CHAPTER 15

inspect ctiqbe ～ inspect xdmcp コマンド

inspect ctiqbe

Computer Telephony Interface Quick Buffer Encoding（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します。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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートする CTIQBE プロトコルをイネーブルにします。これにより、Cisco IP SoftPhone および他の Cisco TAPI/JTAPI アプリケーションと Cisco CallManager を相互運用して、FWSM 経由でコールをセットアップできます。

Telephony Application Programming Interface（TAPI）および Java Telephony Application Programming Interface（JTAPI）は、多数の Cisco VoIP アプリケーションによって使用されています。CTIQBE は、Cisco TAPI Service Provider（TSP）により、Cisco CallManager と通信するために使用されます。

CTIQBE アプリケーション検査を使用する場合、次の制限が適用されます。

- CTIQBE アプリケーション検査では、**alias** コマンドを使用した設定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*されません*。
- **debug ctiqbe** コマンドを使用すると、メッセージの伝送が遅くなり、リアルタイム環境のパフォーマンスに影響することがあります。このデバッグまたはロギングをイネーブルにすると、Cisco IP SoftPhone が、FWSM 経由のコール セットアップを完了できないように認識され、Cisco IP SoftPhone を実行しているシステム上の Cisco TSP 設定のタイムアウト値が増加します。
- CTIQBE アプリケーション検査では、複数の TCP パケットに分割された CTIQBE メッセージはサポート*されません*。

特定の状況で CTIQBE アプリケーション検査を使用する場合には、次の特殊な考慮事項が必要です。

- 2 つの Cisco IP SoftPhone が、異なる Cisco CallManager に登録され、FWSM の異なるインターフェイスに接続している場合、これらの 2 つの SoftPhone 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 の IP アドレスに NAT または外部 NAT が必要な場合には、マッピングをスタティックにする必要があります。Cisco IP SoftPhone では、PC 上の Cisco TSP 設定に Cisco CallManager の IP アドレスが明示的に指定されている必要があるからです。
- PAT または外部 PAT を使用し、Cisco CallManager の 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、TCP ポート 2748 が、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プされている必要があります。CTIQBE の待ち受けポート（TCP 2748）は固定ポートなので、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP 上でユーザが設定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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

位置を判別する場合、**inspect ctiqbe** コマンドは、トンネル デフォルト ゲートウェイ 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 ルートは、**route** *interface* **0 0** *metric* **tunneled** 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 ルートを書き換えます。したがって、VPN トラフィックに **inspect ctiqbe** コマンドを適用する場合には、トンネル デフォルト ゲートウェイ 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てください。

例

次に、CTIQBE インスペクション エンジンをイネーブルにし、CTIQBE トラフィックをデフォルト ポート（2748）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
show conn	各接続タイプの接続状態を表示します。
show ctiqbe	FWSM で確立された CTIQBE セッションの情報を表示します。CTIQBE インスペクション エンジンによって割り当てられたメディア接続の情報が表示されます。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

inspect dns

（ディセーブルに設定されていた）DNS 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 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します。DNS パケットの最大長を指定するには、**inspect dns** コマンドを使用します。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 [***maximum-length*** *max_pkt_length*]

no inspect dns [***maximum-length*** *max_pkt_length*]

シンタックスの説明

maximum-length	（任意）DNS パケットの最大長を指定します。デフォルトは、512 です。**maximum-length** オプションを指定しないで **inspect dns** コマンドを入力すると、DNS パケットのサイズはチェックされません。
max_pkt_length	DNS パケットの最大長を指定します。最大長より長いパケットは、ドロップされます。

デフォルト

このコマンドは、デフォルトでイネーブルです。

DNS パケット サイズのデフォルトの **maximum-length** は、512 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol dns** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン　DNS ガードは、FWSM により DNS 応答が転送されるとすぐに、DNS クエリーに関連づけられた DNS セッションを廃棄します。また、DNS ガードは、メッセージ交換をモニタし、DNS 応答の ID が DNS クエリーの ID と一致しているかどうかを確認します。

DNS 検査がイネーブルの場合（デフォルト）、FWSM は次の処理を実行します。

- **alias**、**static**、および **nat** コマンド（DNS リライト）を使用して完了した設定に基づいて、DNS レコードを変換します。変換の対象になるのは、DNS 応答の A レコードだけです。したがって、PRT レコードを要求するリバース検索は、DNS リライトの影響を受けません。

（注）　DNS リライトは、PAT には適用されません。各 A レコードには複数の PAT ルールを適用できるので、使用する PAT ルールが明確ではないからです。

- DNS メッセージの最大長を使用します（デフォルトは 512 バイトで、最大長は 65535 バイトです）。パケット長が設定された最大長未満であることを確認するために、必要に応じて、再構成を実行します。最大長を超えているパケットは、ドロップされます。

（注）　**maximum-length** オプションを指定しないで **inspect dns** コマンドを入力すると、DNS パケットのサイズはチェックされません。

- ドメイン名の長さは 255 バイト、ラベルの長さは 63 バイトを使用します。
- DNS メッセージに圧縮ポインタが含まれている場合、ポインタが参照するドメイン名の完全性を確認します。
- 圧縮ポインタのループが存在しないかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間にあり、こ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）が同じである場合、これらのセッションに対応する接続が 1 つ作成されます。DNS の ID 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作動します。

app_id は別々に期限切れになるため、正規の DNS 応答が FWSM を通過できるのは特定の期間に限定され、リソースは構築されません。ただし、**show conn** コマンドを入力すると、新しい DNS セッションによってリセットされる DNS 接続のアイドル タイマーが表示されます。これは、共有された DNS 接続の性質によるものであり、設計上の仕様です。

DNS リライトの動作

DNS 検査をイネーブルにすると、DNS リライトにより、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 が完全にサポートされます。

内部ネットワーク上のクライアントが、外部インターフェイス上の DNS サーバに対して内部アドレスの DNS 解決を要求すると、DNS の A レコードが正しく変換されます。DNS インスペクション 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 つの処理を実行します。

- DNS クライアントがプライベート インターフェイス上に存在する場合、*DNS 応答*のパブリック アドレス（ルーティング可能または「マップされた」アドレス）を、プライベート アドレス（「実」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイス上に存在する場合、プライベート アドレスをパブリック アドレスに変換します。

DNS 検査がイネーブルであれば、**alias**、**static**、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構文および機能の詳細は、各コマンドの説明を参照してください。

例

次に、DNS パケットの最大長を、1500 バイトに変更する例を示します。DNS 検査はデフォルトでイネーブルですが、DNS トラフィックを識別し、ポリシー マップを適切なインターフェイスに適用するには、トラフィック マップを作成する必要があります。

```
hostname(config)# class-map dns-port
hostname(config-cmap)# match port udp eq 53
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
hostname(config-pmap-c)# inspect dns maximum-length 1500
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 DNS パケットの最大長を変更するには、**interface outside** の代わりに、**global** パラメータを使用します。

次に、DNS をディセーブルにする例を示します。

```
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
hostname(config-pmap-c)# no inspect dns
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

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	特定のセキュリティ アクションにクラス マップを対応付けます。
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

拡張 SMTP 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 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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

ESMTP アプリケーション検査は、FWSM を通過できる SMTP コマンドのタイプを制限し、モニタ機能を追加することによって、SMTP ベースの攻撃に対する保護を強化します。

inspect esmtp コマンドにより拡張 SMTP アプリケーション検査をイネーブルにすると、制御プレーンのパス処理で検査が実行されます。つまり、FWSM 上の単一の汎用プロセッサ上で実行されます。

ESMTP は、SMTP プロトコルを拡張したもので、大部分は SMTP と類似しています。便宜上、このマニュアルでは、SMTP と ESMTP の両方に SMTP という用語を使用しています。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同様で、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するコマンドのほとんどは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションのほうが、はるかに高速で、配信ステータスの通知など、信頼性とセキュリティに関して、より多くのオプションを使用できます。

inspect esmtp コマンドには、**inspect smtp** コマンドの機能に加え、一部の拡張 SMTP コマンドのサポートが追加されています。拡張 SMTP アプリケーション検査には、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、および VRFY の 8 つの拡張 SMTP コマンドの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、RSET）のサポートを加え、FWSM は、合計 15 の SMTP コマンドをサポートしています。

