CHAPTER 15

inspect ctiqbe コマンド～ inspect xdmcp コマンド

inspect ctiqbe

CTIQBE プロトコル検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。検査をディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect ctiqbe

no inspect ctiqbe

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドは 7.0(1) で導入されました。このコマンドにより、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートする CTIQBE プロトコル検査をイネーブルにします。イネーブルにすると、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と正常に連携動作して、セキュリティ アプライアンスを通じてコール セットアップを実行できるようになります。

Telephony Application Programming Interface（TAPI）と Java Telephony Application Programming Interface（JTAPI）は、多くの Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、Cisco TAPI Service Provider（TSP）が Cisco CallManager と通信するために使用します。

次に、CTIQBE アプリケーション検査を使用するときに適用される制限を要約します。

- CTIQBE アプリケーション検査では、**alias** コマンドを使用したコンフィギュレーションはサポートされません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- **debug ctiqbe** コマンドを使用すると、メッセージ伝送が遅延する場合があります。その結果、リアルタイム環境ではパフォーマンスに影響が及ぶ場合があります。このデバッグまたはロギングをイネーブルにした結果、Cisco IP SoftPhone においてセキュリティ アプライアンスからのコール セットアップを完了できなくなったと思われる場合は、Cisco IP SoftPhone を実行するシステム上で Cisco TSP 設定のタイムアウト値を増やします。
- CTIQBE アプリケーション検査では、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートされていません。

次に、特定のシナリオで CTIQBE アプリケーション検査を使用する場合に特に考慮が必要な事項を要約します。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されている場合、各 Cisco CallManager はセキュリティ アプライアンスの異なるインターフェイスに接続されているため、これら 2 つの電話間のコールは失敗します。
- Cisco CallManager が Cisco IP SoftPhone よりもセキュリティの高いインターフェイス上にあり、Cisco CallManager IP アドレスの NAT または外部 NAT が必要になる場合、Cisco IP SoftPhone では、Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定する必要があるため、マッピングはスタティックにする必要があります。
- PAT または外部 PAT を使用して、Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone の登録を成功させるには、その TCP ポート 2748 を PAT（インターフェイス）アドレスの**同じポート**にスタティックにマッピングする必要があります。CTIQBE リスニング ポート（TCP 2748）は固定されており、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP 上でユーザが設定変更することはできません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect ctiqbe** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect ctiqbe** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect ctiqbe** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、CTIQBE 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2748）上の CTIQBE トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
show conn	さまざまな接続タイプの接続状態を表示します。
show ctiqbe	セキュリティ アプライアンスを越えて確立された CTIQBE セッションに関する情報を表示します。CTIQBE 検査エンジンによって割り当てられたメディア接続に関する情報を表示します。
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。

inspect dcerpc

エンドポイント マッパー宛の DCERPC トラフィックの検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect dcerpc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

シンタックスの説明

map_name	（オプション）DCERPC マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.2(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

inspect dcerpc コマンドは、DCERPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

例

次の例では、DCERPC ピンホールに設定されたタイムアウトを指定して、DCERPC 検査ポリシーを定義する方法を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc_map

hostname(config)# service-policy global-policy global
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
timeout pinhole	DCERPC ピンホールのタイムアウトを設定し、グローバル システム ピンホール タイムアウトを上書きします。

inspect dns

DNS 検査をイネーブルにするには（以前にディセーブルにした場合）、または、DNS 検査のパラメータを設定するには、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。DNS 検査をディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect dns [*map_name*]

no inspect dns [*map_name*]

シンタックスの説明

map_name	（オプション）DNS マップの名前。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。
7.2(1)	さらに多くの DNS 検査パラメータを設定できるように、このコマンドが修正されました。

使用上のガイドライン

DNS guard は、DNS 応答がセキュリティ アプライアンスによって転送されると、DNS クエリーに関連付けられた DNS セッションをただちに停止します。DNS guard は、また、DNS 応答の ID が DNS クエリーの ID と一致していることを確認するために、メッセージ交換を監視します。

DNS 検査がイネーブルの場合（デフォルト）、セキュリティ アプライアンスは次の追加タスクを実行します。

- **alias** コマンド、**static** コマンド、および **nat** コマンドを使用して完成したコンフィギュレーションに基づいて、DNS レコードを変換する（DNS リライト）。変換が適用されるのは、DNS 応答の A レコードのみです。そのため、PTR レコードを要求する逆ルックアップは、DNS リライトの影響を受けません。

（注） DNS リライトは PAT には適用できません。これは、A レコードごとに複数の PAT 規則が適用可能であり、使用される PAT 規則があいまいになるためです。

- DNS メッセージの最大長を適用する（デフォルトは 512 バイト、最大長は 65,535 バイト）。必要に応じて再構成が実行され、パケット長が設定した最大長を超えていないことが確認されます。最大長を超えている場合、そのパケットはドロップされます。
- ドメイン名の長さとして 255 バイトを、ラベルの長さとして 63 バイトを適用する。
- DNS メッセージに圧縮ポインタが出現する場合、ポインタによって参照されるドメイン名の完全性を確認する。
- 圧縮ポインタのループが存在するかどうかを確認する。

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。しかし、**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ることが示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの動作

DNS 検査がイネーブルの場合、DNS リライトは、任意のインターフェイスから発信される DNS メッセージの NAT をフル サポートします。

内部ネットワーク上のクライアントが内部アドレスの DNS 解決を外部インターフェイス上の DNS サーバに要求した場合、DNS A レコードは正しく変換されます。DNS 検査エンジンがディセーブルの場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイス上にある場合、*DNS 応答*内のパブリック アドレス（ルーティング可能なアドレスまたは「マッピングされた」アドレス）を、プライベート アドレス（「実」アドレス）に変換する。
- DNS クライアントがパブリック インターフェイス上にある場合、プライベート アドレスをパブリック アドレスに変換する。

DNS 検査がイネーブルであれば、**alias** コマンド、**static** コマンド、または **nat** コマンドを使用して DNS リライトを設定できます。これらのコマンドのシンタックスや機能の詳細については、該当するコマンドのページを参照してください。

注：アップグレード時に、コマンド シンタックスは現在のシンタックスに変換されます。

例

次の例では、DNS メッセージの最大長を設定する方法を示しています。

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

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。
debug dns	DNS のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect esmtp

SMTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect esmtp

no inspect esmtp

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ESMTP アプリケーション検査では、SMTP ベースの攻撃からの保護を強化するため、セキュリティ アプライアンスを通過できる SMTP コマンドのタイプを制限し、モニタリング機能を追加しています。

（注） ESMTP　検査ポリシーは、低セキュリティのインターフェイスから高セキュリティのインターフェイスに入ってくるトラフィック フローにのみ適用されます。高セキュリティのインターフェイスから低セキュリティのインターフェイスへのフローの場合は、検査は実行されません。

