接続と一致しない場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005
inspect-icmp-error-no-existing-conn	ICMP Error Inspect に既存の接続がありません。	セキュリティ アプライアンスが、ICMP エラー メッセージに埋め込まれたフレームに関連する確立済みの接続を見つけられなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-icmp-out-of-app-id	app id 以外の ICMP Inspect。	ICMP 検査エンジンが App ID データ構造の割り当てに失敗した場合、このカウンタが増分します。このデータ構造は、ICMP パケットのシーケンス番号を保存するのに使用します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
inspect-icmp-seq-num-not-matched	ICMP Inspect シーケンス番号が一致しません。	ICMP エコー応答メッセージ内のシーケンス番号が、同じ接続上で先にセキュリティ アプライアンスを通過した ICMP エコー メッセージのいずれにも一致しない場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313004
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect 無効パケット。	セキュリティ アプライアンスが ICMPv6 パケットに埋め込まれた無効なフレームを検出した場合、このカウンタが増分します。このチェックは IPv6 パケットと同じものです。たとえば、不完全な IPv6 ヘッダーや変造された IPv6 Next Header などです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect に既存の接続がありません。	セキュリティ アプライアンスが、ICMPv6 エラー メッセージに埋め込まれたフレームに関連する確立済みの接続を見つけられなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005
inspect-rtcp-invalid-length	無効な RTCP パケット長。	このカウンタは、UDP パケット長が RTCP ヘッダーのサイズよりも短い場合に増分します。 **推奨事項**：アクションは不要です。キャプチャを利用すると、不適切なパケットを送信している RTP 送信元を特定できるので、アクセス リストを使用してそのホストを拒否できます。 **システム ログ メッセージ**：なし。
inspect-rtcp-invalid-payload-type	無効な RTCP ペイロード タイプ フィールド。	このカウンタは、RTCP ペイロード タイプ フィールドに 200 から 204 の値が含まれていない場合に増分します。 **推奨事項**：RTP のソースを検証して、RFC 1889 で推奨される範囲外のペイロード タイプが送信された理由を確認する必要があります。 **システム ログ メッセージ**：431002

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-rtcp-invalid-version	無効な RTCP バージョン フィールド。	このカウンタは、RTCP バージョン フィールドが 2 以外のバージョンを含む場合に増分します。 **推奨事項**：ネットワーク内の RTP ソースが RFC 1889 に適合する RTCP パケットを送信していないようです。アクセス リストを使用するホストを要求に応じて拒否できるよう、この理由を特定する必要があります。 **システム ログ メッセージ**：431002
inspect-rtp-invalid-length	無効な RTP パケット長。	このカウンタは、UDP パケット長が RTP ヘッダーのサイズより短いと増分します。 **推奨事項**：アクションは不要です。キャプチャを利用すると、不適切なパケットを送信している RTP 送信元を特定できるので、アクセス リストを使用してそのホストを拒否できます。 **システム ログ メッセージ**：なし。
inspect-rtp-invalid-payload-type	無効な RTP ペイロード タイプ フィールド。	このカウンタは、信号を発信しているチャンネルが RTP セカンダリ接続の自動メディア タイプについてネゴシエートしているときに、RTP ペイロード タイプ フィールドにオーディオ ペイロード タイプが含まれていないと増分します。カウンタは、ビデオ ペイロード タイプの場合と同じように増分します。 **推奨事項**：ネットワーク内の RTP ソースはオーディオ RTP セカンダリ接続を使用してビデオを送信しています（逆の場合も同じ）。この操作が行われないようにする場合は、アクセス リストを使用するホストを拒否できます。 **システム ログ メッセージ**：431001
inspect-rtp-invalid-version	無効な RTP バージョン フィールド。	このカウンタは、RTP バージョン フィールドが 2 以外のバージョンを含む場合に増分します。 **推奨事項**：ネットワーク内の RTP ソースは RFC 1889 に適合する RTCP パケットを送信していないようです。この理由を特定する必要があり、必要な場合はアクセス リストを使用するホストを拒否できます。 **システム ログ メッセージ**：431001
inspect-rtp-max-outofseq-paks-probation	検査期間中の順番どおりでない RTP パケット。	このカウンタは、RTP ソースを確認中に、順番どおりでない RTP パケットの数が 20 を超えると増分します。検査では、順番どおりの 5 つのパケットを検出すると、ソースが確認済みであると判断されます。 **推奨事項**：RTP ソースを調べて、最初のいくつかのパケットが順番どおりに着信しない理由を確認し、RTP ソースを訂正します。 **システム ログ メッセージ**：431001

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-rtp-sequence-num-outofrange	範囲外の RTP シーケンス番号。	このカウンタは、パケット内の RTP シーケンス番号が検査により予想された範囲内にないと増分します。 **推奨事項**：RTP ソースからシーケンス番号が順番どおりでない場合、検査によって復元され、新しいシーケンス番号からトラッキングが開始されるので、アクションは必要ありません。 **システム ログ メッセージ**：431001
inspect-rtp-ssrc-mismatch	無効な RTP 同期ソース フィールド。	このカウンタは、パケット内の RTP SSRC フィールドが、すべての RTP パケット内の RTP ソースからの、検査により確認された SSRC と一致しないと増分します。 **推奨事項**：これは、ネットワーク内の RTP ソースがリブートして SSRC を変更したためか、またはネットワーク上の別のホストがファイアウォール上で開かれているセカンダリ RTP 接続を使用して RTP パケットを送信しようとしているために生じます。問題があるかどうか確認するために、さらに調べる必要があります。 **システム ログ メッセージ**：431001
intercept-unexpected	予期しないパケットを代行受信します。	セキュリティ アプライアンスが、サーバからの SYNACK を待機中にクライアントからデータを受信した、または特定の TCP 代行受信状態では処理できないパケットを受信しました。 **推奨事項**：このドロップが接続の失敗の原因である場合、接続のクライアント側およびサーバ側のスニファ トレースを実行し、この問題を報告してください。セキュリティ アプライアンスが攻撃を受けている可能性があり、スニファ トレースまたはスニファ キャプチャが原因の特定に役立ちます。 **システム ログ メッセージ**：なし。
interface-down	インターフェイスがダウンしています。	**shutdown** コマンドを使用して、シャットダウンしているインターフェイス上でパケットを受信するたびに、このカウンタが増分します。入トラフィックでは、セキュリティ コンテキスト分類が行われ、そのコンテキストに関連付けられたインターフェイスがシャットダウンしている場合、このパケットはドロップされます。出トラフィックでは、出トラフィックがシャットダウンしている場合、パケットがドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
invalid-app-length	無効な app 長。	セキュリティ アプライアンスがパケット内にレイヤ 7 ペイロードの無効な長さを検出した場合、このカウンタが増分します。現在は、DNS Guard 機能のみによるドロップをカウントします。たとえば、不完全な DNS ヘッダーなどです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
invalid-encap	無効なカプセル化。	セキュリティ アプライアンスが、サポートされていないリンク レベルのプロトコルに属するフレームを受信した場合、またはフレームに指定されている L3 タイプがセキュリティ アプライアンスによってサポートされていない場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：直接接続されているホストのリンク レベル プロトコルの設定が正しいことを確認します。 **システム ログ メッセージ**：なし。
invalid-ethertype	無効な ethertype。	セキュリティ アプライアンス上のフラグメンテーション モジュールが、IP バージョン 4 またはバージョン 6 に属さないフラグメント化されたパケットを受信した場合、または送信しようとした場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：セキュリティ アプライアンスやネットワークに接続されている他のデバイスの MTU を確認し、セキュリティ アプライアンスがなぜそのようなフラグメントを処理しているのかを判断します。 **システム ログ メッセージ**：なし。
invalid-ip-header	無効な IP ヘッダー。	セキュリティ アプライアンスが、IP ヘッダーの算出されたチェックサムとヘッダーに記録されているチェックサムが一致しない IP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、ピアから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
invalid-ip-length	無効な IP 長。	セキュリティ アプライアンスが IPv4 または IPv6 パケットを受信し、そのパケットの IP ヘッダー内のヘッダー長フィールドまたは全長フィールドが有効でない、または受信したパケット長と矛盾する場合、このカウンタが増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
invalid-ip-option	設定された IP オプションはドロップされます。	ユニキャスト パケットまたはマルチキャスト パケットに対して IP オプションを受信するように設定されていないのに、セキュリティ アプライアンスが受信した場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：IP オプションを指定されたパケットが送信者から送信された理由を調査します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
invalid-tcp-hdr-length	無効な tcp 長。	セキュリティ アプライアンスが、パケット サイズが許可されている最小ヘッダー長よりも小さい TCP パケット、または受信したパケット長と矛盾する TCP パケットを受信した場合、このカウンタが増分します。 **推奨事項**：無効なパケットは、攻撃者から送信された偽造パケットの可能性があります。次のシステム メッセージ内の送信元からのトラフィックを調査します。 **システム ログ メッセージ**：500003
invalid-udp-length	無効な udp 長。	セキュリティ アプライアンスが受信した UDP パケットのサイズが、ヘッダー内のフィールドから計算されたサイズと、ネットワークから受信したときに測定されたサイズで異なる場合、このカウンタが増分します。 **推奨事項**：無効なパケットは、攻撃者から送信された偽造パケットの可能性があります。 **システム ログ メッセージ**：なし。
ipsec-clearpkt-notun	トンネルなしの IPSEC Clear Pkt。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
ipsec-ipv6	IPV6 経由の IPSEC。	セキュリティ アプライアンスが、IPv6 ヘッダーでカプセル化された IPSec ESP パケット、IPSec NAT-T ESP パケット、または IPSec over UDP ESP パケットを受信した場合、このカウンタが増分します。現在セキュリティ アプライアンスは、IPv6 でカプセル化された IPSec セッションをサポートしていません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ipsec-need-sa	IPSEC SA がまだネゴシエートされていません。	セキュリティ アプライアンスが、暗号化の必要があるのに IPSec セキュリティ アソシエーションを確立していないパケットを受信した場合、このカウンタが増分します。通常 LAN-to-LAN IPSec コンフィギュレーションでは、これは正常な状態です。これが表示されると、セキュリティ アプライアンスは宛先ピアとの ISAKMP ネゴシエーションを開始します。 **推奨事項**：セキュリティ アプライアンス上で IPSec LAN-to-LAN を設定している場合は、この表示は正常なもので、問題を示すものではありません。ただし、このカウンタが急速に増分する場合は、**crypto** の設定エラーまたはネットワーク エラーにより、ISAKMP ネゴシエーションが完了できないことを示している可能性があります。宛先ピアと通信可能であることを確認し、**show running-config** コマンドを使用して **crypto** 設定を確認します。 **システム ログ メッセージ**：なし。
ipsec-spoof	IPSEC Spoof が検出されました。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
ipsec-tun-down	IPSEC トンネルがダウンしています。	セキュリティ アプライアンスが、削除中の IPSec 接続に関連付けられたパケットを受信した場合、このカウンタが増分します。 **推奨事項**：IPSec トンネルが何らかの理由で切断された場合、これは正常な状態です。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ipsecudp-keepalive	IPSEC/UDP キープアライブ メッセージ。	セキュリティ アプライアンスが IPSec over UDP キープアライブ メッセージを受信した場合、このカウンタが増分します。IPSec over UDP キープアライブ メッセージは、IPSec over UDP ピアとセキュリティ アプライアンスの間にあるネットワーク デバイスで NAT/PAT フロー情報を常に最新のものにするために、IPSec ピアからセキュリティ アプライアンスに送信されます。 **（注）** UDP 経由でも伝送され UDP ポート 4500 にアドレス指定される、業界標準の NAT-T キープアライブ メッセージはありません。 **推奨事項**：セキュリティ アプライアンス上で IPSec over UDP を設定している場合は、この表示は正常なもので、問題を示すものではありません。セキュリティ アプライアンス上で IPSec over UDP を設定していない場合は、ネットワーク トラフィックを分析し、IPSec over UDP トラフィックの発信元を特定します。 **システム ログ メッセージ**：なし。
ips-fail-close	IPS カードがダウンしています。	AIP SSM がダウンしている状態で、IPS 検査で **fail-close** オプションが使用された場合、このカウンタが増分します。 **推奨事項**：AIP SSM をチェックしてから起動します。 **システム ログ メッセージ**：420001
ips-request	要求された IPS モジュールはドロップされます。	パケットが IPS エンジンのシグニチャと一致した場合、このカウンタが増分し、このパケットは AIP SSM の要求どおりにドロップされます。 **推奨事項**：システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420002
ipv6_sp-security-failed	IPv6 低速パス セキュリティ チェックが失敗しました。	次のいずれかの理由により、このカウンタが増分し、パケットがドロップされます。 • IPv6 through-the-box パケットの送信元アドレスと宛先アドレスが同じである。 • IPv6 through-the-box パケットにリンク ローカル送信元アドレスまたは宛先アドレスがある。 • IPv6 through-the-box パケットの宛先アドレスがマルチキャストである。 **推奨事項**：上記のようなパケットは、悪意のあるアクティビティを示しているか、IPv6 ホストの設定が誤っている結果である可能性があります。パケット キャプチャ機能を使用して type asp パケットをキャプチャし、送信元 MAC アドレスを使用して送信元を特定します。 **システム ログ メッセージ**：送信元アドレスと宛先アドレスが同じ場合、システム メッセージ 106016。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
l2_acl	FP L2 規則がドロップされます。	EtherType アクセス リストによりセキュリティ アプライアンスがパケットを拒否した場合、このカウンタが増分します。デフォルトの場合、ルーテッド モードではセキュリティ アプライアンスは次のものを許可します。 • IPv4 パケット • IPv6 パケット • ARP パケット • FFFF:FFFF:FFFF のレイヤ 2 宛先 MAC（ブロードキャスト） • レイヤ 2 宛先が 0100:5E00:0000-0100:5EFE:FFFF の IPv4 MCAST パケット • レイヤ 2 宛先が 3333:0000:0000-3333:FFFF:FFFF の IPv6 MCAST パケット デフォルトの場合、透過モードではセキュリティ アプライアンスはルーテッド モード アクセス リストおよび次のものを許可します。 • レイヤ 2 宛先が 0100:0CCC:CCCD の BPDU パケット • レイヤ 2 宛先が 0900:0700:0000-0900:07FF:FFFF の Appletalk パケット また、EtherType アクセス リストを設定してインターフェイスに適用することにより、その他のタイプのレイヤ 2 トラフィックを許可することもできます。 **（注）** EtherType アクセス リストに許可されるパケットが、レイヤ 3 またはレイヤ 4 アクセス リストにドロップされる場合もあります。 **推奨事項**：セキュリティ アプライアンスまたはコンテキストを透過モードで実行していて、IP 以外のパケットがセキュリティ アプライアンスにドロップされる場合は、EtherType アクセス リストを設定してこのアクセス リストをアクセス グループに適用することができます。 **（注）** セキュリティ アプライアンスの EtherType アクセス リストは、EtherTypes のみをサポートし、レイヤ 2 宛先 MAC アドレスはサポートしません。 **システム ログ メッセージ**：106026、106027