ATRN、STARTLS、ONEX、VERB、CHUNKING などの他の拡張 SMTP コマンド、およびプライベートな拡張機能はサポート対象外です。サポートされないコマンドは X に変換され、内部サーバにより拒否されます。この場合、「500 Command unknown: 'XXX'」などのメッセージが生成されます。不完全なコマンドは、廃棄されます。

（注）　ポリシー マップに、**inspect smtp** コマンドと **inspect esmtp** コマンドの両方が含まれている場合、ポリシー マップに最初にリストされているコマンドが、トラフィックの照合に使用されます。

inspect esmtp コマンドは、サーバ SMTP バナーの「2」および「0」以外の文字をアスタリスクに変更します。CR（復帰）および LF（改行）の文字は、無視されます。

SMTP 検査をイネーブルにすると、ルールに適合していない場合、対話型 SMTP に使用される Telnet セッションが停止することがあります。ルールとは、SMTP コマンドの長さが最低 4 文字である、CR および LF で終了している、次の応答を発信する前に相手側からの応答を待機する必要がある、などです。

SMTP サーバは、クライアント要求に対して、数値の応答コードおよび任意の判読可能文字列を使用して応答します。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およびサーバが戻すメッセージを制御し、削減します。SMTP 検査が実行するのは、次の 3 つの主要タスクです。

- SMTP 要求を、7 つの基本 SMTP コマンドおよび 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査追跡を生成します ― メール アドレスに含まれている無効文字が置換された場合、監査レコード 108002 が生成されます。詳細は、RFC 821 を参照してください。

SMTP 検査は、コマンド応答シーケンスをモニタし、次の異常がないかどうかを確認します。

- コマンドの短縮
- コマンドの不正な終了（<CR> <LR> で終了していない）
- MAIL および RCPT コマンドは、メールの送信者および受信者を指定します。メール アドレスはスキャンされ、不正文字が含まれていないかどうかが確認されます。縦棒 | は削除されます（ブランクに変更されます）。| が許可されるのは、メール アドレスを定義するために使用され、| の前に [<] が付いている場合だけです。
- SMTP サーバによる予期せぬ変更
- 不明なコマンドの場合、FWSM 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、クライアントにエラー コードを生成します。パケットの内容が変更されるので、TCP チェックサムを再計算するか、調整する必要があります。
- TCP ストリームの編集
- コマンドのパイプライン化

例

次に、SMTP インスペクション エンジンをイネーブルにし、SMTP トラフィックをデフォルト ポート（25）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
debug smtp	SMTP のデバッグ情報をイネーブルにします。
inspect smtp	標準（拡張ではない）SMTP アプリケーション検査をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
show conn	SMTP を含む各種の接続タイプの接続ステートを表示します。

inspect ftp

FTP（ファイル転送プロトコル）検査のポートを設定する、または拡張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 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します。設定を削除するには、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 マップの名前を指定します。
strict	（任意）FTP トラフィックの拡張検査をイネーブルにし、RFC 標準との適合を強制します。

注意　FTP を上位のポートに移動する場合には、注意が必要です。たとえば、FTP ポートを 2021 に設定すると、ポート 2021 に対して開始されるすべての接続のデータ 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

デフォルトでは、FWSM はポート 21 で FTP を待ち受けます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol ftp** コマンドに代わり、このコマンドが追加されました。

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、4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続の準備
- ***ftp*** コマンド応答シーケンスの追跡
- 監査追跡の生成
- IP アドレスに組み込まれた NAT（ネットワーク アドレス変換）

FTP アプリケーション検査は、FTP データ転送用のセカンダリ チャネルを準備します。これらのチャネルは、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 リストのイベントに対して割り当てられ、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 または PASV コマンドによりネゴシエートされます。

（注）　**no inspect ftp** コマンドを使用して FTP インスペクション エンジンをディセーブルにした場合、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 要求内に組み込まれたコマンドを送信するのを防止します。各 ***ftp*** コマンドは、新しいコマンドが許可される前に、確認応答される必要があります。組み込みコマンドを送信している接続は、ドロップされます。**strict** オプションは、FTP サーバに 227 コマンドの生成だけを許可し、FTP クライアントに PORT コマンドの生成だけを許可します。227 コマンドおよび PORT コマンドは、エラー文字列内に表示されないようにチェックされます。

注意　***strict*** オプションを使用すると、RFC 標準に適合していない FTP クライアントが中断されることがあります。

strict オプションをイネーブルにすると、各 ***ftp*** コマンド応答シーケンスが追跡され、次の異常がないかどうかが確認されます。

- コマンドの短縮 — PORT および PASV 応答コマンドのカンマ数が 5 であるかどうかが確認されます。5 以外の場合、PORT コマンドは短縮されているとみなされ、TCP 接続は終了します。
- 不正コマンド — 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。これらの文字で終了していない場合、接続は終了します。
- RETR および STOR コマンドのサイズ — 固定定数に対してチェックされます。サイズが超過している場合、エラー メッセージがロギングされ、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、つね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。これにより、ユーザが [227 xxxxx a1, a2, a3, a4, p1, p2] を実行する場合、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
- 無効のポート ネゴシエーション — ネゴシエートされたダイナミック ポート値が 1024 未満である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ので、ネゴシエートされたポートがこの範囲内である場合、TCP 接続が使用できます。
- コマンドのパイプライン化 — PORT および PASV 応答コマンドのポート番号後の文字数が、定数値 8 とクロスチェックされます。8 を超えている場合、TCP 接続は終了します。

- FWSM は、サーバのシステム タイプが FTP クライアントに対して不明になるように、FTP サーバの応答を、一連の X を伴う SYST コマンドに置換します。このデフォルトの動作を変更するには、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）　FWSM の通過が許可されない特定の FTP コマンドを識別するには、FTP マップを指定し、**request-command deny** コマンドを使用します。詳細は、**ftp-map** コマンドおよび **request-command deny** コマンドの説明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。

- 検索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** コマンドがチェックされ、RETR または STOR、および検索と保存のコマンドがロギングされているかどうかが確認されます。
- IP アドレスを提供するテーブルを検索し、ユーザ名が取得されます。
- 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ギングされます。
- メモリ不足によりセカンダリ ダイナミック チャネルの準備に失敗すると、監査レコード 201005 が生成されます。

NAT の併用により、FTP アプリケーション検査は、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。詳細は、RFC 959 に記載されています。

例

次に、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、ポリシーを外部インターフェイスに適用する例を示します。

```
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上で厳密な 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、データ接続用は指定しません。FWSM のステートフル インスペクション エンジンは、必要に応じて、データ接続をダイナミックに準備します。

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トラフィック クラスを定義します。
mask-syst-reply	クライアントからの FTP サーバ応答を非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
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設定するか、または GTP トラフィックまたはトンネルを制御するように GTP マップを定義するには、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します。このコマンドを削除するには、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、特殊なライセンスが必要です。必要なライセンスを取得せずに、FWSM 上で **inspect gtp** コマンドを入力すると、FWSM にエラー メッセージが表示されます。

シンタックスの説明

map_name	（任意）GTP マップの名前を指定します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

GTP は、GPRS のトンネリング プロトコルで、ワイヤレス ネットワーク上のセキュアなアクセスを支援します。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 サブスクライバに対して、企業ネットワークおよびインターネットへの、中断されないパケット交換データ サービスを提供します。GTP の概要については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』の「Applying Application Layer Protocol Inspection」の章を参照してください。

GTP パラメータの定義に使用する特定のマップを識別するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、コンフィギュレーション モードが開始され、具体的なマップを定義するための各種コマンドを入力できます。条件を満たしていないメッセージに指定できる動作は、**allow**、**reset**、または **drop** などの各種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。これらの動作のほかに、イベントをロギングするかどうかを指定できます。

GTP マップを定義したあと、**inspect gtp** コマンドを使用して、マップをイネーブルにします。次に、**class-map**、**policy-map**、および **service-policy** コマンドを使用して、トラフィック クラスを定義したり、このクラスに **inspect** コマンドを適用したり、1 つまたは複数のインターフェイスにポリシーを適用したりします。

ポート値として使用される **gtp** の文字列は、ポート値 3386 に自動的に変換されます。GTP の既知ポートは、次のとおりです。

- 3386
- 2123

次の機能は、7.0 ではサポートされません。

- NAT（ネットワーク アドレス変換）、PAT（ポート アドレス変換）、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、2152 以外のポート
- トンネル化した IP パケットおよびそのコンテンツの評価

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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

位置を判別する場合、**inspect gtp** コマンドは、トンネル デフォルト ゲートウェイ 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 ルートは、**route** *interface* **0 0** *metric* **tunneled** 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 ルートを書き換えます。したがって、VPN トラフィックに **inspect gtp** コマンドを適用する場合には、トンネル デフォルト ゲートウェイ 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てください。

例

次に、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、外部インターフェイスにポリシーを適用する例を示します。