ESMTP は SMTP プロトコルの機能拡張であり、あらゆる点で SMTP と類似しています。便宜上、このドキュメントでは、SMTP という用語は SMTP と ESMTP の両方を指します。拡張 SMTP のアプリケーション検査プロセスは、SMTP アプリケーション検査と類似しており、SMTP セッションのサポートを備えています。拡張 SMTP セッションで使用されるコマンドのほとんどは、SMTP セッションで使用されるものと同じですが、ESMTP セッションは、動作がはるかに高速で、配信通知ステータスなど、信頼性とセキュリティに関するオプションをより多く備えています。

inspect esmtp コマンドには、**fixup smtp** コマンドで提供されていた機能が含まれています。また、一部の拡張 SMTP コマンドに対する追加サポートも含まれています。拡張 SMTP アプリケーション検査では、8 つの拡張 SMTP コマンド（AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、および VRFY）に対するサポートが追加されています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、および RSET）に対するサポートを合せると、セキュリティ アプライアンスは合計 15 の SMTP コマンドをサポートしています。

他の拡張 SMTP コマンド（ATRN、STARTLS、ONEX、VERB、CHUNKING など）やプライベート拡張はサポートされていません。サポート対象外のコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

inspect esmtp コマンドは、SMTP バナーの文字を、「2」、「0」、「0」の文字を除いて、アスタリスクに変更します。復帰（CR）と改行（LF）は、無視されます。

SMTP 検査がイネーブルの場合、次の規則が順守されていないときは、対話型の SMTP に使用される Telnet セッションは有効なコマンドを待機し、ファイアウォール esmtp ステート マシンはセッションを正しい状態に保ちます。この規則とは、SMTP コマンドは少なくとも 4 文字の長さが必要である、SMTP コマンドは改行と復帰で終了する必要がある、次の返信を発行する前に応答を待つ必要がある、というものです。

SMTP サーバは、数値の応答コードと人が読めるオプションの文字列によって、クライアントの要求に応答します。SMTP アプリケーション検査は、ユーザが使用できるコマンドや、サーバが返すメッセージを制御および削減します。SMTP 検査は、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本的な SMTP コマンドと 8 つの拡張コマンドに制限する。
- SMTP コマンド応答シーケンスを監視する。
- 監査証跡を生成する。メール アドレスに埋め込まれていた無効な文字が置き換えられた場合、監査レコード 108002 が生成されます。詳細については、RFC 821 を参照してください。

SMTP 検査は、コマンドと応答のシーケンスを監視して、次の異常なシグニチャを検出します。

- 不完全なコマンド。
- コマンドの不正な終了（<CR><LR> で終了していない）。
- PIPE シグニチャが MAIL from コマンドまたは RCPT to コマンドへのパラメータとして検出された場合、セッションは閉じられます。ユーザは設定できません。
- SMTP サーバによる予期しない移行。
- 未知のコマンドがあると、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバは、クライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリームの編集。
- コマンドのパイプライン化。

例

次の例に示すように、SMTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（25）上の SMTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

すべてのインターフェイスに対して SMTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug esmtp	SMTP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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	SMTP など、さまざまな接続タイプの接続状態を表示します。

inspect ftp

FTP 検査用のポートを設定する場合、または高度な検査をイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

シンタックスの説明

map_name	FTP マップの名前。
strict	（オプション）FTP トラフィックの高度な検査をイネーブルにし、強制的に RFC 標準に準拠させます。

注意　FTP を上位のポートに移動する場合は、注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に向けて開始する接続はすべて、データ ペイロードが FTP コマンドとして解釈されます。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、ポート 21 で FTP があるかどうかリッスンします。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション検査は、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続を準備する。
- ***ftp*** コマンド応答シーケンスを追跡する。
- 監査証跡を生成する。
- 埋め込み IP アドレスの NAT を実行する。

（注）　バナーを除き、**inspect ftp** は FTP コマンドまたは応答をセグメント化する FTP サーバをサポートしていません。

FTP アプリケーション検査は、FTP データ転送用にセカンダリ チャネルを準備します。チャネルは、ファイルのアップロード、ファイルのダウンロード、またはディレクトリ一覧イベントの応答として割り当てられます。ただし、事前にネゴシエートされている必要があります。ポートは、PORT コマンドまたは PASV コマンドによってネゴシエートされます。

（注）　**no inspect ftp** コマンドを使用して、FTP 検査エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

strict オプションの使用方法

strict オプションは、Web ブラウザが FTP 要求内の埋め込みコマンドを送信しないようにします。各 ***ftp*** コマンドは、新しいコマンドが許可される前に確認される必要があります。埋め込みコマンドを送信する接続は、ドロップされます。**strict** オプションは、FTP サーバが 227 コマンドを生成することだけを許可し、FTP クライアントが PORT コマンドを生成することだけを許可します。227 コマンドと PORT コマンドはチェックして、エラー文字列内に表示されないようにします。

注意　***strict*** オプションを使用すると、RFC 標準に準拠していない FTP クライアントが遮断されることがあります。

strict オプションがイネーブルの場合、次の異常なアクティビティについて、各 ***ftp*** コマンドと応答シーケンスが追跡されます。

- 不完全なコマンド：PORT および PASV 応答コマンド内のカンマの数が 5 つかどうかが確認されます。5 つ以外の場合、PORT コマンドは不完全であると見なされ、TCP 接続は終了します。
- 不正なコマンド：RFC に規定されているように、***ftp*** コマンドが <CR><LF> 文字で終了しているかどうかが確認されます。異なっている場合、接続は終了します。
- RETR コマンドと STOR コマンドのサイズ：固定値になっているかどうかが確認されます。サイズが固定値より大きい場合、エラー メッセージがログに記録され、接続は終了します。
- コマンド スプーフィング：PORT コマンドは常にクライアントから送信される必要があります。PORT コマンドがサーバから送信されている場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV　応答コマンド（227）は常にサーバから送信される必要があります。PASV 応答コマンドがクライアントから送信されている場合、TCP 接続は拒否されます。この拒否により、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行した場合のセキュリティ ホールが防止されます。
- TCP ストリームの編集。
- 無効なポートのネゴシエーション：ネゴシエートされたダイナミック ポートの値が 1024 未満かどうかが確認されます。1 ～ 1024 の範囲のポート番号は既知の接続用に予約されているため、ネゴシエートされたポートがこの範囲内の場合は、TCP 接続は開放されます。
- コマンドのパイプライン化：PORT および PASV 応答コマンド内のポート番号の後にある文字数が定数の 8 であるかどうかが相互確認されます。9 以上の場合、TCP 接続は終了します。
- セキュリティ アプライアンスが、SYST コマンドに対する FTP サーバの応答を一連の X に置き換え、サーバのシステム タイプが FTP クライアントに知られることを防止します。このデフォルト動作を無効にするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

（注）　セキュリティ アプライアンスを通過させない特定の FTP コマンドを指定するには、FTP マップを指定し、**request-command deny** コマンドを使用します。詳細については、**ftp-map** コマンドと **request-command deny** コマンドのページを参照してください。

FTP ログ メッセージ

FTP アプリケーション検査は、次のログ メッセージを生成します。

- 取得またはアップロードされた各ファイルについて、監査レコード 302002 が生成されます。
- **ftp** コマンドが RETR または STOR であるかが確認され、取得コマンドと格納コマンドがログに記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。

FTP アプリケーション検査は、NAT と連携して、アプリケーション ペイロード内の IP アドレスを変換します。詳細については、RFC 959 を参照してください。

例

次の例では、FTP トラフィックを識別し、FTP マップを定義し、ポリシーを定義し、厳密な FTP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-inbound_ftp)# request-command deny put stou appe
hostname(config-ftp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