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
l2_same-lan-port	L2 Src/Dst が同じ LAN ポートです。	セキュリティ アプライアンスまたはコンテキストが透過モードに設定されていて、宛先インターフェイスの L2 MAC アドレスが入力インターフェイスと同じであるとセキュリティ アプライアンスが判断した場合、このカウンタが増分します。 **推奨事項**：セキュリティ アプライアンスまたはコンテキストが透過モードに設定されている場合、これは正常な状態です。セキュリティ アプライアンスが無差別モードで動作しているため、セキュリティ アプライアンスまたはコンテキストはローカル LAN セグメント上のすべてのパケットを受信します。 **システム ログ メッセージ**：なし。
loopback-buffer-full	ループバック バッファがいっぱいです。	セキュリティ アプライアンスのあるコンテキストから別のコンテキストに、共有インターフェイスを介してパケットが送信されたが、ループバック キューにバッファの空き領域がない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：システム CPU をチェックして、過負荷になっていないかどうか確認します。 **システム ログ メッセージ**：なし。
lu-invalid-pkt	無効な LU パケット。	スタンバイ装置が破損した Logical Update パケットを受信しました。 **推奨事項**：ケーブル不良、回線上のノイズ、またはソフトウェアの欠陥により、パケットが破損した可能性があります。インターフェイスが正しく機能しているように見えても、この問題を Cisco TAC に報告してください。 **システム ログ メッセージ**：なし。
mp-pf-queue-full	ポート転送キューがいっぱいです。	このカウンタは、ポート転送アプリケーションの内部キューがいっぱいである際に、別の伝送パケットを受信した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-addr-renew-response	SVC モジュールがアドレス更新応答データ フレームを受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から Address Renew Response メッセージを受信すると増分します。SVC はこのメッセージを送信しません。 **推奨事項**：これは、SVC ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-bad-framing	SVC モジュールが不正にフレーム化されたデータを受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から、またはデコードできないコントロール ソフトウェアからパケットを受信すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037（SVC の受信したデータのみ）
mp-svc-bad-length	SVC モジュールが不正なデータ長を受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から、または計算された指定の長さが一致しないコントロール ソフトウェアからパケットを受信すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037（SVC の受信したデータのみ）
mp-svc-compress-error	SVC モジュール圧縮エラー。	このカウンタは、セキュリティ アプライアンスが、SVC に対してデータを圧縮中にエラーを検出すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037
mp-svc-decompres-error	SVC モジュール圧縮解除エラー。	このカウンタは、セキュリティ アプライアンスが SVC からのデータを圧縮解除中にエラーを検出すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037
mp-svc-delete-in-progress	接続の削除中に SVC モジュールがデータを受信しました。	このカウンタは、セキュリティ アプライアンスが、削除中の SVC 接続に関連付けられたパケットを受信すると増分します。 **推奨事項**：SVC トンネルが何らかの理由で切断された場合、これは正常な状態です。このエラーが繰り返し何度も発生する場合は、クライアントのネットワーク接続に問題があると考えられます。 **システム ログ メッセージ**：なし。
mp-svc-flow-control	SVC セッションがフローを制御しています。	このカウンタは、SVC が一時的にこれ以上データを受信できないため、セキュリティ アプライアンスがデータをドロップする必要がある場合に増分します。 **推奨事項**：クライアントがこれ以上データを受信できないことを示します。クライアントは受信するトラフィックの量を減らす必要があります。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-invalid-mac	SVC モジュールがフレーム内の無効な L2 データを検出しました。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータに添付された L2 MAC ヘッダーが無効であると検出した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-invalid-mac-len	SVC モジュールがフレーム内の無効な L2 データ長を検出しました。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータに添付された L2 MAC 長が無効であると検出した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-channel	SVC モジュールに再注入のためのチャネルがありません。	このカウンタは、暗号化データを受信したインターフェイスが、復号化データを注入する際に検出されないと増分します。 **推奨事項**：インターフェイスが接続中にシャットダウンすると、この現象が発生します。インターフェイスを再イネーブルにしてチェックしてください。接続中にシャットダウンしたのでない場合は、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-mac	SVC モジュールがフレームの L2 データを検出できません。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータの L2 MAC ヘッダーを検出できない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-prepend	SVC　モジュールにヘッダーを挿入するためのスペースがありません。	このカウンタは、ネットワークにパケットを配置するために、パケット データの前に Mac ヘッダーを付加する十分なスペースがない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-session	SVC　モジュールにセッションがありません。	このカウンタは、セキュリティ アプライアンスがこのデータを送信しなければならない SVC セッションを決定できない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-unknown-type	SVC モジュールが不明なデータ フレームを受信しました。	このカウンタは、セキュリティ アプライアンスがデータのタイプが不明な SVC からパケットを受信すると増分します。 **推奨事項**：クライアントが使用している SVC がセキュリティ アプライアンス ソフトウェアのバージョンと適合しているかどうかを確認します。 **システム ログ メッセージ**：なし。
natt-keepalive	NAT-T キープアライブ メッセージ。	セキュリティ アプライアンスが IPSec NAT-T キープアライブ メッセージを受信した場合、このカウンタが増分します。NAT-T キープアライブ メッセージは、NAT-T IPSec ピアとセキュリティ アプライアンスの間にあるネットワーク デバイスで NAT/PAT フロー情報を常に最新のものにするために、IPSec ピアからセキュリティ アプライアンスに送信されます。 **推奨事項**：セキュリティ アプライアンス上で IPSec NAT-T を設定している場合は、この表示は正常なもので、問題を示すものではありません。セキュリティ アプライアンス上で NAT-T を設定していない場合は、ネットワーク トラフィックを分析し、NAT-T トラフィックの発信元を特定します。 **システム ログ メッセージ**：なし。
no-adjacency	有効な隣接情報がありません。	セキュリティ アプライアンスが隣接情報を取得しようとしましたが、ネクストホップの MAC アドレスを取得できなかった場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：このドロップ理由のキャプチャを設定し、指定された宛先アドレスのホストが、接続されたネットワーク上に存在するかどうか、またはセキュリティ アプライアンスからルーティング可能かどうかをチェックします。 **システム ログ メッセージ**：なし。
no-mcast-entry	FP に mcast エントリがありません。	次のいずれかの理由により、このカウンタが増分します。 • マルチキャスト　フローに一致するパケットが着信したが、マルチキャスト サービスがイネーブルでなくなっていた、またはマルチキャスト フローが作成された後で再度イネーブルにされた。 **推奨事項**：マルチキャストがディセーブルの場合は、再度イネーブルにします。 **システム ログ メッセージ**：なし。 • パケットが CP にパントされた後にマルチキャスト エントリの変更が検出され、エントリが存在しないために NP がパケットを転送できない。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
no-mcast-intrf	FP に mcast 出力インターフェイスがありません。	次のいずれかの理由により、このカウンタが増分します。 • すべての出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**: このグループに受信者が存在しないことを確認します。 **システム ログ メッセージ**：なし。 • マルチキャスト パケットを転送できなかった。 **推奨事項**: このパケットにフローが存在することを確認します。 **システム ログ メッセージ**：なし。
non-ip-pkt-in-routed-mode	非 IP パケットがルーテッド モードで受信されました。	セキュリティ アプライアンスが受信したパケットが IPv4 パケット、IPv6 パケット、ARP パケットのいずれでもなく、セキュリティ アプライアンスまたはコンテキストがルーテッド モードに設定されている場合、このカウンタが増分します。通常の動作では、そのようなパケットはドロップされます。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：106026、106027
no-route	ホストへのルートがありません。	セキュリティ アプライアンスがパケットをインターフェイスから送信しようとしましたが、そのためのルートがルーティング テーブルで見つからなかった場合、このカウンタが増分します。 **推奨事項**：生成されたシステム メッセージから取得した宛先アドレスのルートが存在することを確認します。 **システム ログ メッセージ**：110001
np-socket-closed	終了したソケット内の保留パケットがドロップされました。	ソケットがユーザまたはソフトウェアにより突然終了すると、そのソケットのパイプライン中にある保留中のパケットもドロップします。このカウンタは、パイプライン中にある各ソケットがドロップするたびに増分します。 **推奨事項**：このカウンタは、一般的に、通常の動作の一部として増分していきます。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
np-sp-invalid-spi	無効な SPI。	セキュリティ アプライアンスが、現在既知ではない SPI（security parameter index; セキュリティ パラメータ インデックス）を指定するセキュリティ アプライアンスにアドレス変換される IPSec ESP パケットを受信した場合、このカウンタが増分します。 **推奨事項**：無効な SPI が時折表示されるのは珍しいことではなく、特にキーの再生成処理中にはよく起こります。無効な SPI が何度も表示される場合は、何らかの問題または DoS 攻撃を示している可能性があります。無効な SPI が頻繁に表示される場合は、ネットワーク トラフィックを分析して ESP トラフィックの送信元を特定します。 **システム ログ メッセージ**：402114
punt-rate-limit	パントのレート制限を超えました。	セキュリティ アプライアンスがレイヤ 2 パケットをレート制限されたコントロール ポイント サービス ルーチンに転送しようとしたが、レート制限（毎秒）を超えている場合、このカウンタが増分します。現在、レート制限されているコントロール ポイント サービス ルーチン宛てのレイヤ 2 パケットは、ARP パケットだけです。ARP パケットのレート制限は、インターフェイスあたり毎秒 500 ARP です。 **推奨事項**：ネットワーク トラフィックを分析し、ARP パケットのレート制限を超えた理由を判断します。 **システム ログ メッセージ**：322002、322003
queue-removed	キューに入っているパケットがドロップされました。	QoS 設定が変更または削除されると、出力キューで送信の待機をしていた既存のパケットはドロップされ、このカウンタが増分します。 **推奨事項**：正常な状態では、ユーザが QoS 設定を変更した場合に、このような状況が見られます。QoS 設定が何も変更されていないのにこの状況が発生した場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。
rate-exceeded	QoS レートを超えました。	レート制限（ポリシング）が出力 / 入力インターフェイスに設定され、出力/入力トラフィック レートが設定されたバースト レートを超えた場合、このカウンタが増分します。パケットがドロップされるたび、このカウンタが増分します。 **推奨事項**：インターフェイスから送信されるトラフィックのレートがなぜ設定されたレートを超えたのかを調査し、原因を特定します。正常な状態の場合もあれば、ウイルスの感染や攻撃を示している可能性もあります。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
rm-conn-limit	RM 接続制限に達しました。	このカウンタは、コンテキストまたはシステムの最大接続数に達して新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-conn-rate-limit	RM 接続レート制限に達しました。	このカウンタは、コンテキストまたはシステムの最大接続レートに達して新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321002
rpf-violated	逆パス確認が失敗しました。	**ip verify reverse-path** がインターフェイス上に設定されていて、セキュリティ アプライアンスが受信したパケットの発信元 IP ルート検索から得られたインターフェイスが、このパケットが受信されたインターフェイスと異なる場合、このカウンタが増分します。 **推奨事項**：次のシステム メッセージに示されている発信元 IP に基づいてトラフィックの発信元をトレースし、なぜスプーフィングされたトラフィックが送信されているのかを調査します。 **システム ログ メッセージ**：106021
security-failed	早期セキュリティ チェックが失敗しました。	セキュリティ アプライアンスが次のような場合、このカウンタが増分し、パケットはドロップされます。 • IPv4 マルチキャスト パケットを受信したが、パケットのマルチキャスト MAC アドレスがパケットのマルチキャスト宛先 IP アドレスと一致しない。 • オフセットの小さいフラグメントまたは重複するフラグメントが含まれている IPv6 または IPv4 teardrop フラグメントを受信した。 • IP 監査シグニチャと一致する IPv4 パケットを受信した。 **推奨事項**：リモート ピアの管理者に連絡する、またはセキュリティ ポリシーに従ってこの問題の危険度を高くします。IP 監査攻撃チェックの詳細な説明とシステム メッセージについては、**ip audit signature** コマンドを参照してください。 **システム メッセージ**：106020、400xx（IP 監査チェックの場合）
send-ctm-error	CTM　への送信がエラーを返しました。	このカウンタはセキュリティ アプライアンスでは廃止され、増分することはありません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
sp-security-failed	低速パス　セキュリティ チェックが失敗しました。	セキュリティ アプライアンスが次のような場合、このカウンタが増分し、パケットはドロップされます。 • ルーテッド モードで、次の through-the-box パケットを受信した。 — L2 ブロードキャスト パケット — 宛先 IP アドレスが 0.0.0.0 の IPv4 パケット — 送信元 IP アドレスが 0.0.0.0 の IPv4 パケット **推奨事項**：外部ユーザが、保護されたネットワークを侵害しようとしているかどうか判断します。設定に誤りのあるクライアントをチェックします。 **システム ログ メッセージ**：106016 • ルーテッド モードまたは透過モードで、次の through-the-box IPv4 パケットを受信した。 — 送信元 IP アドレスの最初のオクテットがゼロ。 — 送信元 IP アドレスがループバック IP アドレスと等しい。 — 送信元 IP アドレスのネットワーク部分がすべて 0。 — 送信元 IP アドレスのネットワーク部分がすべて 1。 — 送信元 IP アドレスのホスト部分がすべて 0 またはすべて 1。 **推奨事項**：外部ユーザが、保護されたネットワークを侵害しようとしているかどうか判断します。設定に誤りのあるクライアントをチェックします。 **システム ログ メッセージ**：106016 • ルーテッド モードまたは透過モードで、送信元と宛先の IP アドレスが同じ IPv4 パケットまたは IPv6 パケットを受信した。 **推奨事項**：このメッセージ カウンタが急速に増分する場合は、攻撃を受けている可能性があります。パケット キャプチャ機能を使用して type asp パケットをキャプチャし、パケット内の送信元 MAC アドレスをチェックして送信元を特定します。 **システム ログ メッセージ**：106017