```
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） この例では、デフォルト値を使用して GTP 検査をイネーブルにしています。デフォルト値を変更するには、**gtp-map** コマンドの説明、および 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説明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 検査の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。

inspect h323

H.323 アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect h323 {**h225** [*h225_map*] | **ras**}

no inspect h323 {**h225** [*h225_map*] | **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。
h225_map	（任意）Cisco HSI および H.323 エンドポイントを含むトポロジで FWSM を使用するために必要なコンフィギュレーションを定義する、H.225 アプリケーション検査マップの名前を指定します。
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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol h323** コマンドに代わり、このコマンドが追加されました。

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 準拠アプリケーションをサポートします。H.323 は、LAN 上でのマルチメディア会議用として、International Telecommunication Union（ITU; 国際電気通信連合）により定義されたプロトコル スイートです。FWSM は、H.323 v3 の単一コール シグナリング チャネル上での複数コール機能を含む、H.323 Version 4 をサポートしています。

H.323 検査をイネーブルにすると、FWSM は、H.323 Version 3 で導入された、単一コール シグナリング チャネル上での複数コールをサポートします。この機能により、コール セットアップ時間が短縮され、FWSM 上のポート使用率も削減されます。

H.323 検査には、次の 2 つの主要機能があります。

- H.225 および H.245 メッセージに組み込まれた必要な IPv4 アドレスの NAT（ネットワーク アドレス変換）。H.323 メッセージは、PER コード化形式でコード化されるので、FWSM は、H.323 メッセージのデコードに、ASN.1 デコーダを使用します。
- ネゴシエートされた H.245 および RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 の一連のプロトコルでは、2 つまでの TCP 接続および 4 ～ 6 の UDP 接続を集約的に使用できます。登録、アドミッション、およびステータス用に、FastStart は単一の TCP 接続だけを使用し、RAS は単一の UDP 接続を使用します。

H.323 クライアントは、Q.931 コール セットアップを要求するために、最初に TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立することがあります。コール セットアップ プロセスの一環として、H.323 端末はクライアントに、H.245 TCP 接続用のポート番号を提供します。H.245 接続は、コールのネゴシエーションおよびメディア チャネルのセットアップに使用されます。H.323 ゲートキーパを使用する環境では、初回パケットは UDP を使用して転送されます。

H.323 検査は、Q.931 TCP 接続をモニタして、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、FWSM 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）　また、RAS を使用する場合にも、H.225 接続はダイナミックに割り当てられます。

各 H.245 メッセージで、H.323 の両エンドポイントは、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、これらのポートを判別し、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 制御チャネルは、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 — ゲートキーパの検出に使用される UDP ポート
- 1719 — RAS およびゲートキーパの検出に使用される UDP ポート
- 1720 — TCP 制御ポート

ゲートキーパからの ACF メッセージが FWSM を通過する場合には、H.225 接続用のピンホールがオープンされます。H.245 シグナリング ポートは、H.225 シグナリングの両エンドポイント間でネゴシエートされます。H.323 ゲートキーパを使用する場合には、FWSM は、ACF メッセージの検査に基づいて H.225 接続をオープンします。FWSM が ACF メッセージを検出しない場合には、H.225 コール シグナリング用に、既知 H.323 ポート 1720 にアクセス リストをオープンしなければならないことがあります。

FWSM は、H.225 メッセージの検査後に H.245 チャネルをダイナミックに割り当て、H.245 チャネルに接続し、回復します。つまり、FWSM を通過する H.245 メッセージはすべて、H.245 アプリケーション検査の対象となり、組み込み 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 チャネルがオープンされます。

H.323 ITU 規格では、信頼できる接続に渡す前に、H.225 および H.245 の前にメッセージ長を定義する TPKT ヘッダーを送信するよう規定しています。TPKT ヘッダーは、H.225 または H.245 メッセージと同じ TCP パケットで送信する必要はないので、FWSM は、メッセージを適切に処理またはデコードできるように TPKT の長さを記録しておく必要があります。FWSM は、各接続のデータ構造、つまり次に予測されるメッセージの TPKT 長を含むデータ構造を保持します。

NAT が必要な IP アドレスがある場合、FWSM はチェックサム、User-User Information Element（UUIE）長、および TPKT（H.225 メッセージが TCP パケットに含まれていた場合）を変更する必要があります。TPKT が異なる TCP パケットで送信された場合、FWSM はその TPKT にプロキシ ACK を実行し、新しい長さの H.245 メッセージに新しい TPKT を付加します。

（注）　FWSM は、TPKT の プロキシ ACK では、TCP オプションをサポートしません。

H.323 検査対象の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** コマンドにより設定された H.323 タイムアウトに従って、タイムアウトになります。

制限および制約

H.323 アプリケーション検査の使用については、次のような既知の問題および制限事項があります。

- スタティック PAT（ポート アドレス変換）では、H.323 メッセージのオプション フィールドに組み込まれた IP アドレスが適切に変換されないことがあります。この問題が発生した場合には、H.323 にスタティック PAT を使用しないでください。
- NetMeeting クライアントが H.323 ゲートキーパに登録し、同じ H.323 ゲートキーパに登録されている H.323 ゲートウェイを呼び出そうと、接続は確立されますが、どちらの方向でも音声は認識されません。この問題は、FWSM とは無関係です。
- 設定したネットワーク 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一致している場合、すべての発信 H.323 接続に失敗します。

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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

位置を判別する場合、**inspect h323** コマンドは、トンネル デフォルト ゲートウェイ 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 ルートは、**route** *interface* **0 0** *metric* **tunneled** 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 ルートを書き換えます。したがって、VPN トラフィックに **inspect h323** コマンドを適用する場合には、トンネル デフォルト ゲートウェイ 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てください。

H.225 マップの使用方法

H.225 マップにより、H.225 コール シグナリングに HSI が含まれている場合、FWSM で H.245 接続用のダイナミックなポート固有のピンホールをオープンできます。H.225 マップは、HSI および関連するエンドポイントの情報を提供します。これらは、FWSM によって保護されているネットワークのセキュリティを損なわずに接続を確立するために必要な情報です。

表 15-1 に、必要なコンフィギュレーションを実行するためのコマンドの要約を示します。

表 15-1　H.225 コンフィギュレーション コマンド

コマンド	コンフィギュレーション モード	説明
h225-map	グローバル コンフィギュレーション モード	H.225 アプリケーション検査マップを定義し、H.225 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。1 つの H.225 マップに、最大 5 つの HSI グループを設定できます。
hsi-group	H.225 マップ コンフィギュレーション モード	HSI グループを定義し、HSI グループ コンフィギュレーション モードをイネーブルにします。各 HSI グループに、最大 10 のエンドポイントを設定できます。

表 15-1　H.225 コンフィギュレーション コマンド（続き）

コマンド	コンフィギュレーション モード	説明
hsi	HSI グループ コンフィギュレーション モード	HSI を識別します。
endpoint	HSI グループ コンフィギュレーション モード	HSI グループ内の 1 つまたは複数のエンドポイントを識別します。