すべてのインターフェイスに対して厳密な FTP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

（注）　FTP 制御接続用のポートだけを指定して、データ接続用は指定しません。セキュリティ アプライアンス ステートフル検査エンジンは、必要に応じて、ダイナミックにデータ接続を用意します。

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。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
request-command deny	禁止する FTP コマンドを指定します。
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。

inspect gtp

GTP 検査をイネーブルまたはディセーブルにする場合、または GTP トラフィックまたはトンネルを制御するための GTP マップを定義する場合は、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

（注） GTP 検査には、特別なライセンスが必要です。セキュリティ アプライアンス上で **inspect gtp** コマンドを入力する場合、必要なライセンスを持っていないときは、セキュリティ アプライアンスによってエラー メッセージが表示されます。

シンタックスの説明

map_name	（オプション）GTP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(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

GTP は、GPRS 用のトンネリング プロトコルで、無線ネットワーク上のセキュアなアクセスを可能にします。GPRS は、既存の GSM ネットワークを統合するために設計されたデータ ネットワーク アーキテクチャです。モバイル ユーザに対して、企業ネットワークとインターネットにアクセスするためのパケット スイッチ データ サービスを中断なく提供します。GTP の概要については、『*Cisco Security Appliance Command Line Configuration Guide*』の「アプリケーション層プロトコル検査の適用」の章を参照してください。

GTP のパラメータの定義に使用する特定のマップを指定するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**drop** と **rate-limit** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

GTP マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

GTP の既知のポートは、次のとおりです。

- 3386
- 2123

次の機能は 7.0(1) ではサポートされていません。

- NAT、PAT、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、および 2152 以外のポート
- トンネリング IP パケットとその内容の検証

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect gtp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect gtp** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、アクセス リストを使用して GTP トラフィックを識別し、GTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

（注） 次の例では、デフォルト値を使用して GTP 検査をイネーブルにします。デフォルト値を変更するには、**gtp-map** コマンドのページと、GTP マップ コンフィギュレーション モードから入力する各コマンドのページを参照してください。

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。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
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 service-policy inspect gtp	**inspect gtp** ポリシーのステータスと統計を示します。

inspect h323

H.323 アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect h323 {**h225** | **ras**}

no inspect h323 {**h225** | **ras**}

シンタックスの説明

h225	H.225 シグナリング検査をイネーブルにします。
ras	RAS 検査をイネーブルにします。

デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718-1719

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager および VocalTec Gatekeeper などの H.323 に準拠したアプリケーションをサポートしています。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）が定義した LAN 上のマルチメディア会議用のプロトコル スイートです。セキュリティ アプライアンスは、One Call Signaling Channel 上の Multiple Calls の H.323 v3 機能など、バージョン 4 までの H.323 をサポートしています。

H.323 検査がイネーブルの場合、セキュリティ アプライアンスは、H.323 バージョン 3 で導入された機能である、同一のコール シグナリング チャネル上の複数のコールをサポートします。この機能を使用すると、コール セットアップ時間が短縮され、セキュリティ アプライアンス上のポートの使用も削減されます。

H.323 検査には、次の 2 つの主要な機能があります。

- H.225 および H.245 メッセージ内の必要な埋め込み IPv4 アドレスの NAT を実行する。H.323 メッセージは PER 符号化フォーマットで符号化されているため、セキュリティ アプライアンスは、ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 接続および RTP/RTCP 接続をダイナミックに割り当てる。

H.323 の動作

H.323 のプロトコル コレクションでは、集合的に、2 つまでの TCP 接続と 4 ～ 6 の UDP 接続を使用できます。FastStart は TCP 接続を 1 つだけ使用し、RAS は登録、許可、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントでは、最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コールのセットアップを要求できます。コール セットアップ プロセスの一部として、H.323 端末は、H.245 TCP 接続に使用するポート番号をクライアントに提供します。H.245 接続は、コール ネゴシエーションとメディア チャネルのセットアップに使用されます。H.323 ゲートキーパーを使用している環境では、最初のパケットは UDP を使用して送信されます。

H.323 検査は、Q.931 TCP 接続を監視して、H.245 ポート番号を判別します。H.323 端末が FastStart を使用していない場合、セキュリティ アプライアンスは、H.225 メッセージの検査に基づいて、H.245 接続をダイナミックに割り当てます。

（注）　H.225 接続は、RAS を使用してダイナミックに割り当てることもできます。

各 H.245 メッセージ内で、H.323 エンドポイントは、以降の UDP データ ストリームに使用するポート番号を交換します。H.323 検査は、H.245 メッセージを検査してこれらのポートを識別し、メディア交換用の接続をダイナミックに作成します。Real-Time Transport Protocol（RTP）は、ネゴシエートされたポート番号を使用しますが、RTP Control Protocol（RTCP）は、次の上位ポート番号を使用します。

H.323 コントロール チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 検査は、次のポートを使用します。

- 1718：ゲートキーパー検出に使用される UDP ポート
- 1719：RAS およびゲートキーパー検出に使用される UDP ポート
- 1720：TCP 制御ポート

ゲートキーパーからの ACF メッセージがセキュリティ アプライアンスを通過する場合は、H.225 接続用のピンホールが空けられます。H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーが使用される場合、セキュリティ アプライアンスは、ACF メッセージの検査に基づいて、H.225 接続を開きます。セキュリティ アプライアンスに ACF メッセージが表示されない場合は、H.225 コール シグナリング用に既知の H.323 ポート 1720 のアクセス リストを開くことが必要となる場合があります。

セキュリティ アプライアンスは、H.225 メッセージを検査した後で、H.245 チャネルをダイナミックに割り当て、同様に検査する H.245 チャネルに接続します。これは、セキュリティ アプライアンスを通過した H.245 メッセージはすべて、H.245 アプリケーション検査を通過し、埋め込み IP アドレスの NAT が実行され、ネゴシエートされたメディア チャネルが開かれることを意味します。

H.323 ITU 標準では、信頼できる接続に送信する前に、メッセージ長を定義する TPKT ヘッダーを H.225 および H.245 の前に配置することが規定されています。TPKT ヘッダーは H.225/H.245 メッセージと同じ TCP パケットで送信されない場合もあるため、メッセージを正しく処理およびデコードするには、セキュリティ アプライアンスで TPKT 長を保持しておく必要があります。セキュリティ アプライアンスは、各接続のデータ構造を保持し、このデータ構造には、次に受信されるメッセージの TPKT 長が含まれます。

セキュリティ アプライアンスで任意の IP アドレスの NAT を実行する必要がある場合は、チェックサム、UUIE（user-user information element）の長さ、および TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合、

セキュリティ アプライアンスは TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの新しい TPKT を付加します。

（注）　セキュリティ アプライアンスによる TPKT のプロキシ ACK では、TCP オプションはサポートされません。

H.323 検査を通過するパケットを使用する各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドを使用して設定された H.323 タイムアウトでタイムアウトします。