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ssm-app-fail	サービス モジュールがダウンしています。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。SSM により検査されるパケットが、SSM が使用不可になったためにドロップすると増分します。たとえば、ソフトウェアまたはハードウェアの欠陥、ソフトウェアまたはシグナチャのアップグレード、またはシャットダウンするモジュールなどです。 **推奨事項**：セキュリティ アプライアンスのコントロール プレーンで実行する SSM マネージャ プロセスは、システム メッセージと CLI 警告を発行してその障害を通知します。SSM 障害のトラブルシューティングについては、SSM に付属するマニュアルを参照してください。必要な場合は、Cisco TAC にお問い合せください。 **システム ログ メッセージ**：なし。
ssm-app-request	サービス モジュールがドロップを要求しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。このカウンタは、SSM で実行するアプリケーションが、セキュリティ アプライアンスがパケットをドロップすることを要求すると増分します。 **推奨事項**：詳細については、事故レポート、または SSM により生成されるシステム メッセージを照会することで取得することができます。手順については、SSM に付属のマニュアルを参照してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ssm-asdp-invalid	SSM カードから無効な ASDP パケットを受信しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。セキュリティ アプライアンスが内部データ プレーン インターフェイスから ASA SSM Dataplane Protocol（ASDP）パケットを受信したが、このパケットを解析してドライバに問題が生じると増分します。ASDP は、CSC SSM と同様に、特定のタイプの SSM と通信するためにセキュリティ アプライアンスが使用するプロトコルです。この現象は、さまざまな理由により生じます。たとえば、ASDP プロトコルのバージョンがセキュリティ アプライアンスと SSM 間で適合しなかった場合、コントロール プレーン内の SSM マネージャ プロセスがシステム メッセージと CLI 警告を送信して、インストールする適切なバージョンのイメージを通知します。ASDP パケットがセキュリティ アプライアンス側ですでに終了している接続に属している場合もあります。セキュリティ アプライアンスがスタンバイ状態に切り替わっている場合（フェールオーバーがイネーブルになっている場合）には、これ以降トラフィックを通過させることができません。また、ASDP ヘッダーとペイロードの解析時に予期しない値があった場合もあります。 **推奨事項**：カウンタは通常 0 または非常に小さい数値です。ただし、カウンタが長期わたって少しずつ増分した場合、特にフェールオーバーがあったときや、CLI 経由でセキュリティ アプライアンスの接続を手動で消去したときは考慮する必要がありません。カウントが通常動作時に急激に増分した場合は、Cisco TAC に連絡してください。 システム ログ メッセージ：421003、421004
ssm-dpp-invalid	SSM カードから無効なパケットを受信しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。セキュリティ アプライアンスが内部データ プレーン インターフェイスから ASA SSM Dataplane Protocol（ASDP）パケットを受信するが、それを解析する適切なドライバを検出できない場合に増分します。 **推奨事項**：データ プレーン ドライバは、システムにインストールされた SSM のタイプに応じて動的に登録されます。したがって、この現象は、セキュリティ アプライアンスが完全に初期化される前にデータ プレーン パケットが到着すると発生する可能性があります。このカウンタの値は通常 0 です。ドロップが若干あっても気にする必要はありません。ただし、システムが起動して稼働中であるときにこのカウンタの値が上昇し続ける場合は、問題があることを示している可能性があります。これがセキュリティ アプライアンスの正常な動作に影響を与えると思われる場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp_xmit_partial	TCP 再送信が不完全です。	**check-retransmission** 機能がイネーブルになっていて、不完全な TCP 再送信を受信した場合、このカウンタが増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-3whs-failed	TCP が 3 ウェイ ハンドシェイクに失敗しました。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に無効な TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。たとえば、クライアントからの SYN-ACK は、この理由でドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-acked	TCP DUP が確認されました。	セキュリティ アプライアンスが再送信されたデータ パケットを受信し、このデータがピア TCP エンドポイントにより確認応答された場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-ack-syn-diff	SYNACK 内の TCP ACK が無効です。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に不適切な TCP 確認応答番号によって SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-bad-option-len	TCP 内のオプション長が不正です。	セキュリティ アプライアンスが TCP オプションが設定されている TCP パケットを受信しましたが、このオプションの長さが TCP RFC で定義されているオプションの長さと一致しない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-bad-option-list	TCP オプション リストが無効です。	セキュリティ アプライアンスが受信した TCP パケットの TCP ヘッダーに非標準の TCP ヘッダー オプションが付属していた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可する、または非標準の TCP ヘッダー オプションを消去してこのパケットを許可するには、**tcp-options** コマンドを使用します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-bad-sack-allow	TCP SACK ALLOW オプションが不正です。	セキュリティ アプライアンスが受信した TCP パケットに選択的な確認応答オプションが指定されているのに、SYN フラグがセットされていない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-bad-winscale	TCP ウィンドウ スケール値が不正です。	セキュリティ アプライアンスが受信した TCP パケットに 14 より大きい window-scale オプションが指定されている場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-buffer-full	TCP パケット バッファがいっぱいです。	セキュリティ アプライアンスが接続上で順序が乱れた TCP パケットを受信したが、このパケットを保存するバッファがない場合、このカウンタが増分し、このパケットはドロップされます。通常 TCP パケットは、順番に接続上に配置されてセキュリティ アプライアンスによって検査されるか、またはパケットが SSM に送信されて検査されます。デフォルトのキュー サイズがあり、このデフォルトのキュー サイズを超えるパケットを受信すると、ドロップされます。 **推奨事項**：ASA プラットフォームでは、**queue-size** コマンドを使用してキュー サイズを増分できます。 **システム ログ メッセージ**：なし。
tcp-conn-limit	TCP 接続制限値に到達しました。	この理由は、TCP 接続設定フェーズ中に接続制限値を超えたため、TCP パケットがドロップされたことによるものです。接続制限値は、**set connection conn-max** コマンドを使用して設定します。 **推奨事項**：カウンタが急速に増分する場合は、システム メッセージをチェックし、どのホストが接続制限値に到達したのかを判断します。トラフィックが正常な場合、またはホストが攻撃を受けている場合は、接続制限値を増分する必要があることもあります。 **システム ログ メッセージ**：201011

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-data-past-fin	FIN 後に TCP データが送信されました。	FIN を送信済みで接続を終了したエンドポイントから、セキュリティ アプライアンスが新しい TCP データ パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-discarded-ooo	3 方向ハンドシェイクで TCP ACK が無効です。	このカウンタは、セキュリティ アプライアンスが 3 方向ハンドシェイク中にクライアントから TCP ACK パケットを受信し、シーケンス番号が次に予想されるシーケンス番号でない場合に増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-dual-open	TCP デュアル オープンが拒否されました。	セキュリティ アプライアンスがサーバから TCP SYN パケットを受信したが、初期 TCP 接続がすでに開始している場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-fo-drop	TCP の複製されたフロー pak がドロップされました。	このカウンタは、セキュリティ アプライアンスがアクティブ装置となった直後に、確立した接続上でセキュリティ アプライアンスが SYN、FIN、または RST などのコントロール フラグを持つ TCP パケットを受信すると増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-invalid-ack	TCP の無効な ACK。	セキュリティ アプライアンスが受信した TCP パケットの確認応答番号が、ピア TCP エンドポイントから送信されたデータよりも大きい場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-mss-exceeded	TCP データが MSS を超過。	セキュリティ アプライアンスが受信した TCP パケットのデータの長さが、ピア TCP エンドポイントから通知された MSS よりも大きい場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可するには、**exceed-mss** コマンドを使用します。 **システム ログ メッセージ**：4419001

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcpnorm-rexmit-bad	TCP の不正な再送信。	**check-retransmission** 機能がイネーブルになっていて、元のパケットと異なるデータを持つ TCP 再送信を受信した場合、このカウンタが増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcpnorm-win-variation	TCP の予期しない、さまざまなウィンドウ サイズ。	TCP エンドポイントにアドバタイズされたウィンドウ サイズが、大量のデータを受け取ることもなく激変した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのようなパケットを許可するには、**window-variation** コマンドを使用します。 **システム ログ メッセージ**：なし。
tcp-not-syn	最初の TCP パケットが SYN ではありません。	セキュリティ アプライアンスが、代行受信でもなくネイリングもされていない接続の最初のパケットとして、SYN ではないパケットを受信しました。 **推奨事項**：正常な状態では、セキュリティ アプライアンスがすでに接続を終了したのに、クライアントまたはサーバ側がまだ接続が続いていると見なしてデータ転送を続けている場合に、このような現象が見られます。**clear local-host** コマンドまたは **clear xlate** コマンドを発行した直後に、このような状況が発生することがあります。接続が削除された直後でもないのに、このカウンタが急速に増分する場合は、セキュリティ アプライアンスが攻撃を受けている可能性もあります。原因を特定するためには、スニファ トレースを取り込みます。 **システム ログ メッセージ**：6106015
tcp-paws-fail	TCP パケットが PAWS テストに失敗しました。	タイムスタンプ ヘッダー オプションが指定されている TCP パケットが、PAWS（Protect Against Wrapped Sequences）テストに失敗した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような接続の続行を許可するには、**tcp-options** コマンドを使用してタイムスタンプ オプションを消去します。 **システム ログ メッセージ**：なし。
tcp-reserved-set	TCP の予約済みフラグが設定されました。	セキュリティ アプライアンスが受信した TCP パケットの TCP ヘッダーに予約済みのフラグが設定されていた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。そのような TCP パケットを許可するか予約済みフラグを消去して、このパケットを渡すには、**reserved-bits** コマンドを使用します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-rstfin-ooo	順序が異なる TCP RST/FIN。	セキュリティ アプライアンスが受信した RST パケットまたは FIN パケットの TCP シーケンス番号が不適切な場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-rst-syn-in-win	TCP RST/SYN がウィンドウ内にあります。	セキュリティ アプライアンスが確立された接続上で受信した TCP SYN パケットまたは TCP RST パケットのシーケンス番号が、ウィンドウ内にはあるが次に予測されるシーケンス番号ではなかった場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-seq-past-win	TCP パケットの SEQ がウィンドウを超えています。	セキュリティ アプライアンスが受信した TCP データ パケットのシーケンス番号が、ピア TCP エンドポイントで許可されているウィンドウを超えている場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-seq-syn-diff	SYN/SYNACK　内の TCP SEQ が無効です。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に不適切な TCP シーケンス番号によって SYN パケットまたは SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-synack-data	TCP SYNACK にデータがあります。	セキュリティ アプライアンスが受信した TCP SYN-ACK パケットにデータがある場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-synack-ooo	TCP SYNACK が確立された接続上にあります。	セキュリティ アプライアンスが確立された TCP 接続上で TCP SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-syn-data	TCP SYN にデータがあります。	セキュリティ アプライアンスが受信した TCP SYN パケットにデータがある場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可するには、**syn-data** コマンドを使用します。 **システム ログ メッセージ**：なし。
tcp-syn-ooo	TCP SYN が確立された接続上にあります。	セキュリティ アプライアンスが確立された TCP 接続上で TCP SYN パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-winscale-no-syn	TCP ウィンドウ スケールが非 SYN 上にあります。	セキュリティ アプライアンスが受信した TCP パケットが、SYN フラグが設定されずに window-scale TCP オプションが指定されていた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tfw-no-mgmt-ip-config	TFW に管理 IP アドレスが設定されていません。	セキュリティ アプライアンスが透過モードで IP パケットを受信したが、管理 IP アドレスが定義されていない場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：セキュリティ アプライアンスに管理 IP アドレスとマスク値を設定します。 **システム ログ メッセージ**：322004
unable-to-add-flow	フロー ハッシュがいっぱいです。	新しく作成されたフローがフロー ハッシュ テーブルに挿入されましたが、フロー ハッシュ テーブルがいっぱいだったために挿入が失敗した場合、このカウンタが増分します。フローとパケットはドロップされます。このカウンタは、最大接続数の制限値に到達した場合に増分するカウンタとは異なります。 **推奨事項**：このメッセージは、セキュリティ アプライアンスがリソース不足で、操作が成功しなかったことを示しています。**show conn** 出力内の接続が、設定されたアイドル タイムアウト値を超えているかどうかチェックしてください。超えている場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
unable-to-create-flow	リソース制限により拒否されたフロー	このカウンタは、システム リソースが制限されているため、フローの作成が失敗すると増分し、パケットはドロップされます。リソースの制限は、次のとおりです。 • システム メモリ • パケット ブロック拡張メモリ • システムの接続制限 最初の 2 つの原因は、「No memory to complete flow（フローを完了するメモリがない)」というフローのドロップ理由で同時に発生します。 **推奨事項**： • システム メモリの空き容量が少ないかどうか確認します。 • 「No memory to complete flow（フローを完了するメモリがない)」というフローのドロップ理由が発生するかどうか確認します。 • **show resource usage** コマンドを使用して、接続カウントがシステム接続制限に達しているかどうか確認します。 **システム ログ メッセージ**：なし。
unexpected-packet	予測されないパケット。	このカウンタは、透過モードでセキュリティ アプライアンスが MAC アドレス宛の非 IP パケットを受信するが、このパケットを処理するための該当するサービスがセキュリティ アプライアンス上にない場合に増分します。 推奨事項：セキュリティ アプライアンスが攻撃を受けているかどうか確認します。疑わしいパケットがない場合、またはセキュリティ アプライアンスが透過モードでない場合、このカウンタは、ソフトウェア エラーが原因で増分していると考えられます。カウンタの増分の原因であるトラフィックを把握し、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。
unsupported-ip-version	サポートされていない IP バージョン。	セキュリティ アプライアンスが受信した IP パケットの IP ヘッダー内のバージョン フィールドに、サポートされていないバージョンが入っている場合、このカウンタが増分します。特に、このパケットがバージョン 4 またはバージョン 6 に属していない場合、パケットはドロップされます。 **推奨事項**：ネットワークに接続されている他のデバイスが、バージョン 4 または 6 のみに属する IP パケットを送信するように設定されていることを確認します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
unsupport-ipv6-hdr	サポートされていない IPV6 ヘッダー。	サポートされていない IPv6 拡張ヘッダーが付いた IPv6 パケットを受信した場合、このカウンタが増分し、そのパケットはドロップされます。サポートされている IPv6 拡張ヘッダーは、TCP、UDP、ICMPv6、ESP、AH、Hop オプション、Destination オプション、および Fragment です。IPv6 ルーティング拡張ヘッダーはサポートされていません。また、上記以外の拡張ヘッダーもサポートされていません。IPv6 ESP ヘッダーと AH ヘッダーは、パケットが through-the-box の場合にのみサポートされます。To-the-box の IPv6 ESP パケットと AH パケットはサポートされず、ドロップされます。 **推奨事項**：このエラーは、ホスト設定の誤りが原因である可能性があります。このエラーが再発する場合、または何度も発生する場合は、DoS 攻撃など偽のアクティビティや悪意のあるアクティビティを示している可能性があります。 **システム ログ メッセージ**：なし。
vpn-context-expired	期限が切れた VPN コンテキスト。	このカウンタは、暗号化または復号化を必要とするパケットをセキュリティ アプライアンスが受信する場合、または操作を実行するために必要な ASP VPN が有効でなくなる場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
wccp-redirect-no-route	キャッシュ エンジンへのルートはありません。	このカウンタは、セキュリティ アプライアンスがパケットのリダイレクトを試行し、キャッシュ エンジンへのルートを検出できない場合に増分します。 **推奨事項**：キャッシュ エンジンへのルートが存在することを確認してください。 **システム ログ メッセージ**：なし。
wccp-return-no-route	WCCP　が戻したパケットのホストへのルートがありません。	このカウンタは、パケットがキャッシュ エンジンから戻され、セキュリティ アプライアンスがこのパケットの元のソースのルートを検出できない場合に増分します。 **推奨事項**：キャッシュ エンジンから戻されたパケットのソース IP アドレスのルートが存在することを確認します。 **システム ログ メッセージ**：なし。