例

次に、H.323 インスペクション エンジンをイネーブルにし、H.323 トラフィックをデフォルト ポート（1720）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で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。

次に、FWSM が H.323 エンドポイントと相互接続し、Cisco CallManager で両エンドポイント間の接続を確立する場合に必要な H.225 コンフィギュレーションの例を示します。

```
hostname(config)# access-list h323_acl permit udp any any eq 1720
hostname(config)# access-list h323_acl permit udp any any eq 1721
hostname(config)# class-map h323-traffic
hostname(config-cmap)# match access-list h323_acl
hostname(config-cmap)# exit
hostname(config)# h225-map sample_map
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
hostname(config-h225-map-hsi-grp)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class h323_port
hostname(config-pmap-c)# inspect h323 ras
hostname(config-pmap-c)# inspect h323 h225 sample_map
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報表示をイネーブルにします。
show h225	FWSM によって確立された H.225 セッションの情報を表示します。
show h245	低速起動を使用するエンドポイントによって FWSM に確立された H.245 セッションの情報を表示します。
show h323-ras	FWSM に確立された H.323 RAS セッションの情報を表示します。
timeout	H.225 シグナリング接続または H.323 制御接続が終了したあとのアイドル タイムを設定します。

inspect http

HTTP アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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	（任意）HTTP マップの名前を指定します。

デフォルト

HTTP のデフォルト ポートは、80 です。

デフォルトでは、拡張 HTTP 検査はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在廃止されている **fixup protocol http** コマンドに代わり、このコマンドが追加されました。

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付けられている可能性のある特定の攻撃および他の脅威を防御します。HTTP 検査は、次のいくつかの機能を実行します。

- 拡張 HTTP 検査
- N2H2 または Websense を使用した URL スクリーニング
- Java および ActiveX のフィルタリング

最後の 2 つの機能は、**filter** コマンドと併用して設定します。

拡張 HTTP 検査は、HTTP メッセージが RFC 2616 に適合し、RFC に定義された方式またはサポート対象の拡張方式を使用し、各種の他の条件に適合しているかどうかを検証します。ほとんどの場合、これらの条件および条件を満たしていない場合のシステム応答を設定できます。条件を満たしていないメッセージに指定できる動作は、**allow**、**reset**、または **drop** などの各種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。これらの動作のほかに、イベントをロギングするかどうかを指定できます。

HTTP メッセージに適用できる条件は、次のとおりです。

- 設定可能なリストに、いかなる方式も含まれていない
- 特定の転送コード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 仕様に準拠している

- メッセージのボディ サイズが、設定可能な制限の範囲内である
- 要求および応答メッセージのヘッダー サイズが、設定可能な制限の範囲内である
- URI の長さが、設定可能な制限の範囲内である
- メッセージ ボディのコンテンツ タイプが、ヘッダーと一致している
- 応答メッセージのコンテンツ タイプが、要求 メッセージの *accept-type* フィールドと一致している
- メッセージのコンテンツ タイプが、事前定義された内部リストに含まれている
- メッセージが HTTP RFC 形式の条件に適合している
- 選択したサポート対象アプリケーションが存在する、または存在しない
- 選択したコード化タイプが存在する、または存在しない

（注）　条件を満たしていないメッセージに指定できる動作は、**allow**、**reset**、または **drop** などの各種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。これらの動作のほかに、イベントをロギングするかどうかを指定できます。

拡張 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。HTTP トラフィックに適用するルールは、**http-map** コマンドおよび HTTP マップ コンフィギュレーション モードのコマンドを使用して設定する特定の HTTP マップによって定義します。

（注）　HTTP マップを使用して HTTP 検査をイネーブルにすると、動作のリセットとログを伴う厳密な HTTP 検査がデフォルトでイネーブルになります。検査に失敗した場合に実行される動作は変更できますが、HTTP マップがイネーブルである限り、厳密な検査をディセーブルにすることはできません。

例

次に、HTTP トラフィックを指定し、HTTP マップを定義し、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
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、FWSM は、以下を含むトラフィックを検出した場合、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 2000 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（ユニフォーム リソース識別子）

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たトラフィックの詳細情報を表示します。
http-map	拡張 HTTP 検査を設定するために HTTP マップを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。

inspect icmp

ICMP インスペクション 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します。設定を削除するには、このコマンドの **no** 形式を使用します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol icmp** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

ICMP インスペクション エンジンでは、ICMP トラフィックを TCP および UDP トラフィックと同様に検査できます。ICMP インスペクション エンジンを使用しない場合には、ACL で、ICMP の FWSM の通過を許可しないことを推奨します。ステートフル検査を使用しないと、ネットワークの攻撃に ICMP が使用されることがあります。ICMP インスペクション エンジンは、各要求に対する応答が 1 つだけで、シーケンス番号が正しいことを確認します。

ICMP 検査がディセーブル（デフォルト設定）の場合、ICMP エコー要求への応答であっても、セキュリティの低いインターフェイスからセキュリティの高い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。

ICMP インスペクションがディセーブル（デフォルト）になっている場合、トレースルートは機能しません。トレースルートを使用しているとき ICMP 到達不能エラーを受信できるようにするには、ICMP インスペクションをイネーブルにする必要があります。

例

次に、ICMP アプリケーション インスペクション エンジンをイネーブルにし、クラス マップを作成して、IPv4 の場合は 1、IPv6 の場合は 58 の ICMP プロトコル ID を使用して ICMP トラフィックを照合する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
icmp	FWSM のインターフェイスで終端する ICMP トラフィックのアクセス ルールを設定します。
policy-map	1 つまたは複数のトラフィック クラスにセキュリティ動作を関連付ける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 メッセージの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します。設定を削除するには、このコマンドの **no** 形式を使用します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol icmp error** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

スタティック /NAT（ネットワーク アドレス変換）設定に基づいて、ICMP エラー メッセージを送信する中間ホップの変換スロット（xlate）を作成するには、**inspect icmp error** コマンドを使用します。デフォルトでは、中間ホップの IP アドレスは、セキュリティ アプライアンスによって隠されていますが、**inspect icmp error** コマンドを実行すると、中間ホップの IP アドレスが見えるようになります。FWSM は、パケットを、変換した IP アドレスに書き換えます。

ICMP エラー インスペクション エンジンをイネーブルにすると、ICMP パケットに対して次の変更が実行されます。

- IP ヘッダーで、NAT IP がクライアントの IP（宛先アドレスと中間ホップ アドレス）に変更され、IP チェックサムが修正されます。
- ICMP ヘッダーで、ICMP パケットの変更に基づいて ICMP チェックサムが修正されます。
- ペイロードで、次の内容が変更されます。
  - 元のパケットの NAT IP が、クライアントの IP に変更されます。
  - 元のパケットの NAT ポートが、クライアントのポートに変更されます。