制限と制約事項

次に、H.323 アプリケーション検査を使用する上での既知の問題および制限の一部を示します。

- スタティック PAT は、H.323 メッセージ内のオプション フィールドに埋め込まれた IP アドレスを正しく変換しない場合があります。この種の問題が発生した場合は、H.323 に対してスタティック PAT を使用しないでください。
- H.323 アプリケーション検査は、セキュリティ レベルの等しいインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが、H.323 ゲートキーパーに登録されている状態で、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイにコールを発信しようとする場合、接続は確立されますが、音声が双方向で聞こえない現象が報告されています。この問題は、セキュリティ アプライアンスとは無関係です。
- ネットワーク スタティックを設定する場合、そのネットワーク スタティックがサードパーティのネットマスクおよびアドレスと同じであるときは、すべての発信 H.323 接続が失敗します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect h323** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect h323** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、H.323 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1720）上の H.323 トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

すべてのインターフェイスに対して H.323 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
show h225	セキュリティ アプライアンスを越えて確立された H.225 セッションの情報を表示します。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout {h225 | h323}	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

inspect http

HTTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect http** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect http [*map_name*]

no inspect http [*map_name*]

シンタックスの説明

map_name	（オプション）HTTP マップの名前。

デフォルト

HTTP のデフォルト ポートは 80 です。

高度な HTTP 検査は、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect http コマンドは、HTTP トラフィックに関連する可能性のある特定の攻撃やその他の脅威から保護します。HTTP 検査では、高度な HTTP 検査が実行されます。

高度な HTTP 検査は、HTTP メッセージが RFC 2616 に準拠していること、RFC で定義されている方式やサポートされている拡張方式を使用していること、および他のさまざまな基準を満たしていることを確認します。多くの場合、これらの基準と、その基準が満たされないときのシステムの応答を設定できます。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

HTTP メッセージに適用できる基準には、次のものがあります。

- リスト（設定可能）に挙げられているメソッドを含んでいない。
- 特定の転送符号化方式またはアプリケーション タイプ。
- HTTP トランザクションが RFC 仕様に沿っている。
- メッセージ本文のサイズが、制限値（設定可能）以下である。
- 要求と応答のメッセージ ヘッダーのサイズが、制限値（設定可能）以下である。
- URI の長さが制限値（設定可能）以下である。

- メッセージ本文の content-type が、ヘッダーと一致している。
- 応答メッセージの content-type が、要求メッセージの *accept-type* フィールドと一致している。
- メッセージの content-type が、事前定義済みの内部リストに挙げられている。
- メッセージが、RFC による HTTP 形式の基準を満たしている。
- 選択したサポート可能アプリケーションが存在している（または、存在していない）。
- 選択した符号化タイプが存在している（または、存在していない）。

（注）　基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

高度な HTTP 検査をイネーブルにするには、**inspect http** *http-map* コマンドを使用します。このコマンドが HTTP トラフィックに適用する規則は、特定の HTTP マップで定義されます。この HTTP マップを設定するには、**http-map** コマンドと HTTP マップ コンフィギュレーション モードのコマンドを入力します。

（注）　HTTP マップを使用して HTTP 検査をイネーブルにすると、デフォルトでは、アクション reset および log を使用した厳密な HTTP 検査がイネーブルになります。検査に合格しない場合に実行されるアクションは変更できますが、HTTP マップがイネーブルのままである限り、厳密な検査をディセーブルにすることはできません。

inspect http コマンドは syslog メッセージ 304001 を介して、GET 要求のロギングをイネーブルまたはディセーブルにします。

（注）　**inspect http** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例は、HTTP トラフィックを識別し、HTTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、次のコンテンツを含んでいるトラフィックをセキュリティ アプライアンスが検出したときに、接続をリセットして syslog エントリを作成します。

- 100 バイト未満または 2,000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

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。
debug appfw	HTTP アプリケーション検査に関する詳細情報を表示します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

inspect icmp

ICMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp

no inspect icmp

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ICMP 検査エンジンを使用すると、ICMP トラフィックを TCP トラフィックおよび UDP トラフィックと同様に検査できます。ICMP 検査エンジンを使用しない場合は、ACL により ICMP がセキュリティ アプライアンスを通過しないようにすることをお勧めします。ステートフル検査が実行されない場合、ICMP はネットワークの攻撃に利用されることがあります。ICMP 検査エンジンは、各要求に対する応答が 1 つだけであり、シーケンス番号が正しいことを確認します。

ICMP 検査エンジンがディセーブルの場合（デフォルト設定）、低セキュリティ インターフェイスから高セキュリティ インターフェイスへの ICMP エコー応答メッセージは拒否されます。このメッセージが ICMP エコー要求への応答である場合も同様です。

例

次の例に示すように、ICMP アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
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。

inspect icmp error

ICMP エラー メッセージに対するアプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect icmp error** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp error

no inspect icmp error

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect icmp error コマンドは、スタティック /NAT のコンフィギュレーションに基づいて、ICMP エラー メッセージを送信する中間ホップの xlate を作成する場合に使用します。デフォルトでは、セキュリティ アプライアンスは中間ホップの IP アドレスを表示しません。ただし、**inspect icmp error** コマンドを使用すると、中間ホップの IP アドレスが表示されます。セキュリティ アプライアンスは、パケットを変換後の IP アドレスで上書きします。

イネーブルの場合、ICMP エラー検査エンジンは、ICMP パケットに次の変更を加えます。

- IP ヘッダーで、NAT IP が Client IP（宛先アドレスおよび中間ホップ アドレス）に変更され、IP チェックサムが変更されます。
- ICMP ヘッダーで、ICMP チェックサムが ICMP パケットの変更に応じて変更されます。

- ペイロードでは、次の変更が加えられます。
  - 元のパケットの NAT IP が Client IP に変更されます。
  - 元のパケットの NAT ポートが Client Port に変更されます。
  - 元のパケットの IP チェックサムが再計算されます。

ICMP エラー メッセージが取得されると、ICMP エラー検査がイネーブルかどうかに関係なく、ICMP ペイロードがスキャンされ、元のパケットから 5 つのタプル（src ip、dest ip、src port、dest port、および ip プロトコル）が取得されます。取得された 5 つのタプルを使用して検索が実行され、クライアントの元のアドレスが判別され、特定の 5 つのタプルに関連付けられた既存のセッションが検出されます。セッションが検出されない場合、ICMP エラー メッセージはドロップされます。

例

次の例に示すように、ICMP エラー アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP エラー検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
inspect icmp	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
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。

inspect ils

ILS アプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect ils** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ils

no inspect ils

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用して ILS サーバとディレクトリ情報を交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品用の NAT をサポートします。

セキュリティ アプライアンスは ILS の NAT をサポートしています。ILS は、ILS または SiteServer Directory のエンドポイントの登録および検出に使用されます。LDAP データベースには IP アドレスだけが保管されるため、PAT はサポートできません。

LDAP サーバが外部にある場合、検索応答を実行するには、NAT を使用して、外部 LDAP サーバに登録されている内部ピア間のローカル通信を可能にすることを考慮する必要があります。このような検索応答では、xlate、DNAT エントリの順に検索され、正しいアドレスが取得されます。両方の検索に失敗した場合、アドレスは変更されません。NAT 0 を使用している（NAT を使用していない）サイトや、DNAT 対話を想定していないサイトについては、パフォーマンスを向上させるために、検査エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内側にある場合は、追加の設定が必要になることがあります。この場合は、指定ポート（通常は TCP 389）上で LDAP サーバにアクセスする外部クライアント用のホールが必要です。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP 非アクティビティ間隔が経過すると切断されます。デフォルトでは、この間隔は 60 分です。間隔を調整するには、**timeout** コマンドを使用します。