表 25-2 は、ドロップされたフローの *flow_drop_reason* 引数の有効な値を示しています。

表 25-2　フロー ドロップの理由

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
acl-drop	アクセス規則によってフローが拒否されます。	このカウンタは、パケットがセキュリティ アプライアンスに拒否された場合に増分し、フローの作成は拒否されます。拒否規則は、セキュリティ アプライアンスの起動時、さまざまな機能がオンまたはオフにされたとき、アクセス リストがインターフェイスに適用されたとき、またはその他の機能で作成されたデフォルトの規則の可能性があります。デフォルトの規則のドロップを除き、フローが拒否される理由は次のとおりです。 • インターフェイス上にアクセス リストが設定されている。 • アクセス リストが AAA 用に設定されていて、AAA がユーザを拒否した。 • トラフィックを通過して管理専用インターフェイスに到達した。 • IPSec がイネーブルになっているインターフェイスに、暗号化されていないトラフィックが到達した。 • アクセス リストの末尾に暗黙的な拒否がある。 **推奨事項**：パケットのドロップに関連するシステム メッセージが表示されるかどうか確認します。フロー ドロップにより対応するパケットもドロップされ、必要なシステム メッセージが表示されます。 **システム ログ メッセージ**：なし。
audit-failure	監査が失敗しました。	関連付けられたアクションとしてリセットした **ip audit** シグニチャと一致した後、フローは解放されました。 **推奨事項**:このシグニチャと一致したときにフローの削除を望まない場合は、**ip audit** コマンドからリセット アクションを削除します。 **システム ログ メッセージ**：なし。
closed-by-inspection	検査によりフローが終了しました。	この理由は、アプリケーション検査中にエラーが検出されたためにフローが終了したことによるものです。たとえば、H323 メッセージの検査中にエラーが検出された場合、この理由により対応する H323 フローが終了します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
conn-limit-exceeded	接続制限値を超えました。	この理由は、接続制限値を超えたためにフローが終了したことによるものです。接続制限値は、**set connection conn-max** コマンドを使用して設定します。 **推奨事項**：なし。 **システム ログ メッセージ**：201011

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
fin-timeout	FIN のタイムアウト。	この理由は、ハーフクローズ タイマーが時間切れになったためにTCP フローが終了したことによるものです。 **推奨事項**：TCP フローの終了よりも時間のかかる有効なセッションがある場合は、ハーフクローズ タイムアウトを増分します。 **システム ログ メッセージ**：302014
flow-reclaimed	tcp/udp 以外のフローが新しい要求を再要求しました。	再要求可能なフローが削除されて新しいフローの要求が可能になると、このカウンタが増分します。これは、セキュリティ アプライアンスを通過するフロー数がソフトウェアの制限で許可された最大数と等しくなり、新しいフロー要求が受信された場合にのみ発生します。この状況が発生すると、再要求可能なフロー数がセキュリティ アプライアンスで許可されている VPN トンネル数を超えた場合、最も古い再要求可能なフローが削除され、新しいフローが可能になります。すべてのフローが再要求可能とされていますが、次のフローは除きます。 • TCP、UDP、GRE およびフェールオーバー フロー • ICMP フロー（ICMP ステートフル検査がイネーブルの場合） • セキュリティ アプライアンスへの ESP フロー **推奨事項**：このカウンタが徐々に増分する場合は、アクションは不要です。このカウンタが急速に増分する場合は、セキュリティ アプライアンスが攻撃を受けていて、セキュリティ アプライアンスのフロー再作成と再要求に時間がかかっていることを示している可能性があります。 **システム ログ メッセージ**：302021
fo-primary-closed	フェールオーバー プライマリが終了しました。	スタンバイ装置がアクティブ装置からフロー削除メッセージを受信し、フローを終了しました。 **推奨事項**：セキュリティ アプライアンスがステートフル フェールオーバーを実行している場合は、スタンバイ アプライアンス上で切断された接続が複製されるたびに、このカウンタが増分します。 **システム ログ メッセージ**：302014、302016、302018
fo-standby	フェールオーバー スタンバイによりフローが終了しました。	スタンバイ状態のセキュリティ アプライアンスまたはコンテキストに through-the-box パケットが届くと、フローが作成され、そのパケットはドロップされ、作成されたフローは削除されます。このカウンタは、この方法でフローが削除されるたびに増分します。 **推奨事項**：アクティブなセキュリティ アプライアンスまたはコンテキスト上では、このカウンタが増分することはありません。ただし、スタンバイしているセキュリティ アプライアンスまたはコンテキスト上では、増分するのが普通です。 **システム ログ メッセージ**：302014、302016、302018

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
fo_rep_err	スタンバイ フローの複製エラー。	スタンバイ装置がフローの複製に失敗しました。 **推奨事項**：セキュリティ アプライアンスが VPN トラフィックを処理している場合は、IKE SA 情報よりも先にフローが複製されるため、このカウンタはスタンバイ装置上で常に増分しています。この場合、アクションは不要です。セキュリティ アプライアンスが VPN トラフィックを処理していない場合は、この表示はソフトウェアの検出を示しています。スタンバイ装置上で **debug fover fail** コマンドを実行し、デバッグ出力を収集し、この問題を Cisco TAC に報告してください。 **システム ログ メッセージ**：302014、302016、302018
host-removed	ホストが削除されました。	**clear local-host** コマンドに応答して、フローが削除されました。 **推奨事項**：これは情報カウンタです。 **システム ログ メッセージ**：302014、302016、302018、302021、305010、305012、609002
inspect-fail	検査が失敗しました。	セキュリティ アプライアンスが、接続のために NP によって行われるプロトコル検査をイネーブルにできなかった場合、このカウンタが増分します。原因として考えられるのは、メモリ割り当てが失敗したこと、または ICMP エラー メッセージの場合は、この ICMP エラー メッセージに埋め込まれているフレームに関連した確立済みの接続をセキュリティ アプライアンスが検出できなかったことです。 **推奨事項**：システム メモリの使用状況をチェックします。ICMP エラー メッセージに関しては、攻撃が原因の場合、ホストに対してアクセス リストを使用させないようにすることができます。 **システム ログ メッセージ**：ICMP エラーの場合 313004 です。
ips-fail-close	IPS が失敗して終了しました。	この理由は、AIP SSM がダウンしている状態で、fail-close オプションが IPS 検査で使用されたためにフローが終了したことによるものです。 **推奨事項**：AIP SSM をチェックしてから起動します。 **システム ログ メッセージ**：420001
ips-request	IPS によりフローが終了しました。	この理由は、AIP SSM の要求どおりにフローが終了したことによるものです。 **推奨事項**：システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420002

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ipsec-spoof-detect	IPsec スプーフ パケットが検出されました。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
loopback	フローがループバックしています。	この理由は、次のいずれかの状況により、フローが終了したことによるものです。 • U-turn トラフィックがフローに存在する。 • **same-security-traffic permit intra-interface** が設定されていない。 **推奨事項**：インターフェイス上で U-turn トラフィックを許可するには、そのインターフェイスを **same-security-traffic permit intra-interface** コマンドで設定します。 **システム ログ メッセージ**：なし。
mcast-entry-removed	マルチキャスト エントリが削除されました。	この理由は、次のいずれかの場合によるものです。 • マルチキャスト フローに一致するパケットが着信したが、マルチキャスト サービスがイネーブルでなくなっていた、またはマルチキャスト フローが作成された後で再度イネーブルにされた。 **推奨事項**：マルチキャストがディセーブルの場合は、再度イネーブルにします。 **システム ログ メッセージ**：なし。 • マルチキャスト エントリが削除されたのでフローもクリーンアップされるが、パケットはデータ パスに再び挿入される。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
mcast-intrf-removed	マルチキャスト インターフェイスが削除されました。	この理由は、次のいずれかの場合によるものです。 • 出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。 • すべての出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**：このグループに受信者が存在しないことを確認します。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
nat-failed	NAT が失敗しました。	IP を変換する、またはヘッダーを転送するための xlate の作成が失敗しました。 **推奨事項**：NAT が必要でない場合は、**nat-control** をディセーブルにします。そうでない場合は、**static**、**nat**、**global** のいずれかのコマンドを使用して、ドロップされたフローに NAT ポリシーを設定します。ダイナミック NAT では、各 **nat** コマンドが少なくとも 1 つの **global** コマンドとペアになっていることを確認します。NAT 規則を確認するには、**show running-config nat** と **debug pix process** を使用します。 **システム ログ メッセージ**:305005、305006、305009、305010、305011、305012
nat-rpf-failed	NAT 逆パスが失敗しました。	マッピングされたホストの実際のアドレスを使用してそのホストに接続しようとしましたが、拒否されました。 **推奨事項**：NAT を実施しているホストと同じインターフェイス上にない場合は、実際のアドレスの代わりにマッピング アドレスを使用してホストに接続します。また、アプリケーションが IP アドレスを埋め込む場合は、適切な **inspect** コマンドをイネーブルにします。 **システム ログ メッセージ**：305005
need-ike	IKE ネゴシエーションを開始する必要があります。	セキュリティ アプライアンスが、暗号化の必要があるのに IPSec セキュリティ アソシエーションを確立していないパケットを受信した場合、このカウンタが増分します。通常 LAN-to-LAN IPSec コンフィギュレーションでは、これは正常な状態です。これが表示されると、セキュリティ アプライアンスは宛先ピアとの ISAKMP ネゴシエーションを開始します。 **推奨事項**:セキュリティ アプライアンス上で IPSec LAN-to-LAN を設定している場合は、この表示は正常なもので、問題を示すものではありません。ただし、このカウンタが急速に増分する場合は、**crypto** の設定エラーまたはネットワーク エラーにより、ISAKMP ネゴシエーションが完了できないことを示している可能性があります。 宛先ピアと通信可能であることを確認し、**show running-config** コマンドを使用して **crypto** 設定を確認します。 **システム ログ メッセージ**：なし。
no-inspect	検査の割り当てに失敗。	このカウンタは、接続が確立されたときにセキュリティ アプライアンスがランタイム検査のデータ構造の割り当てに失敗すると増分します。接続はドロップされます。 **推奨事項**：このエラーの条件は、セキュリティ アプライアンスがシステム メモリを使い切ると発生します。**show memory** コマンドを発行して、使用可能な空きメモリをチェックします。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
no-ipv6-ipsec	IPsec over IPv6 はサポートされていません。	セキュリティ アプライアンスが、IPv6 ヘッダーでカプセル化された IPSec ESP パケット、IPSec NAT-T ESP パケット、または IPSec over UDP ESP パケットを受信した場合、このカウンタが増分します。現在セキュリティ アプライアンスは、IPv6 でカプセル化された IPSec セッションをサポートしていません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
non_tcp_syn	TCP が SYN 以外です。	この理由は、最初のパケットが SYN パケットではなかったために TCP フローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
out-of-memory	フローを完了するためのメモリがありません。	セキュリティ アプライアンスがメモリ不足のためにフローを作成できない場合、このカウンタが増分します。 **推奨事項**：現在の接続をチェックして、セキュリティ アプライアンスが攻撃を受けていないことを確認します。また、設定したタイムアウト値が大きすぎるために、アイドル状態のフローがメモリに長時間常駐していないかどうかも確認します。**show memory** コマンドを発行して、使用可能な空きメモリをチェックします。空きメモリが少ない場合は、**show processes memory** コマンドを発行し、メモリを大量に使用しているプロセスを特定します。 **システム ログ メッセージ**：なし。
parent-closed	親フローが終了しています。	下位フローの親フローが終了すると、その下位フローも終了します。たとえば、FTP データ制御フロー（親フロー）が終了すると、この理由により FTP データ フロー（下位フロー）も終了します。また、この理由は、制御アプリケーションによってセカンダリ フロー（pin-hole）が終了した場合にも該当します。たとえば、BYE メッセージを受信すると、SIP 検査エンジン（制御アプリケーション）は対応する SIP RTP フロー（セカンダリ フロー）を終了します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
pinhole-timeout	Pinhole のタイムアウト。	セキュリティ アプライアンスがセカンダリ フローを開始しましたが、タイムアウト間隔内にこのフローにパケットが渡されなかったためにフローが削除されたことを報告する場合、このカウンタが増分します。セカンダリ フローの例としては、FTP コントロール チャネル上でネゴシエーションの成功後に作成される FTP データ チャネルがあります。 **推奨事項**：なし。 **システム ログ メッセージ**：302014、302016