  - 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 メッセージを検索すると、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 タプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート、IP プロトコル）が検索されます。検索が実行されると、取得した 5 タプルからクライアントの元のアドレスが判別され、特定の 5 タプルに関連する既存のセッションが特定されます。セッションが見つからない場合、ICMP エラー メッセージはドロップされます。

注意　ICMP エラー インスペクションをセキュリティ レベルが異なるインターフェイス間で使用すると、内部 IP アドレスがマスクされません。このため、セキュリティ アプライアンスは中間ルータの IP アドレスの正しい変換結果を取得することができず、パケットはドロップされます。ICMP エラー インスペクションをセキュリティ レベルが同じインターフェイス間で使用すると、中間ルータの IP アドレスの変換結果が見つからなくても、セキュリティ アプライアンスは ID を想定して、IP アドレスの xlate を割り当てます。SSLC では、NAT を設定しなくてもパケットを受け取ることができるため、同じセキュリティ レベルを選択すると、（ICMP エラー メッセージの場合と同様）内部ルータの IP アドレスが公開される危険があります。

例

次に、ICMP エラー アプリケーション インスペクション エンジンをイネーブルにし、クラス マップを作成して、IPv4 の場合は 1、IPv6 の場合は 58 の ICMP プロトコル ID を使用して ICMP トラフィックを照合する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
icmp	FWSM のインターフェイスで終端する ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション 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	1 つまたは複数のトラフィック クラスにセキュリティ動作を関連付ける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、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol ils** コマンドに代わり、このコマンドが追加されました。

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 製品に NAT（ネットワーク アドレス変換）サポートを提供します。

デフォルトのポート割り当てを 389 から変更するには、*port* オプションを使用します。ILS 検査を一定範囲のポート番号に適用するには、*-port* オプションを使用します。

FWSM は、ILS または SiteServer Directory で、エンドポイントの登録および検索に使用される ILS 用の NAT をサポートします。LDAP データベースには IP アドレスだけが保管されるので、PAT（ポート アドレス変換）はサポートされません。

検索応答では、LDAP サーバが外部に存在する場合、NAT により、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が許可されるとみなされます。これらの検索応答では、最初に変換スロット（xlate）が検索され、次に DNAT エントリが検索されて、適正な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（非 NAT）を使用し、DNAT の相互通信を行わないサイトでは、パフォーマンスを向上するために、このインスペクション エンジンをオフにすることを推奨します。

ILS サーバが FWSM の境界の内側に存在する場合には、追加設定が必要になることがあります。たとえば、外部クライアントが特定のポート、一般的には TCP 389 上で LDAP サーバにアクセスできるホールが必要になります。

ILS トラフィックが発生するのはセカンダリ UDP チャネル上だけなので、TCP の休止インターバルが経過すると、TCP 接続は切断されます。デフォルトでは、このインターバルは 60 分ですが、**timeout** コマンドにより調整できます。

ILS/LDAP は、単一 TCP 接続上でセッションが処理されるクライアント / サーバ モデルに準拠しています。クライアントの動作に応じて、いくつかのセッションが作成されることがあります。

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。サーバから正常な BIND RESPONSE を受信すると、ILS Directory 上で処理を実行するために、他の操作メッセージ（ADD、DEL、SEARCH、または MODIFY）が交換されます。ADD REQUEST および SEARCH RESPONSE PDU には、H.323（SETUP および CONNECT メッセージ）で使用される、NetMeeting セッションを確立するための NetMeeting ピアの IP アドレスが含まれていることがあります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS 検査は、次の処理を実行します。

- BER デコード機能による LDAP REQUEST/RESPONSE PDU のデコード
- LDAP パケットの解析
- IP アドレスの抽出
- 必要な場合、IP アドレスの変換
- BER コード化機能による、変換したアドレスでの PDU のコード化
- TCP パケットへの、新しくコード化された PDU のコピー
- 増分 TCP チェックサムの実行およびシーケンス番号の調整

ILS 検査には、次の制限があります。

- 照会用の要求および応答はサポートされません。
- 複数ディレクトリのユーザは、統合されません。
- 複数ディレクトリに複数の ID を持つ単一ユーザは、NAT で認識できません。

（注）　H.225 コール シグナリング トラフィックが発生するのはセカンダリ UDP チャネル上だけなので、TCP の **timeout** コマンドにより指定されたインターバルが経過すると、TCP 接続は切断されます。デフォルトでは、このインターバルは 60 分です。

例

次に、ILS インスペクション エンジンをイネーブルにし、ILS トラフィックをデフォルト ポート（389）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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	特定のセキュリティ アクションにクラス マップを対応付けます。
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 mgcp

MGCP アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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	（任意）MGCP マップの名前を指定します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol mgcp** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

MGCP を使用するには、通常、最低 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、もう 1 つはコール エージェントがコマンドを受信するポート用です。通常、コール エージェント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、コール エージェントのデフォルトの 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コール制御エレメントからメディア ゲートウェイを制御する場合に使用されます。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音声信号と、インターネット上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 パケット間の変換を提供するネットワーク エレメントです。NAT（ネットワーク アドレス変換）および PAT（ポート アドレス変換）と MGCP を併用することにより、外部（グローバル）アドレス数が限定された内部ネットワーク上で、多数のデバイスをサポートできます。

メディア ゲートウェイの例は次のとおりです。

- 電話ネットワークと Voice over IP ネットワーク間のインターフェイスを提供するトランキング ゲートウェイ。これらのゲートウェイは通常、多数のデジタル回線を管理します。
- Voice over IP ネットワークに従来型のアナログ（RJ11）インターフェイスを提供するレジデンシャル ゲートウェイ。レジデンシャル ゲートウェイには、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 ワイヤレス デバイスなどが含まれます。

- Voice over IP ネットワークに従来型のデジタル PBX インターフェイスまたは統合 *ソフト PBX* インターフェイスを提供するビジネス ゲートウェイ。

MGCP メッセージは、UDP 上で伝送されます。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）に戻されますが、コマンドの送信先と同じアドレスから応答が戻されるとは限りません。たとえば、複数のコール エージェントがフェールオーバー設定で使用されている場合、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、バックアップ コール エージェントから応答が送信される場合などです。

（注）　MGCP コール エージェントは、AUEP メッセージを送信し、MGCP エンドポイントが存在するかどうかを判別します。これにより、FWSM を経由するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

1 つまたは複数のコール 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** コマンドおよび **gateway** コマンドを使用します。コマンド キューに一度に設定できる 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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

例

次に、MGCP トラフィックを指定し、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例を示します。デフォルト ポート（2427 および 2727）上で MGCP トラフィックを照合するクラス マップを作成します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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
```