ILS/LDAP は、クライアント / サーバ モデルに基づいて、単一 TCP 接続上のセッションを処理します。これらのセッションの一部は、クライアントのアクションに応じて作成される場合があります。

接続のネゴシエーション中に、クライアントからサーバに対して BIND PDU が送信されます。サーバから BIND RESPONSE を正常に受信すると、他の操作メッセージ（ADD、DEL、SEARCH、または MODIFY など）が交換され、ILS Directory 上で処理が実行されます。ADD REQUEST および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される NetMeeting ピアの IP アドレスが含まれる場合があります。Microsoft NetMeeting v2.X および v3.X では、ILS がサポートされています。

ILS 検査は、次の処理を実行します。

- BER デコード機能を使用して、LDAP REQUEST/RESPONSE PDU をデコードする。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスで PDU を符号化する。
- 新しく符号化した PDU を TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号を差分的に調整する。

ILS 検査には、次の制限があります。

- 照会の要求および応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに別々の ID を持つ単一ユーザは、NAT では認識できません。

（注） H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP **timeout** コマンドで指定された間隔が経過すると切断されます。この間隔は、デフォルトでは 60 分に設定されています。

例

次の例に示すように、ILS 検査エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

すべてのインターフェイスに対して ILS 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug ils	ILS のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect im

IM トラフィックの検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect im** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect im [*map_name*]

no inspect im [*map_name*]

シンタックスの説明

map_name	（オプション）IM マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.2(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

inspect im コマンドは、IM プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

（注）　**inspect im** コマンドは、**inspect http** コマンドと共に設定した場合、またはポート 80 に対して **filter activex**、**filter java**、または **filter url** の各 **filter** コマンドと共に設定した場合にディセーブルになります。

例

次の例では、IM 検査ポリシー マップを定義する方法を示します。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname3 "darshant\@yahoo.com"
hostname(config)# regex yhoo_version_regex "1\.0"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type regex match-any yhoo_file_block_list
hostname(config-cmap)# match regex ".*\.gif"
hostname(config-cmap)# match regex ".*\.exe"

hostname(config)# class-map type regex match-any new_im_regexp
hostname(config-cmap)# match regexp "new_im_regexp"

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yhoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yhoo_dst_login_name_regex

hostname(config)# class-map type inspect im yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type im im_policy_all
hostname(config-pmap)# class yahoo_in_file_xfer_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yhoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yhoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config-pmap)# match im-pattern regex class new_im_regexp
hostname(config-pmap-c)# action log
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspection_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
match protocol	検査クラス マップまたは検査ポリシー マップに含まれている、特定の IM プロトコルに一致するかどうかを調べます。

inspect ipsec-pass-thru

IPSec Pass Thru 検査をイネーブルにするには、クラス マップ コンフィギュレーション モードで **inspect ipsec-pass-thru** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

シンタックスの説明

map_name	（オプション）IPSec Pass Thru マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(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

inspect ipsec-pass-thru コマンドはアプリケーション検査をイネーブルまたはディセーブルにします。IPSec Pass Through アプリケーション検査では、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）トラフィックと AH（IP プロトコル 51）トラフィックの便利な Traversal が提供されます。これにより、ESP トラフィックと AH トラフィックを許可するためのアクセス リスト設定が長くなることを回避でき、タイムアウトと最大接続数を使用したセキュリティも実現できます。

検査のパラメータを定義するために使用する特定のマップを指定するには、IPSec Pass Through パラメータ マップを使用します。パラメータ コンフィギュレーションにアクセスするには、**policy-map type inspect** コマンドを使用します。その後、ESP トラフィックまたは AH トラフィックに対する制約を指定できます。パラメータ コンフィギュレーションでは、クライアントごとの最大接続数、およびアイドル タイムアウトを設定できます。

class-map、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。定義したパラメータ マップは、**inspect IPSec-pass-thru** コマンドと共に使用されたときにイネーブルになります。

NAT トラフィックおよび非 NAT トラフィックが許可されます。ただし、PAT はサポートされていません。

（注）　ASA 7.0 では、**inspect ipsec-pass-thru** コマンドは、ESP トラフィックだけに通過を許可していました。以降のバージョンでも同じ動作が保持されるように、引数なしで **inspect ipsec-pass-thru** コマンドを指定した場合は、ESP を許可するデフォルトのマップが作成されて対応付けられます。このマップは、**show running-config all** コマンドの出力で確認できます。

例

次の例は、アクセス リストを使用して IKE トラフィックを識別し、IPSec Pass Thru パラメータ マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
match protocol	検査クラス マップまたは検査ポリシー マップに含まれている、特定の IM プロトコルに一致するかどうかを調べます。

inspect mgcp

MGCP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect mgcp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

シンタックスの説明

map_name	（オプション）MGCP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

MGCP を使用する場合、通常、少なくとも 2 つの **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つは Call Agent がコマンドを受信するポート用です。通常、Call Agent は、ゲートウェイのデフォルトの MGCP ポート 2427 にコマンドを送信し、ゲートウェイは、Call Agents のデフォルトの MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは、一般的に、電話回線上で伝送されるオーディオ信号と、インターネットまたは他のパケット ネットワーク上で伝送されるデータ パケットとの変換を行うネットワーク要素です。MGCP で NAT および PAT を使用すると、限られた数の外部（グローバル）アドレスで、内部ネットワーク上の多数のデバイスをサポートできます。

次に、メディア ゲートウェイの例を示します。

- トランキング ゲートウェイ。これは、電話網と Voice over IP ネットワーク間のインターフェイスです。このゲートウェイは、一般的に、多数のデジタル回線を管理します。
- レジデンシャル ゲートウェイ。これは、Voice over IP ネットワークに従来のアナログ（RJ11）インターフェイスを提供します。レジデンシャル ゲートウェイの例には、ケーブル モデム / ケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド無線デバイスなどがあります。

- ビジネス ゲートウェイ。これは、Voice over IP ネットワークに従来のデジタル PBX インターフェイスまたは統合 *soft PBX* インターフェイスを提供します。

MGCP メッセージは、UDP 上で転送されます。応答は、コマンドの送信元アドレス（IP アドレスおよび UDP ポート番号）に返送されますが、コマンドの宛先と同じアドレスから返送されない場合があります。この状況が発生するのは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用され、コマンドを受信したコール エージェントからバックアップ コール エージェントに制御が渡された後で、バックアップ コール エージェントが応答を返送する場合です。

（注）　MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判別します。この結果、セキュリティ アプライアンスからのフローが確立され、MGCP エンドポイントがコール エージェントに登録できるようになります。

1 つ以上のコール エージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドと **gateway** コマンドを使用します。コマンド キューに一度に入れることができる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect mgcp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect mgcp** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、MGCP トラフィックを識別し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

このコンフィギュレーションにより、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようになり、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようになります。キューに入れることができる MGCP コマンドの最大数は、150 です。

すべてのインターフェイスの MGCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug mgcp	MGCP デバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	セキュリティ アプライアンスを介して確立された MGCP セッションに関する情報を表示します。
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。

inspect netbios

NetBIOS アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect netbios コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

シンタックスの説明

map_name	（オプション）NetBIOS マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

例

次の例では、NetBIOS 検査ポリシー マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

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。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect pptp

PPTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect pptp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect pptp

no inspect pptp

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションを構成するのは、1 つの TCP チャネルと、通常 2 つの PPTP GRE トンネルです。TCP チャネルは、PPTP GRE トンネルをネゴシエートおよび管理するためのコントロール チャネルです。GRE トンネルは、2 つのホスト間で PPP セッションを伝送します。

イネーブルの場合、PPTP アプリケーション検査は、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するのに必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 に定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合、GRE **[**RFC 2637**]** の修正版に対してだけ実行されます。Port Address Translation（PAT; ポート アドレス変換）は、修正前のバージョンの GRE **[**RFC 1701、RFC 1702**]** に対しては*実行されません*。

特に、セキュリティ アプライアンスは、PPTP バージョンのアナウンスメントと発信コールの要求 / 応答シーケンスを検査します。RFC 2637 に定義されている PPTP バージョン 1 だけが検査されます。どちらかの側でアナウンスされたバージョンがバージョン 1 でなければ、TCP コントロール チャネルはそれ以上検査されません。さらに、発信コール要求と応答シーケンスが追跡されます。接続と xlate は、必要に応じてダイナミックに割り当てられて、それ以後のセカンダリ GRE データ トラフィックを送ることが可能になります。

PPTP 検査エンジンは、PPTP トラフィックを PAT で変換するためにイネーブルにする必要があります。さらに、PAT は、GRE（RFC2637）の修正版に対してだけで実行されます。これは、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合だけです。PAT は、修正前のバージョンの GRE（RFC 1701 と RFC 1702）に対しては実行されません。

RFC 2637 で規定されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始された PPP セッションをヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）へトンネリングするために使用されます。この使用方法では、PAC はリモート クライアントとなり、PNS はサーバとなります。

ただし、Windows によって VPN 用に使用される場合、対話関係は逆になります。PNS は、ヘッドエンド PAC への接続を開始して中央ネットワークにアクセスするリモート シングルユーザ PC です。

例

次の例に示すように、PPTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

すべてのインターフェイスに対して PPTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug pptp	PPTP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect radius-accouting

RADIUS アカウンティング検査をイネーブルまたはディセーブルにする場合、またはトラフィックまたはトンネルを制御するためのマップを定義する場合は、クラス コンフィギュレーション モードで **inspect radius-accounting** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

シンタックスの説明

map_name	（オプション）RADIUS アカウンティング マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.2(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

RADIUS アカウンティングのパラメータの定義に使用する特定のマップを指定するには、**radius-accounting** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。さまざまなコンフィギュレーション コマンドを使用して設定した基準を満たさないメッセージに対して指定できるアクションは、**send**、**host**、**validate-attribute**、**enable gprs**、**timeout users** などです。***parameter*** モードからこれらのコマンドにアクセスできます。

RADIUS アカウンティング マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

（注）　**inspect radius-accounting** コマンドと共に使用できるのは **class-map type management** コマンドだけです。