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
recurse	再帰的フローを終了します。	フローが再帰的に解放されました。この理由はペア フローとマルチキャスト スレーブ フローに該当し、これらの各下位フローに対するシステム メッセージは発行されません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
reinject-punt	パント アクションによりフローが終了しました。	検査や AAA などの強化されたサービスによって、処理のための例外パスにパケットがパントされた場合、このカウンタが増分します。このサービス ルーチンは、フロー上を流れるトラフィック内に違反を検出すると、そのフローをドロップするよう要求します。このフローはただちにドロップされます。 **推奨事項**：サービス ルーチンによってトリガーされるシステム メッセージに注意してください。フロー ドロップにより、対応する接続も終了します。 **システム ログ メッセージ**：なし。
reset-by-ips	IPS によりフローがリセットされました。	この理由は、AIP SSM の要求どおりに TCP フローが終了したことによるものです。 **推奨事項**：システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420003
reset-in	TCP リセット I。	この理由は、（セキュリティが低いインターフェイスからセキュリティが同じまたは高いインターフェイスへの）発信フロー上で TCP リセットを受信して、そのフローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：302014
reset-out	TCP リセット O。	この理由は、（セキュリティが高いインターフェイスからセキュリティが低いインターフェイスへの）着信フロー上で TCP リセットを受信して、そのフローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：302014
shunned	フローが排除されました。	排除データベース内にあるホストと一致する送信元 IP アドレスを持つパケットを受信した場合、このカウンタが増分します。**shun** コマンドが適用される場合、それぞれの既存のフローが **shun** コマンドに一致するたびに増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：401004

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ssl-bad-record-detect	SSL 不良レコードが検出されました。	このカウンタは、リモート ピアから不明の SSL レコード タイプを受信するたびに増分します。ピアから受信した不明のレコード タイプはすべて重大エラーとして処理され、このエラーが検出された SSL 接続は終了しなければなりません。 **推奨事項**: このカウンタが増分するのはどんなときでも正常でありません。このカウンタが増分する場合、通常、SSL プロトコルの状態がクライアント ソフトウェアと同期していないこと示します。この問題の原因として最も可能性があるのは、クライアント ソフトウェア内のソフトウェアの欠陥です。Cisco TAC にそのクライアント ソフトウェアまたは Web ブラウザのバージョンについて問い合せ、この問題を解決するために SSL データ交換のネットワーク トレースを提供してください。 **システム ログ メッセージ**：なし。
ssl-handshake-failed	SSL ハンドシェイクが失敗しました。	このカウンタは、SSL ハンドシェイクの失敗により TCP 接続がドロップすると増分します。 **推奨事項**: このカウンタは、SSL ハンドシェイクの失敗により TCP 接続がドロップしたことを示します。ハンドシェイク障害状況により生成されたシステム ログ メッセージ情報に基づいて問題が解決できない場合は、Cisco TAC に問い合せる際に、関連するシステム ログ メッセージ情報を提供してください。 **システム ログ メッセージ**：725006、725014
rm-xlate-limit	RM xlate 制限に達しました。	このカウンタは、あるコンテキストまたはシステムの xlate が最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-host-limit	RM ホスト制限に達しました。	このカウンタは、あるコンテキストまたはシステムのホストが最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-inspect-rate-limit	RM 検査レート制限に達しました。	このカウンタは、コンテキストまたはシステムの検査レートが最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321002

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ctm-crypto-request-error	CTM 暗号要求エラー。	このカウンタは、CTM が暗号要求を受け入れない場合に、その都度増分します。これは通常、暗号ハードウェア要求のキューがいっぱいになっていることを示します。 **推奨事項**：show crypto protocol statistics ssl コマンドを発行し、この情報を Cisco TAC に提供してください。 **システム ログ メッセージ**：なし。
ssl-record-decrypt-error	SSL レコード復号化が失敗しました。	このカウンタは、SSL データを受信中に復号化エラーが発生すると増分します。これは通常、ASA またはピアの SSL コードにバグがある場合、または攻撃者がデータ ストリームを変更している可能があることを示します。SSL 接続は終了されます。 **推奨事項**：ASA に対する SSL データ ストリームを検証します。攻撃者がいない場合は、Cisco TAC へ報告すべきソフトウェア エラーがあることを示します。 **システム ログ メッセージ**：なし。
np-socket-conn-not-accepted	新規のソケット接続が受け入れられませんでした。	このカウンタは、セキュリティ アプライアンスによって新規のソケット接続が受け入れられない場合に増分します。 **推奨事項**：このカウンタは、通常の動作が行われる過程で増分していく可能性があります。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。
np-socket-failure	NP ソケットの欠陥。	これは、重大なソケット処理エラーに対する一般的なカウンタです。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
np-socket-data-move-failure	NP ソケット データ移動エラー。	このカウンタは、ソケット データの移動時にエラーがあると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
np-socket-new-conn-failure	NP ソケットの新規接続エラー。	このカウンタは、ソケットの新規接続が失敗すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
np-socket-transport-closed	NP ソケット転送が終了しました。	このカウンタは、ソケットに関連する転送が異常終了すると増分します。 **推奨事項**：このカウンタは、通常の動作が行われる過程で増分していく可能性があります。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。
np-socket-block-conv-failure	NP ソケット ブロック変換エラー。	このカウンタは、ソケット ブロック変換エラーがあると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
ssl-received-close-alert	SSL が終了アラートを受信しました。	このカウンタは、セキュリティ アプライアンスがリモート クライアントから終了アラートを受信すると増分します。これは、クライアントが接続をドロップしようとしていることを通知したことを示します。通常の接続切断プロセスの一部です。 **推奨事項**：なし。 **システム ログ メッセージ**：725007
tracer-flow	packet-tracer がフローのドロップをトレースしました。	このカウンタは、トレースが完了して解放されたフローについて、packet-tracer により内部的に使用されます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
ssl-malloc-error	SSL の malloc のエラー。	このカウンタは、SSL ライブラリ内で malloc のエラーが発生すると増分します。これは、SSL がメモリ バッファまたはパケット ブロックを割り当てることができないメモリ不足状態であることを示します。 **推奨事項**：セキュリティ アプライアンスのメモリとパケット ブロックの状態を調べ、このメモリ情報を Cisco the TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ssm-app-fail	サービス モジュールが失敗しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。このカウンタは、SSM により検査中の接続が、SSM にエラーが生じたために終了すると増分します。 **推奨事項**：セキュリティ アプライアンスのコントロール プレーン内で動作しているカード マネージャ プロセスが、システム メッセージと CLI 警告を発行してこのエラーを通知します。SSM エラーの問題解決については、SSM に付属のマニュアルを参照してください。必要な場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：421001
ssm-app-incompetent	サービス モジュールが機能しませんでした。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。SSM による接続の検査が予定されているが、SSM が検査できない場合に増分します。このカウンタは将来使用するために予約されます。現在のリリースでは常に 0 である必要があります。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
ssm-app-request	サービス モジュールによりフローが終了しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。カウンタは、SSM で実行するアプリケーションがセキュリティ アプライアンスに接続を終了するよう要求すると増分します。 **推奨事項**：SSM によって生成された事故レポートまたはシステム メッセージを照会して、詳細情報を取得することができます。手順については、SSM に付属のマニュアルを参照してください。 **システム ログ メッセージ**：なし。
svc-failover	SVC ソケット接続がスタンバイ装置側で切断中です。	このカウンタは、アクティブ装置がフェールオーバー変遷の一部としてスタンバイ状態に移行するときに新規の SVC ソケット接続が切断されると増分します。 **推奨事項**：なし。これは、現在のデバイスがアクティブからスタンバイに移行する際の SVC 接続の通常のクリーンアップの一部です。デバイスでの既存の SVC 接続は有効でなるので、削除する必要があります。 **システム ログ メッセージ**：なし。
svc-spoof-detect	SVC スプーフ パケットが検出されました。	このカウンタは、暗号化されているはずが暗号化されていないパケットをセキュリティ アプライアンスが受信すると増分します。このパケットは、セキュリティ アプライアンスで設定、確立された SVC 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた SVC トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
syn-timeout	SYN のタイムアウト。	この理由は、初期タイマーが時間切れになったために TCP フローが終了したことによるものです。 **推奨事項**:接続の確立に時間のかかる有効なセッションがある場合は、初期タイムアウトを増分します。 **システム ログ メッセージ**：302014
tcp-fins	TCP FIN。	この理由は、TCP FIN パケットを受信した時に TCP フローが終了したことによるものです。 **推奨事項**：各 TCP 接続が FIN で正常に終了した場合、このカウンタが増分します。 **システム ログ メッセージ**：302014
tcp-intercept-no-response	TCP 代行受信サーバが応答しませんでした。	SYN 再送信は、1 秒に 1 回の割合で 3 回試行した後にタイムアウトになります。サーバが到達不能のため、接続が切断されました。 **推奨事項**：サーバがセキュリティ アプライアンスから到達可能であるかどうかをチェックします。 **システム ログ メッセージ**：なし。
tcp-intercept-kill	TCP 代行受信によりフローが終了しました。	次の理由により、TCP 代行受信が接続を切断しました。 **1.** これは最初の SYN である。 **2.** 接続が SYN 用に作成されている。 **3.** TCP 代行受信が SYN クッキーで応答した。または TCP 代行受信が SYN をサーバに送信し、サーバがクライアントからの有効な ACK を確認した後、RST で応答した。 **推奨事項**：ネイリング規則がある、パケットが VPN トンネル経由で着信する、またはクライアントに到達するネクストホップ ゲートウェイ アドレスが解決されない場合を除き、通常 TCP 代行受信では最初の SYN に対する接続は作成されません。そのため、これは最初の SYN に対して接続が作成されたことを示しています。TCP 代行受信がサーバから RST を受信すると、そのサーバ上の対応するポートが閉じる可能性があります。 **システム ログ メッセージ**：なし。
tcp-intercept-unexpected	TCP 代行受信の予期しない状態。	TCP 代行受信モジュールの論理エラーです。このようなことは発生しないようになっています。 **推奨事項**：メモリの破損、または TCP 代行受信モジュールの論理エラーを示しています。 **システム ログ メッセージ**：なし。
tcpmod-connect-clash	TCP モジュール ポート衝突がクライアントとサーバの間で発生しました。	TCP 接続ソケットは、既存のリッスン接続と衝突します。これは、内部システムのエラーです **推奨事項**：TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
tcpnorm-invalid-syn	TCP の無効な SYN。	この理由は、SYN パケットが無効の場合に TCP フローが終了したことによるものです。 **推奨事項**：チェックサムや TCP ヘッダーが無効な場合など、さまざまな理由で SYN パケットが無効になる可能性があります。なぜ SYN パケットが無効になるかを理解するには、パケット キャプチャ機能を使用してください。これらの接続を許可する場合は、**tcp-map** 設定を使用してチェックをバイパスします。 **システム ログ メッセージ**：302014
tcpnorm-rexmit-bad	TCP の不正な再送信。	この理由は、**check-retransmission** 機能がイネーブルになっている時に、TCP エンドポイントから元のパケットと異なるデータが再送信されて TCP フローが終了したことによるものです。 **推奨事項**：TCP の再送信の際に異なるデータを送信するという方法で、TCP エンドポイントが攻撃を加えている可能性があります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：302014
tcpnorm-win-variation	TCP の予期しない、さまざまなウィンドウ サイズ。	この理由は、TCP エンドポイントにアドバタイズされたウィンドウ サイズが、大量のデータを受け取ることもなく激変し、TCP フローが終了したことによるものです。 **推奨事項**：この接続を許可するために、**window-variation** コマンドを使用します。 **システム ログ メッセージ**：302014
timeout	接続のタイムアウト。	非アクティビティ タイマーの期限切れのためフローが終了した場合、このカウンタが増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：302014、302016、302018、302021
tunnel-pending	トンネルを確立または切断しています。	セキュリティ アプライアンスがセキュリティ ポリシー データベース（たとえば **crypto map**）のエントリに一致するパケットを受信したが、セキュリティ アソシエーションがネゴシエーションの途中でまだ完了していない場合、このカウンタが増分します。 また、セキュリティ アプライアンスがセキュリティ ポリシー データベースのエントリに一致するパケットを受信したが、セキュリティ アソシエーションが削除された、または削除中である場合にも、このカウンタが増分します。この表示と「Tunnel has been torn down（トンネルが切断されました。）」表示の違いは、「Tunnel has been torn down（トンネルが切断されました。）」表示は確立済みのフロー用であるということです。 **推奨事項**：IPSec トンネルがネゴシエーション中または削除中の場合、これは正常な状態です。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
tunnel-torn-down	トンネルが切断されました。	セキュリティ アプライアンスが、IPSec セキュリティ アソシエーションが削除中の確立済みフローに関連付けられたパケットを受信した場合、このカウンタが増分します。 **推奨事項**：IPSec トンネルが何らかの理由で切断された場合、これは正常な状態です。 **システム ログ メッセージ**：なし。
xlate-removed	Xlate の消去。	**clear xlate** コマンドまたは **clear local-host** コマンドに応答して、フローが削除されました。 **推奨事項**：これは情報カウンタです。 **システム ログ メッセージ**:302014、302016、302018、302021、305010、305012、609002

例

次に、**show asp drop** コマンドの出力例を示します。

```
hostname# show asp drop

Frame drop:
  Invalid encapsulation                                10897
  Invalid tcp length                                    9382
  Invalid udp length                                      10
  No valid adjacency                                    5594
  No route to host                                      1009
  Reverse-path verify failed                              15
  Flow is denied by access rule                       25247101
  First TCP packet not SYN                              36888
  Bad TCP flags                                         67148
  Bad option length in TCP                                731
  TCP MSS was too large                                 10942
  TCP Window scale on non-SYN                            2591
  Bad TCP SACK ALLOW option                               224
  TCP Dual open denied                                     11
  TCP data send after FIN                                  62
  TCP failed 3 way handshake                           328859
  TCP RST/FIN out of order                             258871
  TCP SEQ in SYN/SYNACK invalid                           142
  TCP ACK in SYNACK invalid                               278
  TCP packet SEQ past window                            46331
  TCP invalid ACK                                     1234749
  TCP packet buffer full                             90009943
  TCP RST/SYN in window                                 43136
  TCP DUP and has been ACKed                           927075
  TCP packet failed PAWS test                            9907
  Early security checks failed                              3
  Slowpath security checks failed                          19
  DNS Inspect invalid packet                             1097
  DNS Inspect invalid domain label                         10
  DNS Inspect packet too long                               5
  DNS Inspect id not matched                             8270
  FP L2 rule drop                                         783
  FP no mcast output intrf                                  5
  Interface is down                                      3881
  Non-IP packet received in routed mode                   158

Flow drop:
  Flow is denied by access rule                            24
  NAT failed                                            28739
  NAT reverse path failed                               22266
  Inspection failure                                    19433
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp ドロップ コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	アクセラレーション セキュリティ パスのドロップ統計情報を消去します。
show conn	接続に関する情報を表示します。

show asp table arp

アクセラレーション セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

シンタックスの説明

address*ip_address*	（オプション）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（オプション）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（オプション）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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

show arp コマンドが制御プレーンの内容を表示するのに対して、**show asp table arp** コマンドはアクセラレーション セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

アクセラレーション セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類規則と対応付けます。それぞれの規則には、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。

show asp table classify [**crypto** | **domain** *domain_name* | **interface** *interface_name*]

シンタックスの説明

domain *domain_name*	（オプション）特定の分類子ドメインのエントリを表示します。ドメインのリストについては、「使用上のガイドライン」を参照してください。
interface *interface_name*	（オプション）分類子テーブルを表示する特定のインターフェイスを指定します。
crypto	（オプション）encrypt ドメイン、decrypt ドメイン、および ipsec-tunnel-flow ドメインのみを表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

show asp table classify コマンドは、アクセラレーション セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

分類子ドメインには、次のものがあります。

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
l2tp
l2tp-ppp
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
```

```
priority-q
punt
punt-l2
punt-root
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show asp table interfaces

アクセラレーション セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

show asp table interfaces コマンドは、アクセラレーション セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show asp table mac-address-table

アクセラレーション セキュリティ パスの MAC アドレス テーブルをデバッグするには、特権 EXEC モードで **show asp table mac-address-table** コマンドを使用します。

show asp table mac-address-table [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）特定のインターフェイスの MAC アドレス テーブルを表示します。

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。

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

コマンド履歴

リリース	変更内容
7.0(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

show asp table mac-address-table コマンドは、アクセラレーション セキュリティ パスの MAC アドレス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table mac-address-table** コマンドの出力例を示します。