次に、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 で 2 つのゲートウェイ 10.10.10.116 および 10.10.10.117 を制御するように設定する例を示します。キューに格納できる 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で 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トラフィック クラスを定義します。
debug mgcp	MGCP の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 モードを開始します。
show mgcp	FWSM を介して確立された MGCP セッションの情報を表示します。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

inspect netbios

NetBIOS アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect netbios

no inspect netbios

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1	このコマンドが追加されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコル用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設定します。

例

次に、NetBIOS インスペクション エンジンをイネーブルにし、NetBIOS トラフィックをデフォルトの UDP ポート（137 および 138）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
hostname(config)# class-map netbios-port
hostname(config-cmap)# match port udp range 137 138
hostname(config-cmap)# exit
hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class netbios-port
hostname(config-pmap-c)# inspect netbios
hostname(config-pmap-c)# exit
hostname(config)# service-policy netbios_policy interface outside
```

すべてのインターフェイス上で NetBIOS 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トラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
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

Point-to-Point Tunneling Protocol（PPTP）アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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 セッションは、1 つの TCP チャネルと、通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエーションおよび管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション検査をイネーブルにすると、PPTP 制御パケットが検査され、PPTP トラフィックを許可するために必要な GRE 接続および変換スロット（xlate）がダイナミックに作成されます。サポートされるのは、RFC 2637 に定義されている Version 1 だけです。

PAT（ポート アドレス変換）は、GRE の修正版（RFC 2637）が、PPTP TCP 制御チャネル上でネゴシエートされた場合に限り、実行されます。GRE の無修正版（RFC 1701、RFC 1702）では、PAT は実行*されません*。

具体的には、FWSM は、PPTP バージョン通知および発信コールの要求 / 応答シーケンスを検査します。RFC 2637 に定義されているように、検査されるのは PPTP Version 1 だけです。いずれかの側から通知されたバージョンが Version 1 ではない場合、TCP 制御チャネルの以降の検査はディセーブルになります。また、発信コールの要求 / 応答シーケンスが追跡されます。接続および変換スロット（xlate）は、以降のセカンダリ GRE データ トラフィックを許可するために、必要に応じて、ダイナミックに割り当てられます。

PPTP トラフィックを PAT を使用して変換するには、PPTP インスペクション エンジンをイネーブルにする必要があります。また、PAT が実行されるのは GRE の修正版（RFC 2637）が PPTP TCP 制御チャネル上でネゴシエートされる場合だけです。GRE の無修正版（RFC 1701 および RFC 1702）では、PAT は実行されません。

RFC 2637 に説明されているように、PPTP プロトコルは、主として、モデム バンク PPTP Access Concentrator（PAC）からヘッドエンド PPTP Network Server（PNS）に対して開始される PPP セッションのトンネリングに使用されます。この場合、PAC がリモート クライアント、PNS がサーバです。

ただし、Windows の VPN で使用する場合、相互通信が逆転します。PNS は、中央ネットワークへのアクセスを取得するためにヘッドエンド PAC に接続を開始する、リモートの単一ユーザ PC になります。|

例

次に、PPTP インスペクション エンジンをイネーブルにし、PPTP トラフィックをデフォルト ポート（1723）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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	特定のセキュリティ アクションにクラス マップを対応付けます。
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 rsh

RSH アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol rsh** コマンドに代わり、このコマンドが追加されました。

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 出力ストリームを待ち受ける 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（ネットワーク アドレス変換）をサポートします。

例

次に、RSH インスペクション エンジンをイネーブルにし、RSH トラフィックをデフォルト ポート（514）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
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、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol rtsp** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン　**inspect rtsp** コマンドにより、FWSM で 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 接続により使用されます。

（注）　Cisco IP/TV の場合には、RTSP TCP ポート 554 および TCP 8554 を使用します。

RTSP アプリケーションは、既知ポート 554 および制御チャネルとして TCP（まれに UDP）を使用します。FWSM は、RFC 2326 に基づいて、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上に設定された転送モードに基づいて、音声 / ビデオ トラフィックを送信するデータ チャネルのネゴシエーションに使用されます。

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。

FWSM は、ステータス コード 200 の SETUP 応答メッセージを解析します。応答メッセージが着信伝送される場合、サーバは FWSM に関連した外部にあり、サーバからの着信接続用にダイナミック チャネルをオープンする必要があります。応答メッセージが発信の場合、FWSM でダイナミック チャネルをオープンする必要はありません。

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 ポートを含める必要がないので、FWSM はステートを保持し、SETUP メッセージ内のクライアント ポートを記録しておく必要があります。QuickTime は、SETUP メッセージでクライアント ポートを指定するので、サーバはサーバ ポートだけで応答します。

RealPlayer の使用方法

RealPlayer を使用するには、転送モードを正しく設定することが重要です。FWSM では、サーバからクライアントへ、またはクライアントからサーバへの **access-list** コマンド ステートメントを追加します。RealPlayer では、**Options**>**Preferences**>**Transport**>**RTSP Settings** をクリックし、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には、**Use TCP to Connect to Server** チェックボックスおよび **Attempt to use TCP for all content** チェックボックスをオンにします。FWSM 上でインスペクション 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には、**Use TCP to Connect to Server** チェックボックスおよび **Attempt to use UDP for static content** チェックボックスを選択し、マルチキャスト経由でライブ コンテンツを使用できないように設定します。FWSM 上で、**inspect rtsp** *port* コマンド ステートメントを追加します。

制約および制限

inspect rtsp コマンドには、次の制約が適用されます。

- FWSM は、マルチキャスト RTSP または UDP 上の RTSP メッセージをサポートしません。
- **inspect rtsp** コマンドでは、PAT（ポート アドレス変換）はサポートされません。
- FWSM には、HTTP メッセージに RTSP メッセージが隠されている HTTP クローキングを認識する機能はありません。
- FWSM は、RTSP メッセージ上では NAT（ネットワーク アドレス変換）を実行できません。組み込み IP アドレスが、HTTP 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、分割されることがあります。FWSM は、分割されたパケット上で NAT を実行できません。
- Cisco IP/TV の場合、FWSM が メッセージの SDP 部分に対して実行できる NAT 数は、Content Manager のプログラム リスト数に比例します（各プログラム リストに最低 6 の組み込み IP アドレスを設定可能）。
- Apple QuickTime 4 または RealPlayer には、NAT を設定できます。Cisco IP/TV では、Viewer および Content Manager が外部ネットワーク上にあり、サーバが内部ネットワーク上にある場合に限り、NAT を使用できます。
- HTTP 上で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の対象になりません。RTSP 検査は、HTTP クローキング（HTTP に隠された RTSP）をサポートしていないからです。

例

次に、RTSP インスペクション エンジンをイネーブルにし、RTSP トラフィックをデフォルト ポート（554 および 8554）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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-traffic
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で 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	特定のセキュリティ アクションにクラス マップを対応付けます。
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、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sip [*map_name*]

no inspect sip [*map_name*]

シンタックスの説明

map_name	（任意）**sip-map** コマンドを使用して作成した SIP マップの名前を指定します。SIP マップでは、SIP マップ コンフィギュレーション モードの **ip-address-privacy** コマンドで設定できる IP アドレス プライバシなど、SIP 検査の追加検査パラメータを指定できます。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在廃止されている **fixup protocol sip** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

IETF に定義されているように、SIP は VoIP コールをイネーブルにします。SIP は、SDP と相互作用して、コール シグナリングをサポートします。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、FWSM で、すべての SIP Voice over IP（VoIP）ゲートウェイまたは VoIP プロキシ サーバをサポートできます。SIP および 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

FWSM を使用して SIP コールをサポートするには、メディア接続アドレス、メディア ポート、およびメディア用初期接続のシグナリング メッセージを検査する必要があります。シグナリングは、既知の宛先ポート（UDP/TCP 5060）上で送信されますが、メディア ストリームはダイナミックに割り当てられるからです。また、SIP は、IP パケットのユーザ データ部分に IP アドレスを組み込みます。SIP 検査では、これらの組み込み IP アドレスに対して NAT を適用します。

（注）　リモート エンドポイントが、FWSM により保護されているネットワーク上の SIP プロキシに登録しようとした場合、非常に特殊な条件のもとでは、登録に失敗します。これらの条件とは、リモート エンドポイントに PAT（ポート アドレス変換）が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存在する場合、およびエンドポイントからプロキシ サーバに送信された REGISTER メッセージの宛先フィールドにポートが設定されていない場合です。

インスタント メッセージング

Instant Messaging（IM; インスタント メッセージング）とは、ほぼリアルタイムでのユーザ間のメッセージ転送を意味します。IM をサポートするには、次の RFC に定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用します。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3248

MESSAGE/INFO 要求は、登録 / サブスクリプションのあとはいつでも着信できます。たとえば、2 人のユーザをいつでもオンラインにできますが、何時間ものチャットは実行できません。そのため、SIP インスペクション エンジンはピンホールをオープンし、設定された SIP タイムアウト値に従って、タイムアウトが発生します。タイムアウト値は、最低 5 分以上で、サブスクリプションの継続時間より長い値を設定する必要があります。サブスクリプションの継続時間は、Contract Expires 値に定義され、通常 30 分です。

MESSAGE/INFO 要求は通常、ポート 5060 以外のダイナミックに割り当てられたポートを使用して送信されるので、SIP インスペクション 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、チャット機能だけです。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、サポート対象外です。RTC クライアント 5.0 はサポートされません。

技術的な詳細

SIP 検査は、SIP のテキストベース メッセージに NAT（ネットワーク アドレス変換）を実行し、メッセージの SDP 部分のコンテンツ長を再計算し、パケット長およびチェックサムを再計算します。SIP メッセージの SDP 部分に、エンドポイントが待ち受けるアドレス / ポートとして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オープンします。