例

次の例は、アクセス リストを使用して RADIUS アカウンティング トラフィックを識別し、RADIUS アカウンティングを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# policy-map type inspect radius-accountin ra
```

（注） 次の例では、デフォルト値を使用して RADIUS アカウンティング検査をイネーブルにします。デフォルト値を変更するには、**parameters** コマンドのページと、RADIUS アカウンティング コンフィギュレーション モードから入力する各コマンドのページを参照してください。

関連コマンド

コマンド	説明
parameters	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。
class-map type management	アクションを適用するセキュリティ アプライアンスに宛てたレイヤ 3 またはレイヤ 4 の管理トラフィックを識別します。
show および **clear service-policy**	サービス ポリシーの設定を表示および消去します。
debug inspect radius-accounting	RADIUS アカウンティング検査をデバッグします。
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。

inspect rsh

RSH アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rsh** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect rsh

no inspect rsh

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 上で、RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームをリッスンする TCP ポート番号をネゴシエートします。RSH 検査は、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次の例に示すように、RSH 検査エンジンをイネーブルにします。この例では、デフォルト ポート（514）上の RSH トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

すべてのインターフェイスに対して RSH 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect rtsp

RTSP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rtsp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect rtsp

no inspect rtsp

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　このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン　**inspect rtsp** コマンドを使用すると、セキュリティ アプライアンスが RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続が使用します。

（注）　Cisco IP/TV の場合は、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、コントロール チャネルとして、既知ポート 554 と TCP（まれに UDP）を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートしています。この TCP コントロール チャネルは、クライアント上で設定された転送モードに応じて、オーディオ/ビデオ トラフィックの伝送に使用するデータ チャネルをネゴシエートするために使用されます。

サポートされる RDT 転送は、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、および x-pn-tng/udp です。

セキュリティ アプライアンスは、Setup 応答メッセージをステータス コード 200 によって解析します。応答メッセージが内側へ進んでいる場合、サーバはセキュリティ アプライアンスの外側にあるため、サーバから内側へ来る接続用にダイナミック チャネルを開く必要があります。応答メッセージが発信の場合、セキュリティ アプライアンスでダイナミック チャネルを開く必要はありません。

RFC 2326 では、SETUP 応答メッセージにクライアント ポートとサーバのポートを含めることを規定していないため、セキュリティ アプライアンスで状態を保持し、SETUP メッセージ内のクライアント ポートを記憶しておく必要があります。QuickTime では、SETUP メッセージにクライアント ポートが設定され、サーバはサーバ ポートでのみ応答します。

RealPlayer の使用方法

RealPlayer を使用している場合、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、**access-list** コマンド文は、サーバからクライアントへと、またはその逆で追加されます。RealPlayer の場合、**Options**>**Preferences**>**Transport**>**RTSPSettings** をクリックすることで、転送モードを変更します。

RealPlayer 上で TCP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use TCP for all content** チェックボックスをオンにします。セキュリティ アプライアンス上では、検査エンジンを設定する必要はありません。

RealPlayer 上で UDP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use UDP for all content** チェックボックスをオンにします。マルチキャスト経由で入手できないライブ コンテンツに対しても同様です。セキュリティ アプライアンス上で、**inspect rtsp** *port* コマンド文を追加します。

制約事項と制限

inspect rtsp コマンドには、次の制約事項が適用されます。

- セキュリティ アプライアンスは、UDP を介したマルチキャスト RTSP メッセージも RTSP メッセージもサポートしていません。
- **inspect rtsp** コマンドは、PAT をサポートしていません。
- セキュリティ アプライアンスには、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- セキュリティ アプライアンスは、RTSP メッセージについて NAT は実行できません。その理由は、埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として、SDP ファイルに含まれているからです。パケットはフラグメント化される可能性があり、セキュリティ アプライアンスは、フラグメント化されたパケットについて NAT は実行できません。
- Cisco IP/TV では、メッセージの SDP 部分についてセキュリティ アプライアンスが実行する NAT の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Viewer と Content Manager が外部ネットワークに、サーバが内部ネットワークにある場合、Cisco IP/TV は、NAT が使用できる場合に限り動作します。
- HTTP を介して配信されるメディア ストリームは、RTSP アプリケーション検査ではサポートされません。これは、RTSP 検査が HTTP クローキング（HTTP でラップされた RTSP）をサポートしていないためです。

例

次の例に示すように、RTSP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（554 および 8554）上の RTSP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-port
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

すべてのインターフェイスに対して RTSP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug rtsp	RTSP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect sip

SIP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sip** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sip

no inspect sip

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

このコマンドは、デフォルトではディセーブルになっています。

SIP に対するデフォルトのポート割り当ては 5060 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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SIP は、IETF で定義されているように、VoIP コールをイネーブルにします。SIP は SDP と連携して、コール シグナリングを処理します。SDP は、メディア ストリームの詳細を指定します。SIP を使用すると、セキュリティ アプライアンスは、あらゆる SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP は、次の RFC に定義されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートするには、メディア接続アドレス宛のシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。これは、シグナリングが既知の宛先ポート（UDP/TCP 5060）を通じて送信されている間に、メディア ストリームがダイナミックに割り当てられるためです。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP 検査は、これらの埋め込み IP アドレスに NAT を適用します。

（注）　リモート エンドポイントから、セキュリティ アプライアンスによって保護されたネットワーク上の SIP プロキシに登録する場合、ごく特殊な条件に合致すると登録が失敗します。この条件とは、PAT がリモート エンドポイントに対して設定されている場合、SIP レジストラ サーバが外部ネットワーク上にある場合、およびエンドポイントからプロキシ サーバに送信される REGISTER メッセージの contact フィールドにポートが指定されていない場合です。

インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムで行われるユーザ間のメッセージ転送を指します。MESSAGE/INFO 方式と 202 Accept 応答は、次の RFC で定義されている IM をサポートするために使用されます。

- Session Initiation Protocol (SIP)-Specific Event Notification、RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録 / 加入が完了するといつでも受信できます。たとえば、2 つのユーザはいつでもオンラインにできますが、何時間もチャットすることはできません。そのため、SIP 検査エンジンは、設定された SIP タイムアウト値に従ってタイムアウトするピンホールを空けます。この値には、加入期間より 5 分以上長い値を設定する必要があります。加入期間は、Contact Expires 値で定義されます。通常は、30 分にします。

MESSAGE/INFO 要求は、通常、ダイナミックに割り当てられたポート（ポート 5060 を除く）を使用して送信されるため、SIP 検査エンジンを通過する必要があります。

（注）　現在サポートされているのは、チャット機能のみです。ホワイトボード、ファイル転送、およびアプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

技術的詳細

SIP 検査は、SIP のテキストベースのメッセージについて NAT を実行し、メッセージの SDP 部分に関するコンテンツの長さを再計算し、パケット長とチェックサムを再計算します。また、エンドポイントがリッスンするアドレス / ポートとして SIP メッセージの SDP 部分で指定されたポートに対して、メディア接続をダイナミックに開きます。

SIP 検査には、コールや送信元 / 宛先を識別する SIP ペイロードからの CALL_ID/FROM/TO インデックスに関するデータベースがあります。このデータベースには、SDP メディア情報フィールドに含まれていたメディア アドレスとメディア ポート、およびメディア タイプが保管されます。1 つのセッションに対して複数のメディア アドレスとポートを指定できます。RTP/RTCP 接続は、これらのメディア アドレス / ポートを使用して 2 つのエンドポイント間で開かれます。

初回のコール セットアップ（INVITE）メッセージには、既知ポート 5060 を使用する必要があります。ただし、以降のメッセージには、このポート番号を使用しなくてもかまいません。SIP 検査エンジンは、シグナリング接続のピンホールを空け、これらの接続を SIP 接続としてマークします。これは、メッセージを SIP アプリケーションに到達させ、メッセージに NAT を適用するためです。

コールがセットアップされると、SIP セッションは「一時的な」状態にあると見なされます。この状態は、宛先エンドポイントがリッスンしている RTP メディア アドレスおよびポートを示す Response メッセージが受信されるまで維持されます。1 分以内に応答メッセージが受信されなかった場合、シグナリング接続は切断されます。

最後のハンドシェイクが完了すると、コールの状態がアクティブに移行し、BYE メッセージを受信するまでシグナリング接続が維持されます。

内部エンドポイントから外部エンドポイントにコールを開始する場合は、内部エンドポイントからの INVITE メッセージに指定される内部エンドポイントのメディア アドレスおよびメディア ポートに RTP/RTCP UDP パケットが転送されるように、外部インターフェイスに対してメディア ホールが空けられます。内部インターフェイスへの非送信請求 RTP/RTCP UDP パケットは、セキュリティ アプライアンス コンフィギュレーションで特別に許可されている場合を除き、セキュリティ アプライアンスを通過しません。

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、このタイムアウトは設定変更できるため、期間を増減して設定できます。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect sip** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect sip** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SIP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（5060）上の SIP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

すべてのインターフェイスに対して SIP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
debug sip	SIP のデバッグ情報をイネーブルにします。
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。

inspect skinny

SCCP（Skinny）アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect skinny** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect skinny

no inspect skinny

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Skinny（または Simple）Client Control Protocol（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境で共存できます。Cisco CallManager を併用することで、SCCP クライアントは、H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション レイヤ機能は、SCCP バージョン 3.3 を認識します。アプリケーション レイヤ ソフトウェアの機能により、SCCP シグナリング パケットの NAT を実行して、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できることが保証されます。

SCCP プロトコルのバージョンには、2.4、3.0.4、3.1.1、3.2、および 3.3.2 の 5 つがあります。セキュリティ アプライアンスは、バージョン 3.3.2 までのバージョンをすべてサポートします。また、SCCP の PAT および NAT を両方サポートします。IP Phone で使用するグローバル IP アドレスの数を制限している場合は、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックは、SCCP を使用します。また、特に設定しない限り、SCCP 検査によって処理されます。セキュリティ アプライアンスは、DHCP option 150 および DHCP option 66 もサポートしているため、TFTP サーバの場所を Cisco IP Phone や他の DHCP クライアントに送信できます。詳細については、**dhcp-server** コマンドを参照してください。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone よりもセキュリティの高いインターフェイス上にあるトポロジにおいて、Cisco CallManager IP アドレスの NAT が必要になる場合、Cisco IP Phone では Cisco CallManager IP アドレスをそのコンフィギュレーションで明示的に指定する必要があるため、マッピングは**スタティック**にする必要があります。ID スタティック エントリを使用した場合、高セキュリティ インターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。