```
hostname# show asp table mac-address-table

interface                  mac  address       flags
-------------------------------------------------------
    inside1                     0009.b74d.3800     None
    inside1                     0007.e903.ad6e     None
    inside1                     0007.e950.2067     None
    inside1                     0050.0499.3749     None
    inside1                     0012.d96f.e200     None
    inside1                     0001.02a7.f4ec     None
    inside1                     0001.032c.6477     None
    inside1                     0004.5a2d.a1c8     None
    inside1                     0003.4773.c87b     None
    inside1                     000d.88ef.5d1c     None
    inside1                     00c0.b766.adce     None
    inside1                     0050.5640.450d     None
    inside1                     0001.03cf.0431     None
...
```

関連コマンド

コマンド	説明
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show asp table routing

アクセラレーション セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show asp table routing [**input** | **output**] [**address** *ip_address* [***netmask*** *mask*] | **interface** *interface_name*]

シンタックスの説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、サブネット マスクを含めることができます。スラッシュ（/）に続けて、プレフィックス（0 ～ 128）を入力します。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（オプション）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合に、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

show asp table routing コマンドは、アクセラレーション セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

関連コマンド

コマンド	説明
show route	制御プレーン内のルーティング テーブルを表示します。

show asp table vpn-context

アクセラレーション セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

シンタックスの説明

detail	（オプション）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

show asp table vpn-context コマンドは、アクセラレーション セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

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

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{***address*** *hex* | ***all*** | ***assigned*** | ***free*** | ***old*** | ***pool*** *size* [***summary***]} [**diagnostics** | ***dump*** | ***header*** | ***packet***] | ***queue history*** [***detail***]]

シンタックスの説明

address *hex*	（オプション）このアドレスに対応するブロックを 16 進形式で表示します。
all	（オプション）すべてのブロックを表示します。
assigned	（オプション）アプリケーションによって割り当てられ、使用されているブロックを表示します。
detail	（オプション）一意の各キュー タイプの最初のブロックの一部（128 バイト）を表示します。
dump	（オプション）ヘッダーとパケットの情報を含めて、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（オプション）ブロックに関する診断を表示します。
free	（オプション）使用可能なブロックを表示します。
header	（オプション）ブロックのヘッダーを表示します。
old	（オプション）1 分より前に割り当てられたブロックを表示します。
packet	（オプション）パケットの内容をブロックのヘッダーと共に表示します。
pool *size*	（オプション）特定のサイズのブロックを表示します。
queue history	（オプション）セキュリティ アプライアンスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。ブロックはプールから割り当てられますが、一度もキューに割り当てられないことがあります。この場合に表示される位置は、ブロックを割り当てたコードのアドレスです。
summary	（オプション）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。

使用上のガイドライン

show blocks コマンドは、セキュリティ アプライアンスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックがセキュリティ アプライアンスを経由して移動している限り、メモリがすべて使用されている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが移動しているかどうかを確認できます。トラフィックが移動していないで、かつメモリがすべて使用されている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の最高水準点について、コンテキスト固有の情報と共にシステム全体の情報も含まれています。

表示される出力については、「例」の項を参照してください。

例

次に、シングルモードでの **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
  SIZE    MAX    LOW    CNT
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

表 25-3 に、各フィールドの説明を示します。

表 25-3　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。下に例を示します。
4	DNS モジュール、ISAKMP モジュール、URL フィルタリング モジュール、uauth モジュール、TFTP モジュール、TCP モジュールなどのアプリケーションの既存ブロックを複製します。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。

表 25-3　show blocks のフィールド（続き）

フィールド	説明
256	ステートフル フェールオーバーのアップデート、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブなセキュリティ アプライアンスは、パケットを生成してスタンバイ セキュリティ アプライアンスに送信し、変換と接続のテーブルをアップデートします。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイ セキュリティ アプライアンスに対してアップデートされなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、セキュリティ アプライアンスの処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態をセキュリティ アプライアンスが維持できない問題が発生しています。 セキュリティ アプライアンスから送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバに記録していないことを確認してください。この情報は、セキュリティ アプライアンス コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することをお勧めします。
1550	セキュリティ アプライアンスで処理するイーサネット パケットを格納するために使用されます。 パケットは、セキュリティ アプライアンス インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。セキュリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを出力インターフェイス上の出力キューに配置します。セキュリティ アプライアンスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT カラムに示されます）。CNT カラムが 0 になると、セキュリティ アプライアンスはさらにブロックを確保しようとします（最大で 8,192 個まで）。使用可能なブロックがなくなった場合、セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御アップデートに使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。ブロックの最大数は、ブートアップ時にメモリに基づいて配分されます。ブロックの最大数は、通常は変化しません。例外は 256 バイト ブロックと 1,550 バイト ブロックで、セキュリティ アプライアンスはこれらのブロックを必要に応じて動的に作成できます（最大で 8,192 個まで）。

表 25-3　show blocks のフィールド（続き）

フィールド	説明
LOW	最低水準点。この数は、セキュリティ アプライアンスの電源がオンになった時点、またはブロックの内容が（**clear blocks** コマンドで）最後に消去された時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがすべて使用されたことを示します。
CNT	指定したサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在すべて使用されていることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc
not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 25-4 に、各フィールドの説明を示します。

表 25-4　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。割り当て、取得、入力、解放の 4 つのいずれかです。
location	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

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

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

表 25-5 に、各フィールドの説明を示します。

表 25-5　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリで報告されなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されてコンテンツが無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられているメモリを増やします。
clear blocks	システム バッファの統計情報を消去します。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権コンフィギュレーション モードで ***show bootvar*** コマンドを使用します。

show bootvar

シンタックスの説明

show bootvar	システムのブート プロパティ。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定するものです。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ ***boot system*** コマンドと ***boot config*** コマンドで設定します。

例

次の例では、BOOT 変数が disk0:/f1_image を保持しています。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:f1_backupimage です。これは、BOOT 変数が boot system コマンドで変更されているものの、実行コンフィギュレーションがまだ ***write memory*** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブート ローダーは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションをポイントします。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、***boot config*** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、***boot config*** コマンドで変更して、***write memory*** コマンドで保存することができます。

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show capture

キャプチャのコンフィギュレーションを表示するには、オプションを指定せずに **show capture** コマンドを使用します。

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

シンタックスの説明

capture_name	（オプション）パケット キャプチャの名前。
access-list *access_list_name*	（オプション）特定のアクセス リストの IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
count *number*	（オプション）指定したパケットの数に関するデータを表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する isakmp データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報と共に表示されます。
detail	（オプション）各パケットの詳細なプロトコル情報を表示します。
dump	（オプション）データ リンク トランスポート経由で伝送されるパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

セキュリティ コンテキスト モード: シングル コンテキスト モードおよびマルチ コンテキスト モード

アクセス場所：システムおよびコンテキストのコマンドライン

コマンド モード：特権モード

ファイアウォール モード : ルーテッド ファイアウォール モードおよび透過ファイアウォール モード

コマンド履歴

リリース	変更内容
7.0(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

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC に関する情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって形式が異なります。表 25-6 で [ ] に囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 25-6　パケット キャプチャの出力形式

パケットのタイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*

表 25-6　パケット キャプチャの出力形式（続き）

パケットのタイプ	キャプチャの出力形式
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/ その他	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
その他	*HH:MM:SS.ms ether-hdr*: *hex-dump*

例

次の例は、キャプチャのコンフィギュレーションを表示する方法を示しています。

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次の例は、ARP キャプチャによってキャプチャされたパケットを表示する方法を示しています。

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファを消去します。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show chardrop** コマンドの出力例を示します。

```
hostname# show chardrop
```

Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0

関連コマンド

コマンド	説明
show running-config	現在の実行コンフィギュレーションを表示します。

show checkheaps

チェックヒープに関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ピープ メモリ バッファ（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられる）の健全性およびコード領域の完全性を確認する定期的なプロセスです。

show checkheaps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

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

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	チェックヒープの確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 16 進数の 4 つのグループを表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（セキュリティ アプライアンス フラッシュ パーティションからの読み込み、またはセキュリティ アプライアンス フラッシュ パーティションへの書き込み時）。「.」は、セキュリティ アプライアンスが処理に占有されているが「ハングアップ」していないことを示しています。このメッセージは、「system processing, please wait」メッセージと同様です。

例

次の例は、コンフィギュレーションまたはチェックサムを表示する方法を示しています。

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、チャンクに関する統計情報を表示する方法を示しています。

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

シンタックスの説明

name	20 文字までの長さの文字列として名前を指定します。デフォルト クラスを表示するには、名前として **default** と入力します。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

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

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションを消去します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスに対してリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。

show clock

セキュリティ アプライアンス上の時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

シンタックスの説明

detail	（オプション）クロックのソース（NTP またはユーザ設定）と現在のサマータイム設定（存在する場合）を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show clock** コマンドの出力例を示します。

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

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

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show compression svc

SVC 接続の圧縮統計情報をセキュリティ アプライアンス上に表示するには、特権 EXEC モードで **show compression svc** コマンドを使用します。

show compression svc

デフォルト

このコマンドには、デフォルトの動作はありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

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

```
hostname# show compression svc
Compression SVC Sessions                        1
Compressed Frames                          249756
Compressed Data In (bytes)                0048042
Compressed Data Out (bytes)               4859704
Expanded Frames                                 1
Compression Errors                              0
Compression Resets                              0
Compression Output Buf Too Small                0
Compression Ratio                            2.06
Decompressed Frames                        876687
Decompressed Data In                     279300233
```

関連コマンド

コマンド	説明
compression	すべての SVC および WebVPN 接続の圧縮をイネーブルにします。
svc compression	SVC 接続上の http データの圧縮を特定のグループまたはユーザに対してイネーブルにします。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show conn [**all** | **count**] [**state** *state_type*] | [{{**foreign** | **local**} *ip* [*-ip2*] **netmask** *mask*}] | [**long** | ***detail***] | [{{**lport** | **fport**} *port1*} [*-port2*]] | [**protocol** {**tcp** | **udp**}]

シンタックスの説明

all	デバイスを通過するトラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（オプション）アクティブな接続の数を表示します。
detail	変換タイプとインターフェイスの情報を含めて、接続の詳細を表示します。
foreign	指定した外部 IP アドレスとの接続を表示します。
fport	指定した外部ポートとの接続を表示します。
ip	ドット付き 10 進表記の IP アドレス。または、IP アドレス範囲の開始アドレス。
-ip2	（オプション）IP アドレス範囲の終了 IP アドレス。
local	指定したローカル IP アドレスとの接続を表示します。
long	（オプション）接続をロング フォーマットで表示します。
lport	指定したローカル ポートとの接続を表示します。
netmask	指定した IP アドレスに使用するサブネット マスクを指定します。
mask	ドット付き 10 進表記のサブネット マスク。
port1	ポート番号。または、ポート番号範囲の開始ポート番号。
-port2	（オプション）ポート番号範囲の終了ポート番号。
protocol	（オプション）接続プロトコルを指定します。
state	（オプション）指定した接続の状態を表示します。
state_type	接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 25-7 を参照してください。
tcp	TCP プロトコル接続を表示します。
udp	UDP プロトコル接続を表示します。

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。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注）　セカンダリ接続を可能にするためのピンホールをセキュリティ アプライアンスが作成するとき、この接続は **show conn** コマンドでは不完全な接続として表示されます。この不完全な接続を消去するには、**clear local** コマンドを使用します。

表 25-7 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。

表 25-7　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ検査エンジン接続

detail オプションを使用すると、表 25-8 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

表 25-8　接続フラグ

フラグ	説明
a	SYN に対する外部 ACK（確認応答）を待機
A	SYN に対する内部 ACK（確認応答）を待機
B	外部からの初期 SYN
C	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）メディア接続
d	ダンプ
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN

表 25-8　接続フラグ（続き）

フラグ	説明
g	Media Gateway Control Protocol（MGCP）接続
G	接続がグループの一部[1]
h	H.225
H	H.323
i	不完全な TCP または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製（未使用）
P	内部バック接続
q	SQL*Net データ
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC[2]
s	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続[3]
T	SIP 接続[4]
U	アップ
X	CSC SSM などのサービス モジュールに検査される。

1. G フラグは、接続がグループの一部であることを示します。GRE および FTP の Strict フィックスアップによって設定され、制御接続と関連するすべてのセカンダリ接続を指定します。制御接続が終了すると、関連するすべてのセカンダリ接続も終了します。
2. **show conn** コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
3. UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
4. UDP 接続の場合、値 T は、**timeout sip** コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。

（注） DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS の識別情報は、*app_id* によって追跡され、各 app_id のアイドル タイマーはそれぞれ独立して動作します。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注）　**conn timeout** コマンドで定義した非アクティブ期間（デフォルトは 01:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

例

複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。次の例では、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示しています。