SIP 検査は、コールおよび送信元と宛先を識別する SIP ペイロードを参照し、CALL_ID/FROM/TO の各インデックスを持つデータベースを使用します。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 タイプが含まれます。1 つのセッションに、複数のメディア アドレスおよびポートを含めることができます。これらのメディア アドレスおよびポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続がオープンされます。

最初のコール 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、以降のメッセージが、このポート番号を使用するとは限りません。SIP インスペクション エンジンは、シグナリング接続ピンホールをオープンし、これらの接続を SIP 接続としてマークします。これにより、メッセージは SIP アプリケーションに到達して NAT が実行されます。

コールがセットアップされると、SIP セッションは「一時」ステートであるとみなされます。このステートは、宛先エンドポイントが待ち受ける RTP メディア アドレスとポートを示す応答メッセージを受信するまで持続します。1 分以内に応答メッセージを受信しなかった場合、シグナリング接続は切断されます。

最終ハンドシェイクが完了すると、コールはアクティブ ステートになり、BYE メッセージを受信するまでシグナリング接続は持続します。

内部エンドポイントが外部エンドポイントに対してコールを開始すると、外部インターフェイスに対してメディア ホールがオープンされ、内部エンドポイントからの INVITE メッセージに指定された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 ポートに対して、RTP/RTCP UDP パケットが通過できるようになります。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、FWSM の設定により特別に許可されていない限り、FWSM を通過しません。

メディア接続が休止状態になると、2 分以内に接続が切断されます。これは、設定可能なタイムアウト値なので、切断までの時間を、これより長い時間または短い時間に設定できます。

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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

位置を判別する場合、**inspect sip** コマンドは、トンネル デフォルト ゲートウェイ 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 ルートは、**route** *interface* **0 0** *metric* **tunneled** 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 ルートを書き換えます。したがって、VPN トラフィックに **inspect sip** コマンドが必要な場合には、トンネル デフォルト ゲートウェイ 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てください。

例

次に、SIP インスペクション エンジンをイネーブルにし、SIP トラフィックをデフォルト ポート（5060）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

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

すべてのインターフェイス上で 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トラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
show sip	FWSM を使用して確立した SIP セッションに関する情報を表示します。
show conn	各接続タイプの接続状態を表示します。
sip-map	追加の SIP 検査パラメータを定義します。

inspect skinny

SCCP（Skinny）アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在廃止されている **fixup protocol skinny** コマンドに代わり、このコマンドが追加されました。

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 環境で複数存在できます。Cisco CallManager と併用すると、SCCP クライアントと H.323 準拠端末を相互運用できます。FWSM のアプリケーション レイヤ機能は、SCCP Version 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は、すべての SCCP シグナリングおよびメディア パケットが FWSM を確実に通過できるように、SCCP シグナリング パケットの NAT を提供します。

SCCP プロトコルには、5 つのバージョンがあります。2.4、3.0.4、3.1.1、3.2、および 3.3.2 です。FWSM は、Version 3.3.2 までの全バージョンをサポートしています。FWSM は、SCCP に対して PAT および NAT の両方をサポートします。IP Phone で使用するグローバル IP アドレス数が限定されている場合には、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の標準トラフィックは、特別に設定しなくても、SCCP を使用して SCCP 検査により処理されます。また、FWSM は、DHCP オプション 150 および 66 をサポートしているので、FWSM から Cisco IP Phone および他の DHCP クライアントに、TFTP（簡易ファイル転送プロトコル）サーバの位置を送信できます。詳細は、**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 レベルが高いインターフェイス上に存在するトポロジで、Cisco CallManager の IP アドレスに NAT が必要な場合には、マッピングを**スタティック**にする必要があります。Cisco IP Phone は、設定に明示的に指定された Cisco Call Manager の IP アドレスを必要とするからです。アイデンティティがスタティックなエントリにより、セキュリティ レベルの高いインターフェイス上の Cisco CallManager で、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、Cisco CallManager サーバへの接続に必要な設定情報をダウンロードするために、TFTP（簡易ファイル転送プロトコル）サーバにアクセス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 レベルが低いインターフェイス上に存在する場合には、アクセス リストを使用して、UDP ポート 69 上の保護された 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なエントリが必要ですが、「アイデンティティ」がスタティックなエントリである必要はありません。NAT を使用する場合、アイデンティティがスタティックなエントリを同じ IP アドレスにマップします。PAT を使用する場合、同じ IP アドレスおよびポートにマップします。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager よりもセキュリティ レベルが*高い*インターフェイス上に存在する場合には、アクセス リストまたはスタティック エントリを設定しなくても、Cisco IP Phone で接続を開始できます。

制約および制限

現在の SCCP 用の PAT および NAT サポートには、次の制限が適用されます。

- PAT は、**alias** コマンドを使用したコンフィギュレーションとは併用できません。
- 外部 NAT または PAT は、サポート**されません**。

（注） 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き、サポートされるようになりました。

内部 Cisco CallManager のアドレスに、異なる IP アドレスまたはポートへの NAT または PAT が設定されていると、外部 Cisco IP Phone の登録は失敗します。FWSM は現在、TFTP 経由で転送されたファイル コンテンツの NAT または PAT をサポートしていないからです。FWSM は、TFTP メッセージの NAT をサポートし、TFTP ファイルが FWSM を通過できるようにピンホールをオープンしますが、FWSM では、IP Phone の登録中に TFTP を使用して転送されている Cisco IP Phone コンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスおよびポートを変換できません。

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、メディア エンドポイント（IP Phone など）の位置の判別が必要になることがあります。

この情報は、手動設定を行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス制御と NAT ステートを準備するために使用されます。

位置を判別する場合、**inspect skinny** コマンドは、トンネル デフォルト ゲートウェイ 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 ルートは、**route** *interface* **0 0** *metric* **tunneled** 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 ルートを書き換

えます。したがって、VPN トラフィックに **inspect skinny** コマンドが必要な場合には、トンネル デフォルト ゲートウェイ 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てください。

例

次に、SCCP インスペクション エンジンをイネーブルにし、SCCP トラフィックをデフォルト ポート（2000）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
debug skinny	SCCP デバッグ情報をイネーブルにします。
show skinny	FWSM を使用して確立した SCCP セッションに関する情報を表示します。
show conn	各接続タイプの接続状態を表示します。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

inspect smtp

非拡張 SMTP 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 smtp** 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します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect smtp

no inspect smtp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol smtp** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

SMTP アプリケーション検査は、FWSM を通過できる SMTP コマンドのタイプを制限し、モニタ機能を追加することによって、SMTP ベースの攻撃に対する基本的な保護を提供します。SMTP のアプリケーション検査プロセスには、拡張 SMTP セッションは含まれません。

inspect smtp コマンドにより SMTP アプリケーション検査をイネーブルにすると、高速パス処理で検査が実行されます。つまり、FWSM 上の 3 つのネットワーク プロセッサの 1 つで実行されます。

inspect smtp コマンドには、以前、**fixup smtp** コマンドにより提供されていた機能が含まれています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）がサポートされます。その他の SMTP コマンドおよび拡張 SMTP コマンドは、サポートされません。サポートされないコマンドは X に変換され、内部サーバにより拒否されます。この場合、「500 Command unknown: 'XXX'」などのメッセージが生成されます。不完全なコマンドは、廃棄されます。

（注） ポリシー マップに、**inspect smtp** コマンドと **inspect esmtp** コマンドの両方が含まれている場合、ポリシー マップに最初にリストされているコマンドが、トラフィックの照合に使用されます。

inspect smtp コマンドは、サーバ SMTP バナーの「2」および「0」以外の文字をアスタリスクに変更します。CR（復帰）および LF（改行）の文字は、無視されます。

SMTP 検査をイネーブルにすると、ルールに適合していない場合、対話型 SMTP に使用される Telnet セッションが停止することがあります。ルールとは、SMTP コマンドの長さが最低 4 文字である、CR および LF で終了している、次の応答を発信する前に相手側からの応答を待機する必要がある、などです。

SMTP サーバは、クライアントの要求に対して、数値の応答コードおよび任意の判読可能文字列を使用して応答します。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およびサーバが戻すメッセージを制御し、削減します。SMTP 検査が実行するのは、次の 3 つの主要タスクです。

- SMTP 要求を、7 つの基本 SMTP コマンドに制約します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査追跡を生成します ― メール アドレスに含まれている無効文字が置換された場合、監査レコード 108002 が生成されます。詳細は、RFC 821 を参照してください。

SMTP 検査は、コマンド応答シーケンスをモニタし、次の異常がないかどうかを確認します。

- コマンドの短縮
- コマンドの不正な終了（<CR> <LR> で終了していない）
- MAIL および RCPT コマンドは、メールの送信者および受信者を指定します。メール アドレスはスキャンされ、不正文字が含まれていないかどうかが確認されます。縦棒 | は削除されます（ブランクに変更されます）。| が許可されるのは、メール アドレスを定義するために使用され、| の前に [<] が付いている場合だけです。
- SMTP サーバによる予期せぬ変更
- 不明なコマンドの場合、FWSM 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、クライアントにエラー コードを生成します。パケットの内容が変更されるので、TCP チェックサムを再計算するか、調整する必要があります。
- TCP ストリームの編集
- コマンドのパイプライン化

例

次に、SMTP インスペクション エンジンをイネーブルにし、SMTP トラフィックをデフォルト ポート（25）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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 smtp
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上で 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トラフィック クラスを定義します。
debug smtp	SMTP のデバッグ情報をイネーブルにします。
inspect esmtp	拡張 SMTP アプリケーション検査をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
show conn	SMTP を含む各種の接続タイプの接続ステートを表示します。

inspect snmp

SNMP（簡易ネットワーク管理プロトコル）アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

inspect snmp コマンドは、**snmp-map** コマンドを使用して作成する SNMP マップの設定に基づいて、SNMP 検査をイネーブルにします。SNMP トラフィックを特定バージョンの 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。

SNMP の旧バージョンはセキュリティ レベルが低いので、セキュリティ ポリシーにより、SNMP トラフィックを Version 2 に制約することが必要になる場合があります。特定バージョンの SNMP を拒否するには、**snmp-map** コマンドを使用して作成する SNMP マップ内で、**deny version** コマンドを使用します。SNMP マップの設定後、**inspect snmp** コマンドを使用してマップをイネーブルにし、**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

次に、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、ポリシーを外部インターフェイスに適用する例を示します。