Cisco IP Phone は、TFTP サーバにアクセスして、Cisco CallManager サーバへの接続時に必要となるコンフィギュレーション情報ダウンロードする必要があります。

Cisco IP Phone が TFTP サーバよりもセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して、UDP ポート 69 上で保護された TFTP サーバに接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、「ID」スタティック エントリにする必要はありません。NAT を使用する場合、ID スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスおよびポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager よりもセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone で接続を開始できるようにするためのアクセス リストまたはスタティック エントリは必要ありません。

制約事項と制限

次に、SCCP に対する現行バージョンの PAT および NAT サポートに適用される制限を示します。

- PAT は、**alias** コマンドを使用するコンフィギュレーションは扱いません。
- 外部 NAT または PAT は**サポートされません**。

（注）　現在、SCCP コールのステートフル フェールオーバーは、コール セットアップ中のコールを除いて、サポートされています。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、セキュリティ アプライアンスは、現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。セキュリティ アプライアンスは、TFTP メッセージの NAT をサポートしており、TFTP ファイル用のピンホールを空けて、セキュリティ アプライアンスを通過するようにしますが、電話機の登録中に TFTP を使用して転送される Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれている Cisco CallManager IP アドレスとポートは変換できません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect skinny** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect skinny** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SCCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2000）上の SCCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

すべてのインターフェイスに対して SCCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
show skinny	セキュリティ アプライアンスを介して確立された SCCP セッションに関する情報を表示します。
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。

inspect snmp

SNMP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect snmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect snmp *map_name*

no inspect snmp *map_name*

シンタックスの説明

map_name	SNMP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(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

inspect snmp コマンドは、SNMP マップに関する設定値を使用して SNMP 検査をイネーブルにするために使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP トラフィックを特定のバージョンの SNMP に制限するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。

以前のバージョンの SNMP はセキュリティ レベルが低いため、セキュリティ ポリシーで SNMP トラフィックをバージョン 2 に制限することが必要となる場合があります。特定のバージョンの SNMP を拒否するには、SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP マップを設定したら、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**service-policy** コマンドを使用して、1 つまたは複数のインターフェイスにマップを適用します。

例

次の例では、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義し、SNMP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

すべてのインターフェイスに対して厳密な SNMP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect sqlnet

Oracle SQL*Net アプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect sqlnet** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sqlnet

no inspect sqlnet

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

このコマンドは、デフォルトではイネーブルになっています。

デフォルトのポート割り当ては 1521 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
クラス 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
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SQL*Net プロトコルは種々のパケット タイプで構成されています。セキュリティ アプライアンスは、セキュリティ アプライアンスの両側でデータ ストリームが Oracle アプリケーションに同一に見えるように、これらのパケット タイプを処理します。

SQL*Net のデフォルトのポート割り当ては 1521 です。この値は、Oracle for SQL*Net で使用されるものですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。**class-map** コマンドを使用して、一定範囲のポート番号に SQL*Net 検査を適用します。

セキュリティ アプライアンスは、すべてのアドレスの NAT を実行し、パケット内の埋め込みポートをすべて検索して、SQL*Net バージョン 1 用に開きます。

SQL*Net バージョン 2 では、データ長が 0 の REDIRECT パケットの直後に続くすべての DATA または REDIRECT パケットがフィックスアップされます。

フィックスアップを必要とするパケットには、埋め込みホスト / ポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の TNSFrame タイプ（Connect、Accept、Refuse、Resend、および Marker）では、NAT 対象のアドレスを検出するためのスキャンは実行されません。また、検査によってパケット内の埋め込みポートに対してダイナミック接続が開かれることもありません。

SQL*Net バージョン 2 の TNSFrames パケット、Redirect パケット、および Data パケットは、直前に、ペイロードのデータ長が 0 である REDIRECT TNSFrame タイプがある場合は、開くポートおよび NAT 対象のアドレスを検出するためにスキャンされます。データ長が 0 の Redirect メッセージがセキュリティ アプライアンスを通過すると、次に到着する Data または Redirect メッセージが NAT 対象で、ポートがダイナミックに開かれることを示すために、接続データ構造にフラグが設定されます。前述の TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net 検査エンジンは、新しいメッセージと古いメッセージの長さのデータを使用して、チェックサムを再計算し、IP/TCP の長さを変更し、シーケンス番号と確認応答番号を再調整します。

その他すべてのケースでは、SQL*Net バージョン 1 の使用が前提となっています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、および Data）とすべてのパケットがスキャンされ、ポートとアドレスが検出されます。アドレスに NAT が適用され、ポート接続が開かれます。

例

次の例に示すように、SQL*Net 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1521）上の SQL*Net トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

すべてのインターフェイスに対して SQL*Net 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug sqlnet	SQL*Net のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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	SQL*Net など、さまざまな接続タイプの接続状態を表示します。

inspect sunrpc

Sun RPC アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc

no inspect sunrpc

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Sun RPC アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、ポリシー マップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。このモードには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用してアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc コマンドは、Sun RPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスは、システム上のどのポートでも動作可能です。クライアントからサーバ上の Sun RPC サービスにアクセスする場合は、サービスが動作しているポートを検出する必要があります。検出するには、既知ポート 111 上のポートマッパー プロセスにクエリーします。

クライアントは、サービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点で、クライアント プログラムはその新しいポートに Sun RPC クエリーを送信します。サーバから応答が送信されると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポート上で TCP および UDP の両方の初期接続を開きます。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

例

次の例に示すように、RPC 検査エンジンをイネーブルにします。この例では、デフォルト ポート（111）上の RPC トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して RPC 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されたコンフィギュレーションを削除します。
clear sunrpc-server active	NFS や NIS など、特定のサービスの Sun RPC アプリケーション検査で空けられたピンホールを消去します。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションに関する情報を表示します。
sunrpc-server	NFS や NIS などの Sun RPC サービスに対して、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービスに対して空けられたピンホールを表示します。

inspect tftp

TFTP アプリケーション検査をディセーブルにする場合、またはディセーブルの状態からイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect tftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ftp

no inspect tftp

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

このコマンドは、デフォルトではイネーブルになっています。

デフォルトのポート割り当ては 69 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
クラス 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
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RFC 1350 で規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバとクライアント間でファイルの読み書きを行うための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じて接続と変換をダイナミックに作成して、TFTP クライアントとサーバ間のファイル転送を許可します。特に、検査エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）およびエラー通知（ERROR）を検査します。

有効な読み取り（RRQ）要求または書き込み（WRQ）要求が受信されると、必要に応じて、ダイナミック セカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、後で TFTP によってファイル転送またはエラー通知に使用されます。

セカンダリ チャネル上でトラフィックを開始できるのは、TFTP サーバのみです。また、TFTP クライアントとサーバ間に存在できる不完全なセカンダリ チャネルは最大で 1 つです。サーバからエラー通知が送信されると、セカンダリ チャネルは閉じられます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用される場合は、TFTP 検査をイネーブルにする必要があります。

例

次の例に示すように、TFTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（69）上の TFTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

すべてのインターフェイスに対して TFTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。

inspect xdmcp

XDMCP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect xdmcp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect xdmcp

no inspect xdmcp

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

このコマンドは、デフォルトではディセーブルになっています。

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
クラス 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
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは、確立後は TCP を使用します。

ネゴシエーションを成功させ、XWindows セッションを正常に起動するには、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP バック接続を許可する必要があります。バック接続を許可するには、セキュリティ アプライアンス上で **established** コマンドを使用します。XDMCP がディスプレイ送信用ポートをネゴシエートすると、**established** コマンドが参照され、このバック接続を許可する必要があるかどうかが確認されます。

XWindows セッション中は、管理者は既知ポート 6000 | n 上で Xserver ディスプレイと通信します。次の端末設定を行うと、各ディスプレイが Xserver に個別に接続されます。

```
setenv DISPLAY Xserver:n
```

ここで、*n* は、ディスプレイの番号です。

XDMCP を使用すると、ディスプレイが IP アドレスを使用してネゴシエートされます。この IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を実行できるものです。XDCMP 検査は、PAT をサポートしていません。

例

次の例に示すように、XDMCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（177）上の XDMCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

すべてのインターフェイスに対して XDMCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
debug xdmcp	XDMCP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
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。