```
hostname# show conn state up,rpc,h323,sip
```

次の例は、内部ホスト 10.1.1.15 から 192.168.49.10 の外部 Telnet サーバへの TCP セッション接続を示しています。B フラグが存在しないため、接続は内部から開始されています。「U」フラグ、「I」フラグ、および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示しています。

```
hostname# show conn
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

次の例には、接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
hostname(config)# show conn local 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03 bytes 2733 flags UIOX
```

次の例は、外部ホスト 192.168.49.10 から内部ホスト 10.1.1.15 への UDP 接続を示しています。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
hostname(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIBQE media, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, g - MGCP, H - H.323, h - H.255.0, I - inbound data, i - incomplete,
       k - Skinny media, M - SMTP data, m - SIP media
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
       X - inspected by service module
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

次に、**show conn all** コマンドの出力例を示します。

```
hostname# show conn all
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
  UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
  UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
  UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

例では、内部のホスト 10.3.3.4 が 209.165.201.1 の Web サイトにアクセスしています。外部インターフェイス上のグローバル アドレスは、209.165.201.7 です。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
inspect sip	Java アプレットを HTTP トラフィックから削除します。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、コンソール出力がない場合に表示されるメッセージを示しています。

```
hostname# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションにあるアイドル期間をデフォルトに戻します。
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

show context

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 ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

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

シンタックスの説明

count	（オプション）設定済みコンテキストの数を表示します。
detail	（オプション）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（オプション）コンテキスト名を設定します。名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。

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。

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

コマンド履歴

リリース	変更内容
7.0(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

表示される出力については、「例」の項を参照してください。

例

次に、**show context** コマンドの出力例を示します。この表示例では、3 つのコンテキストが表示されています。

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 25-9 に、各フィールドの説明を示します。

表 25-9　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一覧表示されます。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。
Interfaces	コンテキストに割り当てられるインターフェイス。
URL	セキュリティ アプライアンス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。

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/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
```

表 25-10 に、各フィールドの説明を示します。

表 25-10　コンテキストの状態

フィールド	説明
コンテキスト	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
（状態メッセージ）	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。

表 25-10　コンテキストの状態（続き）

フィールド	説明
Has been created, but initial ACL rules not complete	セキュリティ アプライアンスはコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、セキュリティ レベルの低い方から高い方に向かうトラフィックを拒否し、アプリケーション検査およびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックがセキュリティ アプライアンスを一切通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだセキュリティ アプライアンスがコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、空白の実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Real Interfaces	コンテキストに割り当てられるインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はインターフェイスの実際の名前を示しています。システム実行スペースは、すべてのインターフェイスを含んでいます。

表 25-10　コンテキストの状態（続き）

フィールド	説明
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はマッピングされた名前を示しています。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

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

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

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。

show controller

ASA 5505 適応型セキュリティ アプライアンスのシステムに存在するすべてのインターフェイスのコントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [*switch_port*]

シンタックスの説明

switch_port	（オプション）インターフェイス ID を特定します（**ethernet0/0** ～ **ethernet0/7**）。

デフォルト

スイッチ ポートを特定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(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

Cisco TAC では、このコマンドを使用して内部で見つかった欠陥や、顧客が見つけた欠陥を調査する際にコントローラに関するデバッグ情報を収集します。

例

次に、**show controller** コマンドの出力例を示します。

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482
```

```
-------------------------------------------------------------------
Number of VLANs: 1
-------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
-------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-------------------------------------------------------------------

Ethernet0/1:
   Marvell 88E6095 revision 2, switch port 6
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x0130
         PHY Status:    0x0040  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07bf
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0040
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/2:
   Marvell 88E6095 revision 2, switch port 5
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07df
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0020
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/3:
   Marvell 88E6095 revision 2, switch port 4
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07ef
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0010
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
```

```
Ethernet0/4:
   Marvell 88E6095 revision 2, switch port 3
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07f7
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0008
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/5:
   Marvell 88E6095 revision 2, switch port 2
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fb
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0004
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
```

```
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Ethernet0/7:
   Marvell 88E6095 revision 2, switch port 0
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fe
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0001
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:
    mac_addr1_lo                  0xe0004100 = 0x00000000
    mac_addr1_hi                  0xe0004104 = 0x00000000
    mac_addr2_lo                  0xe0004108 = 0x00000000
    mac_addr2_hi                  0xe000410c = 0x00000000
    mac_addr3_lo                  0xe0004110 = 0x00000000
    mac_addr3_hi                  0xe0004114 = 0x00000000
    chip_info                     0xe0004118 = 0xb0110000
    eprom                         0xe000411c = 0x00000000
    flash_addr_reg                0xe0004120 = 0x0001fffe
    flash_data_port               0xe0004124 = 0x000000ff
```

```
 loader                          0xe0004128 = 0x00000400
 timer_init_val                  0xe0004130 = 0x00000000
 timer_val                       0xe0004134 = 0x00000000
 timer_ctrl                      0xe0004138 = 0x00000202
 irq_mod_timer_init_val          0xe0004140 = 0x00000000
 irq_mod_timer                   0xe0004144 = 0x00000000
 irq_mod_timer_ctrl              0xe0004148 = 0x00000202
 irq_mod_msk                     0xe000414c = 0x00000000
 irq_hw_err_mod_mask             0xe0004150 = 0x00000000
 tst_ctrl                        0xe0004158 = 0x00000001
 gp_io                           0xe000415c = 0x0000000f
 i2c_ctrl                        0xe0004160 = 0x00000000
 i2c_data                        0xe0004164 = 0x00000000
 i2c_irq                         0xe0004168 = 0x00000000
 i2c_sw                          0xe000416c = 0x00000003

RAM Random Registers:
 ram_addr                        0xe0004180 = 0x00000000
 ram_data_port_lo                0xe0004184 = 0x00000000
 ram_data_port_hi                0xe0004188 = 0x00000000

Ram Interface Registers:
 ram_if_to_lo                    0xe0004190 = 0x24242424
 ram_if_to_hi                    0xe0004194 = 0x00002424
 ram_if_timeout_val              0xe000419c = 0x00000000
 ram_if_ctrl                     0xe00041a0 = 0x000a0002

Transmit Arbiter MAC:
 tx_arb_iti_init                 0xe0004200 = 0x00000000
 tx_arb_iti_val                  0xe0004204 = 0x00000000
 tx_arb_lim_init                 0xe0004208 = 0x00000000
 tx_arb_lim_val                  0xe000420c = 0x00000000
 tx_arb_ctrl_tst_status          0xe0004210 = 0x00001256

Bank 8: Receive queue registers:
 rx_qregs.buf_ctrl               0xe0004400 = 0xc8550800
 rx_qregs.next_desc_addr_lo      0xe0004404 = 0x016d4020
 rx_qregs.buf_addr_lo            0xe0004408 = 0x019acd00
 rx_qregs.buf_addr_hi            0xe000440c = 0x00000000
 rx_qregs.frame_sw               0xe0004410 = 0x00000000
 rx_qregs.time_stamp             0xe0004414 = 0x00000000
 rx_qregs.tcp_csum               0xe0004418 = 0x00000000
 rx_qregs.tcp_csum_start         0xe000441c = 0x00000000
 rx_qregs.desc_addr_lo           0xe0004420 = 0x016d4000
 rx_qregs.desc_addr_hi           0xe0004424 = 0x00000000
 rx_qregs.addr_cntr_lo           0xe0004428 = 0x016d4020
 rx_qregs.addr_cntr_hi           0xe000442c = 0x00000000
 rx_qregs.byte_cntr              0xe0004430 = 0x00000000
 rx_qregs.bmu_cs                 0xe0004434 = 0x002aaa80
 rx_qregs.flag                   0xe0004438 = 0x00000600
 rx_qregs.tst1                   0xe000443c = 0xd2020202
 rx_qregs.tst2                   0xe0004440 = 0x00000050
 rx_qregs.tst3                   0xe0004444 = 0x00000000

Bank 12: Synchronous transmit queue registers:
 stx_qregs.buf_ctrl              0xe0004600 = 0x00000000
 stx_qregs.next_desc_addr_lo     0xe0004604 = 0x00000000
 stx_qregs.buf_addr_lo           0xe0004608 = 0x00000000
 stx_qregs.buf_addr_hi           0xe000460c = 0x00000000
 stx_qregs.frame_sw              0xe0004610 = 0x00000000
 stx_qregs.time_stamp            0xe0004614 = 0x00000000
 stx_qregs.tcp_csum              0xe0004618 = 0x00000000
 stx_qregs.tcp_csum_start        0xe000461c = 0x00000000
 stx_qregs.desc_addr_lo          0xe0004620 = 0x00000000
 stx_qregs.desc_addr_hi          0xe0004624 = 0x00000000
 stx_qregs.addr_cntr_lo          0xe0004628 = 0x00000000
 stx_qregs.addr_cntr_hi          0xe000462c = 0x00000000
 stx_qregs.byte_cntr             0xe0004630 = 0x00000000
 stx_qregs.bmu_cs                0xe0004634 = 0x01155540
```

```
 stx_qregs.flag                0xe0004638 = 0x0a000600
 stx_qregs.tst1                0xe000463c = 0x02020202
 stx_qregs.tst2                0xe0004640 = 0x00000050
 stx_qregs.tst3                0xe0004644 = 0x00000000

Bank 13: Asynchronous transmit queue registers:
 atx_qregs.buf_ctrl            0xe0004680 = 0x00000000
 atx_qregs.next_desc_addr_lo   0xe0004684 = 0x00000000
 atx_qregs.buf_addr_lo         0xe0004688 = 0x00000000
 atx_qregs.buf_addr_hi         0xe000468c = 0x00000000
 atx_qregs.frame_sw            0xe0004690 = 0x00000000
 atx_qregs.time_stamp          0xe0004694 = 0x00000000
 atx_qregs.tcp_csum            0xe0004698 = 0x00000000
 atx_qregs.tcp_csum_start      0xe000469c = 0x00000000
 atx_qregs.desc_addr_lo        0xe00046a0 = 0x016d9000
 atx_qregs.desc_addr_hi        0xe00046a4 = 0x00000000
 atx_qregs.addr_cntr_lo        0xe00046a8 = 0x016d901c
 atx_qregs.addr_cntr_hi        0xe00046ac = 0x00000000
 atx_qregs.byte_cntr           0xe00046b0 = 0x00000000
 atx_qregs.bmu_cs              0xe00046b4 = 0x012aaa80
 atx_qregs.flag                0xe00046b8 = 0x0a000600
 atx_qregs.tst1                0xe00046bc = 0x02020202
 atx_qregs.tst2                0xe00046c0 = 0x00000050
 atx_qregs.tst3                0xe00046c4 = 0x00000000

Bank 16: Receive RAM buffer registers:
 rx_ram_buf_regs.start_addr    0xe0004800 = 0x00000000
 rx_ram_buf_regs.end_addr      0xe0004804 = 0x000017ff
 rx_ram_buf_regs.wr_ptr        0xe0004808 = 0x00000000
 rx_ram_buf_regs.rd_ptr        0xe000480c = 0x00000000
 rx_ram_buf_regs.up_thres_pp   0xe0004810 = 0x00001400
 rx_ram_buf_regs.lo_thres_pp   0xe0004814 = 0x00001000
 rx_ram_buf_regs.up_thres_hp   0xe0004818 = 0x00000000
 rx_ram_buf_regs.lo_thres_hp   0xe000481c = 0x00000000
 rx_ram_buf_regs.pak_cnt       0xe0004820 = 0x00000000
 rx_ram_buf_regs.level         0xe0004824 = 0x00000000
 rx_ram_buf_regs.ctrl          0xe0004828 = 0x0002222a

Bank 20: Synchronous transmit RAM buffer registers:
 stx_ram_buf_regs.start_addr   0xe0004a00 = 0x00000000
 stx_ram_buf_regs.end_addr     0xe0004a04 = 0x00000000
 stx_ram_buf_regs.wr_ptr       0xe0004a08 = 0x00000000
 stx_ram_buf_regs.rd_ptr       0xe0004a0c = 0x00000000
 stx_ram_buf_regs.pak_cnt      0xe0004a20 = 0x00000000
 stx_ram_buf_regs.level        0xe0004a24 = 0x00000000
 stx_ram_buf_regs.ctrl         0xe0004a28 = 0x00022215

Bank 21: Asynchronous transmit RAM buffer registers:
 atx_ram_buf_regs.start_addr   0xe0004a80 = 0x00001800
 atx_ram_buf_regs.end_addr     0xe0004a84 = 0x00002fff
 atx_ram_buf_regs.wr_ptr       0xe0004a88 = 0x00001800
 atx_ram_buf_regs.rd_ptr       0xe0004a8c = 0x00001800
 atx_ram_buf_regs.up_thres_pp  0xe0004a90 = 0x00000000
 atx_ram_buf_regs.lo_thres_pp  0xe0004a94 = 0x00000000
 atx_ram_buf_regs.up_thres_hp  0xe0004a98 = 0x00000000
 atx_ram_buf_regs.lo_thres_hp  0xe0004a9c = 0x00000000
 atx_ram_buf_regs.pak_cnt      0xe0004aa0 = 0x00000000
 atx_ram_buf_regs.level        0xe0004aa4 = 0x00000000
 atx_ram_buf_regs.ctrl         0xe0004aa8 = 0x0002222a

Bank 24: Receive GMAC FIFO registers:
 rx_gmfifo_regs.end_addr       0xe0004c40 = 0x0000007f
 rx_gmfifo_regs.thr            0xe0004c44 = 0x00000070
 rx_gmfifo_regs.ctrl           0xe0004c48 = 0x0000224a

Bank 26: Transmit GMAC FIFO registers:
 tx_gmfifo_regs.end_addr       0xe0004d40 = 0x0000007f
 tx_gmfifo_regs.thr            0xe0004d44 = 0x00000010
 tx_gmfifo_regs.ctrl           0xe0004d48 = 0x0002220a
```

```
    tx_gmfifo_regs.wr_ptr         0xe0004d60 = 0x00000000
    tx_gmfifo_regs.wr_shdw_ptr    0xe0004d64 = 0x00000000
    tx_gmfifo_regs.wr_level       0xe0004d68 = 0x00000000
    tx_gmfifo_regs.rd_ptr         0xe0004d70 = 0x00000000
    tx_gmfifo_regs.restart_ptr    0xe0004d74 = 0x00000000
    tx_gmfifo_regs.rd_level       0xe0004d78 = 0x00000000