```
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上で厳密な 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 を使用してトラフィックを禁止します。
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	特定のセキュリティ アクションにクラス マップを対応付けます。
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します。設定を削除するには、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、引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。

デフォルトのポート割り当ては、1521 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol sqlnet** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

SQL*Net プロトコルは、FWSM が処理する各種パケット タイプで構成され、データ ストリームが、FWSM の両側の Oracle アプリケーションと互換性があるように見せるプロトコルです。

SQL*Net のデフォルトのポート割り当ては、1521 です。これは、Oracle for SQL*Net が使用する値ですが、Structured Query Language（SQL）の IANA ポート割り当てとは一致していません。一連のポート番号の範囲に対して SQL*Net 検査を適用するには、**class-map** コマンドを使用します。

FWSM は、すべてのアドレスに NAT（ネットワーク アドレス変換）を実行し、パケット内のすべての埋め込みポートを調べて、SQL*Net Version 1 用にオープンします。

SQL*Net Version 2 では、データ長がゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットが修正されます。

修正が必要なパケットには、次の形式で、ホスト / ポート アドレスが埋め込まれています。

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

SQL*Net Version 2 の TNSFrame タイプ（Connect、Accept、Refuse、Resend、および Marker）の場合、NAT 対象のアドレスはスキャンされず、パケット内のどの埋め込みポートに対してもダイナミック接続はオープンされません。

SQL*Net Version 2 の TNSFrame、Redirect、および Data パケットは、ペイロードのデータ長がゼロである REDIRECT TNSFrame タイプが先行送信された場合に限り、オープンするポートと NAT 対象アドレスがスキャンされます。データ長がゼロの Redirect メッセージが FWSM を通過すると、NAT 対象となり、ポートをダイナミックにオープンする Data または Redirect メッセージが続くことを想定して、接続データ構造にフラグが設定されます。 Redirect メッセージのあとに、続くパラグラフ内に TNS フレーム の 1 つが到達すると、フラグはリセットされます。

SQL*Net インスペクション 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ルタを使用して、チェックサムを再計算し、IP および TCP の長さを変更し、シーケンス番号および確認応答番号を再調整します。

その他の場合はすべて、SQL*Net Version 1 であるとみなされます。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）およびすべてのパケットについて、ポートとアドレスがスキャンされます。アドレスに NAT が実行され、ポート接続がオープンします。

例

次に、SQL*Net インスペクション エンジンをイネーブルにし、SQL*Net トラフィックをデフォルト ポート（1521）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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	特定のセキュリティ アクションにクラス マップを対応付けます。
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 を含む各種の接続タイプの接続ステートを表示します。

inspect sunrpc

Sun RPC アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	現在は廃止されている **fixup protocol rpc** コマンドに代わり、このコマンドが追加されました。

使用上のガイドライン

Sun RPC アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、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るポリシー 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。設定を削除するには、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 プロトコル用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設定します。Sun RPC は、NFS および NIS により使用されます。Sun RPC サービスは、システムの任意のポート上で実行できます。クライアントがサーバ上の Sun RPC サービスにアクセスしようとする場合、サービスを実行しているポートを検出する必要があります。ポートを検出するには、既知ポート 111 のポートマッパー プロセスにクエリーを送信します。

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、ポート番号を取得します。この時点から、クライアントのプログラムは、新しいポートに対して Sun RPC クエリーを送信できます。サーバが応答を送信すると、FWSM はそのパケットを代行受信し、対象ポート上で TCP および UDP の両方の初期接続をオープンします。

（注） Sun RPC ペイロード情報の NAT（ネットワーク アドレス変換）または PAT（ポート アドレス変換）は、サポートされません。

例

次に、RPC インスペクション エンジンをイネーブルにし、RPC トラフィックをデフォルト ポート（111）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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るコンフィギュレーションを削除します。
clear sunrpc-server active	NFS または NIS などの特定サービス用の Sun RPC アプリケーション検査によってオープンされたピンホールをクリアします。
show running-config sunrpc-server	Sun RPC サービスのテーブル 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 または NIS などの Sun RPC サービス用に、指定したタイムアウトでのピンホールの作成を許可します。
show sunrpc-server active	Sun RPC サービス用にオープンさ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、またはディセーブルにした設定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 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します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect tftp

no inspect tftp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。

デフォルトのポート割り当ては、69 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）は、RFC 1350 に定義されているように、TFTP サーバとクライアント間でファイルを読み書きするための簡易プロトコルです。

FWSM は、TFTP トラフィックを検査し、TFTP クライアントとサーバ間のファイル転送を許可するために、必要に応じて、ダイナミックに接続を作成し、変換を実行します。具体的には、このインスペクション エンジンは、TFTP 読み込み要求（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）または書き込み（WRQ）要求を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルおよび PAT 変換を割り当てます。以降、TFTP のファイル転送またはエラー通知に、このセカンダリ チャネルが使用されます。

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 サーバだけで、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 1 つだけです。サーバからエラー通知が送信されると、セカンダリ チャネルはクローズされます。

スタティック PAT を使用して TFTP トラフィックをリダイレクトする場合には、TFTP 検査をイネーブルにする必要があります。

例

次に、TFTP インスペクション エンジンをイネーブルにし、TFTP トラフィックをデフォルト ポート（69）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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トラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
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、または FWSM が待ち受けるポートを変更するには、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します。設定を削除するには、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、引数またはキーワードはありません。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコル用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設定します。

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

ネゴシエーションを成功させ、XWindows セッションを開始するには、FWSM で、X ホスト 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、FWSM 上で **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、バック接続を許可すべきかどうかが確認されます。

XWindows セッション中に、マネージャは既知ポート 6000 | n 上で ディスプレイ Xserver と通信します。次のターミナル設定の結果のように、各ディスプレイは Xserver に個別に接続します。

```
setenv DISPLAY Xserver:n
```

n は、ディスプレイ番号です。

XDMCP を使用すると、ディスプレイは IP アドレスを使用してネゴシエートされます。FWSM は、必要に応じて、このアドレスに NAT（ネットワーク アドレス変換）を実行できます。XDMCP 検査は、PAT をサポートしていません。

例

次に、XDMCP インスペクション エンジンをイネーブルにし、XDMCP トラフィックをデフォルト ポート（177）上で照合するクラス マップを作成する例を示します。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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上で 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	特定のセキュリティ アクションにクラス マップを対応付けます。
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。