  Descriptor poll timer registers:
    dpt_init_val                  0xe0004e00 = 0x00000000
    dpt_val                       0xe0004e04 = 0x00000000
    dpt_ctrl                      0xe0004e08 = 0x00020001

  Timestamp timer register:
    ts_timer_val                  0xe0004e14 = 0x00000000
    ts_timer_ctrl                 0xe0004e18 = 0x00000202

  GMAC and GPHY control registers:
    gmac_ctrl                     0xe0004f00 = 0x00000056
    gphy_ctrl                     0xe0004f04 = 0x0b7de002
    gmac_irq_src                  0xe0004f08 = 0x00000000
    gmac_irq_msk                  0xe0004f0c = 0x0000003a
    gmac_link_ctrl                0xe0004f10 = 0x00000002

  Wake on LAN control registers:
    wol_ctrl                      0xe0004f20 = 0x00000555
    wol_mac_addr_lo               0xe0004f24 = 0x00000000
    wol_mac_addr_hi               0xe0004f28 = 0x00000000
    wol_patt_rd_ptr               0xe0004f2c = 0x00000000
    wol_patt_len_lo               0xe0004f30 = 0x3b3b3b3b
    wol_patt_len_hi               0xe0004f34 = 0x003b3b3b
    wol_patt_cnt_lo               0xe0004f38 = 0x00000000
    wol_patt_cnt_hi               0xe0004f3c = 0x00000000

  Bank 80 (0x50): GMAC registers:
    gmac_gpsr                     0xe0006800 = 0x0000f014
    gmac_gpcr                     0xe0006804 = 0x000038ff
    gmac_tx_ctrl                  0xe0006808 = 0x00001c00
    gmac_rx_ctrl                  0xe000680c = 0x0000a000
    gmac_tx_fctrl                 0xe0006810 = 0x0000ffff
    gmac_tx_parm                  0xe0006814 = 0x0000c000
    gmac_smod                     0xe0006818 = 0x00002306
    gmac_sa1_lo                   0xe000681c = 0x0000d000
    gmac_sa1_md                   0xe0006820 = 0x0000ff2b
    gmac_sa1_hi                   0xe0006824 = 0x00009f44
    gmac_sa2_lo                   0xe0006828 = 0x0000d000
    gmac_sa2_md                   0xe000682c = 0x0000ff2b
    gmac_sa2_hi                   0xe0006830 = 0x00009f44
    gmac_mcast_addr_hash1         0xe0006834 = 0x00000000
    gmac_mcast_addr_hash2         0xe0006838 = 0x00000000
    gmac_mcast_addr_hash3         0xe000683c = 0x00000000
    gmac_mcast_addr_hash4         0xe0006840 = 0x00000000
    gmac_tx_irq_src               0xe0006844 = 0x00000000
    gmac_rx_irq_src               0xe0006848 = 0x00000000
    gmac_tr_irq_src               0xe000684c = 0x00000000
    gmac_tx_irq_msk               0xe0006850 = 0x00000000
    gmac_rx_irq_msk               0xe0006854 = 0x00000000
    gmac_tr_irq_msk               0xe0006858 = 0x00000000

Internal-Data0/1:
  Marvell 88E6095 revision 2, switch port 8
    Port Registers:
        Status:        0x0e84  PCS Ctrl:      0xc13e
        Identifier:    0x0952  Port Ctrl:     0x0177
        Port Ctrl-1:   0x0000  Vlan Map:      0x06ff
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0100
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計を表示します。
show tech-support	Cisco TAC が問題を診断できるように情報を表示します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

シンタックスの説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみ表示します。範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、すべてのカウンタを表示する方法を示しています。

```
hostname# show counters all
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   single_vf
IOS_IPC       OUT_PKTS              2   single_vf

hostname# show counters
Protocol      Counter           Value   Context
NPCP          IN_PKTS            7195   Summary
NPCP          OUT_PKTS           7603   Summary
IOS_IPC       IN_PKTS             869   Summary
IOS_IPC       OUT_PKTS            865   Summary
IP            IN_PKTS             380   Summary
IP            OUT_PKTS            411   Summary
IP            TO_ARP              105   Summary
IP            TO_UDP                9   Summary
UDP           IN_PKTS               9   Summary
UDP           DROP_NO_APP           9   Summary
FIXUP         IN_PKTS             202   Summary
```

次の例は、カウンタの要約を表示する方法を示しています。

```
hostname# show counters summary
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   Summary
IOS_IPC       OUT_PKTS              2   Summary
```

次の例は、コンテキストのカウンタを表示する方法を示しています。

```
hostname# show counters context single_vf
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               4   single_vf
IOS_IPC       OUT_PKTS              4   single_vf
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタを消去します。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu usage** コマンドを使用します。

show cpu [**usage** | **profile**]

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

show cpu [**usage**] [**context** {**all** | *context_name*}]

シンタックスの説明

all	すべてのコンテキストを表示の対象にすることを指定します。
context	1 つのコンテキストを表示の対象にすることを指定します。
context_name	表示の対象にするコンテキストの名前を指定します。
profile	CPU プロファイルの使用状況を表示します。表示された情報は、トラブルシューティングの目的で TAC が使用することがあります。
usage	（オプション）CPU 使用状況を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

CPU の使用状況は、負荷の近似値を使用して 5 秒ごとに算出されます。この近似値は、次回と次々回の移動平均に提供されます。

show cpu コマンドを使用すると、負荷に関係しているプロセス（つまり、シングルモードで実行した ***show process*** コマンドと、マルチ コンテキスト モードのシステム コンフィギュレーションから実行した ***show process*** コマンドの両方の出力に表示されている項目のためのアクティビティ）を発見できます。

さらに、マルチ コンテキスト モードでは、いずれかの設定済みコンテキストが CPU に負荷をかけている場合、その負荷に関係しているプロセスを中断するように要求できます。このためには、各コンテキストに移動して ***show cpu*** コマンドを入力するか、このコマンドの変化型である ***show cpu context*** を入力します。

プロセスに関係する負荷は、直近の整数に四捨五入されます。それに対して、コンテキストに関係する負荷には小数点第 1 位が含まれています。たとえば、***show cpu*** をシステム コンテキストから入力すると、***show cpu context system*** コマンドを入力したときとは別の数値が示されます。前者は ***show cpu context all*** のすべての要素の近似的な要約であり、後者はその要約の一部にすぎません。

show cpu profile コマンドを **cpu profile activate** コマンドと組み合せて使用すると、TAC が CPU 問題のトラブルシューティングを支援するために収集および使用できる情報が表示されます。**show cpu profile** コマンドによって表示される情報は 16 進形式です。

例

次の例は、CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次の例は、マルチモードでシステム コンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次の例は、すべてのコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次の例は、one というコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

次の例では、プロファイラを有効にし、5000 個のサンプルを格納するように指示します。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

show cpu profile コマンドを使用して、結果を確認します。

（注）　**cpu profile activate** コマンドの実行中に **show cpu profile** コマンドを実行すると、進行状況が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

処理が完了すると、**show cpu profile** コマンド出力によって結果が表示されます。この情報をコピーし、TAC に提出します。TAC がこの情報をデコードします。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000
samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d
002198af 0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPU プロファイリングを有効にします。

show crashinfo

フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示するには、特権 EXEC モードで ***show crashinfo*** コマンドを入力します。

show crashinfo [**save**]

シンタックスの説明

save	（オプション）クラッシュ情報をフラッシュ メモリに保存するようにセキュリティ アプライアンスが設定されているかどうかを表示します。

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。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンドで生成）のものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Test_Crash**」であり、最後の文字列は「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュのものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Crash**」であり、最後の文字列は「**: End_Crash**」です（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データを消去していた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

例

次の例は、現在のクラッシュ情報コンフィギュレーションを表示する方法を示しています。

```
hostname# show crashinfo save
crashinfo save enable
```

次の例は、クラッシュ ファイル テストの出力を示しています（このテストによって、セキュリティ アプライアンスが実際にクラッシュすることはありません。このテストで生成されるのは、擬似的なサンプル ファイルです）。

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
```

```
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
```

```
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
```

```
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------
```

```
0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


     PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
```

```
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
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
TCP Fixup            0/s          0/s
TCPIntercept         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
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。

show crashinfo console

フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行うには、**crashinfo console disable** コマンドを使用します。このコマンドは、クラッシュを強制的に発生させます。

show crashinfo console

シンタックスの説明

console	クラッシュ情報をコンソールに出力するかどうかを制御します。

デフォルト

このコマンドにデフォルト設定はありません。

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。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 140-2 に準拠すると、キーやパスワードなどのクリティカル セキュリティ パラメータを暗号境界（シャーシ）の外側に配布することができません。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域は、機密データを含んでいることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

show crypto accelerator statistics

ハードウェア暗号アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、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 **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードも変数もありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、グローバルな暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                              Boot microcode   : CNlite-MC-Boot-Cisco-1.2
```

```
                                SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                                IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

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 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、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 **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにインストールされているすべての証明書が表示されます。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CA 証明書を表示しています。

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ca crls

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、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 **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにキャッシュされているすべての CRL 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CRL を表示しています。

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットの IPSec DF ビット ポリシーを表示するには、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 **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

シンタックスの説明

interface	インターフェイス名を指定します。
token	ユーザ認証にトークン ベースのサーバを使用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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、inside というインターフェイスの IPSec DF ビット ポリシーを表示しています。

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、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 **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

シンタックスの説明

interface	インターフェイス名を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、inside というインターフェイスの IPSec フラグメンテーション ポリシーを表示しています。

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec sa

IPSec SA のリストを表示するには、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 **show crypto ipsec sa** コマンドを使用します。このコマンドの別の形式である、**show ipsec sa** を使用することもできます。

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

シンタックスの説明

detail	（オプション）表示対象に関する詳細なエラー情報を表示します。
entry	（オプション）IPSec SA をピア アドレスでソートして表示します。
identity	（オプション）IPSec SA を ID でソートして、ESP を除いて表示します。これは圧縮された形式です。
***map** map-name*	（オプション）指定した暗号マップの IPSec SA を表示します。
***peer**peer-addr*	（オプション）指定したピア IP アドレスの IPSec SA を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

（注） 断片化の統計は、IPSec 処理前に断片化が発生することを IPSec SA ポリシーが記述している場合は、断片化前の統計になります。断片化後の統計は、IPSec 処理後に断片化が発生することを SA ポリシーが記述している場合に表示されます。

グローバル コンフィギュレーション モードで入力した次の例では、def という暗号マップの IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
```

```
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 263
          IV size: 8 bytes
          replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

```
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
```

```
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例では、キーワード ***identity*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、キーワード ***identity*** と ***detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

一連の IPSec 統計情報を表示するには、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 **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

シンタックスの説明

このコマンドには、キーワードも変数もありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec 統計情報を表示しています。

```
hostname(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA またはカウンタを、指定したパラメータに基づいて消去します。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show crypto isakmp stats

実行時の統計情報を表示するには、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 **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが導入されました。
7.2(1)	**show isakmp stats** コマンドが廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、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 **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [**detail**]

シンタックスの説明

detail	SA データベースに関する詳細な出力を表示します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合：

表 25-11

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合：

表 25-12

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

グローバル コンフィギュレーション モードで入力した次の例では、SA データベースに関する詳細な情報を表示しています。

```
hostname(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時の統計情報を表示するには、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 **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが導入されました。
7.2(1)	**show isakmp stats** コマンドが廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto protocol statistics

暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、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 **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を表示するプロトコルの名前を指定します。指定できるプロトコルは、次のとおりです。 ***ikev1***：Internet Key Exchange バージョン 1 ***ipsec***：IP セキュリティ フェーズ 2 プロトコル ***ssl***：Secure Socket Layer ***other***：新しいプロトコルのために予約済み ***all***：現在サポートされているすべてのプロトコル

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、指定したプロトコルに関する暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
```

```
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

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 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。

show csc node-count

ノードとは、固有のソース IP アドレス、またはセキュリティ アプライアンスにより保護されているネットワーク上のデバイスのアドレスです。セキュリティ アプライアンスは、毎日のノード カウントをトラッキングし、ユーザ ライセンス管理を目的に CSC SSM に伝えます。CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

show csc node-count [**yesterday**]

シンタックスの説明

yesterday	（オプション）CSC SSM が前日の 24 時間（午前零時から翌日の午前零時まで）スキャンしたトラフィックのノード数を表示します。

デフォルト

デフォルトで表示されるノード カウントは、午前零時からスキャンされたノード数です。

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。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

この例では、**show csc node-count** コマンドを使用して、CSC SSM が午前零時からスキャンしたトラフィックのノード数を表示する方法を示します。

```
hostname# show csc node-count
```

この例では、**show csc node-count** コマンドを使用して、CSC SSM が前日の 24 時間（午前零時から翌日の午前零時まで）スキャンしたトラフィックのノード数を表示する方法を示します。

```
hostname(config)# show csc node-count yesterday
```

関連コマンド

csc	ネットワーク トラフィックを CSC SSM に送信して、CSC SSM で設定されているとおりに FTP、HTTP、POP3、および SMTP をスキャンします。
show running-config class-map	現在のクラス マップ コンフィギュレーションを表示します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス マップ コンフィギュレーションを表示します。

show ctiqbe

セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show ctiqbe コマンドは、セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** と共に、このコマンドは、CTIQBE 検査エンジンの問題のトラブルシューティングに使用されます。

（注） **show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンスを越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# | show ctiqbe

Total: 1
 | LOCAL | FOREIGN | STATE | HEARTBEAT
-------------------------------------------------------------
1 | 10.0.0.99/1117  172.29.1.77/2748 | 1 | 120
 | RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 | 1029)
 | MEDIA: Device ID 27 | Call ID 0
 | Foreign 172.29.1.99 | (1028 | 1029)
 | Local | 172.29.1.88 | (26822 | 26823)
 | ---------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスと RTP リスニング ポートは、172.29.1.99 UDP ポート 1028 に PAT 変換されています。その RTCP リスニング ポートは、UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートは、その外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP リスニング ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D | DNS, d | dump, I | identity, i | inside, n | no random,
 | o | outside, r | portmap, s | static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
hostname#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように修正されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次の例は、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力を示しています。ユーザ名はログイン時にユーザが入力した名前を示し、P_PRIV はユーザが **enable** コマンドを入力したことを示し、P_CONF は **config terminal** コマンドを入力したことを示します。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
show running-config privilege	コマンドの特権レベルを表示します。