



# inspect ctiqbe コマンド～ inspect xdmcp コマンド

## inspect ctiqbe

CTIQBE プロトコル インспекション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できます。インспекション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

デフォルトでは、このコマンドはディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、以前の <b>fixup</b> 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 ctique** コマンドは、NAT、PAT、および双方向 NAT をサポートしている CTIQBE プロトコルインスペクションを有効にします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を越えてコールセットアップを行えるようになります。

Telephony Application Programming Interface (TAPI) および Java Telephony Application Programming Interface (JTAPI) は、多数の Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding (CTIQBE) は、Cisco TAPI Service Provider (TSP) によって 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 インスペクションの使用時に適用される制限を次にまとめます。

- 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 ctique** コマンドを使用すると、メッセージ送信が遅延することがあり、これによってリアルタイム環境のパフォーマンスに影響が出る可能性があります。このデバッグまたはログをイネーブルにし、ASA を介して Cisco IP SoftPhone でコールセットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。
- CTIQBE アプリケーション インスペクションでは、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していません。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2つの Cisco IP SoftPhone が、ASA のそれぞれ異なるインターフェイスに接続された別々の Cisco CallManager に登録されている場合、これら 2つの電話機間のコールが失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。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ことが必要なためです。
- PAT または外部 PAT を使用しているときに Cisco CallManager の IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録するためには、TCP ポート 2748 を PAT (インターフェイス) アドレスの同一ポートに対してスタティックにマッピングする必要があります。CTIQBE 受信ポート (TCP 2748) は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

### シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect ctique** コマンドでメディア エンドポイント (IP 電話など) の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、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 コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、**inspect ctique** コマンドではトンネル 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 ctique** 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 ルートを設定しないようにしてください。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

次に、CTIQBE インспек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。その後、サービス ポリシーは外部インターフェイスに適用されます。

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

すべてのインターフェイスに対して CTIQBE インспекション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
<b>class-map</b>	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。
<b>show conn</b>	さまざまな接続タイプの接続状態を表示します。
<b>show ctiqbe</b>	ASA を介して確立されている CTIQBE セッション、および CTIQBE インспекション エンジンで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。
<b>timeout</b>	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プ宛ての DCERPC トラフィックのインスペクション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。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 dcerpc [map_name]
```

```
no inspect dcerpc [map_name]
```

## 構文の説明

*map\_name* (オプション)DCERPC インスペクション マップの名前。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

**inspect dcerpc** コマンドは、DCERPC プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

## 例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

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

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

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

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

関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>class-map type inspect</b>	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インスペクションクラス マップを作成します。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。
<b>timeout pinhole</b>	DCERPC ピンホールのタイムアウトを設定して、グローバル システムのピンホール タイムアウトを上書きします。

# inspect diameter

Diameter アプリケーション インспекション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 diameter** 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できます。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 diameter** [*diameter\_map*] [**tls-proxy proxy\_name**]

**no inspect diameter** [*diameter\_map*] [**tls-proxy proxy\_name**]



(注) Diameter インспекションには Carrier ライセンスが必要です。

## 構文の説明

<i>diameter_map</i>	Diameter ポリシー マップ名を指定します。
<b>tls-proxy proxy_name</b>	暗号化された接続を検査できるように、指定された TLS プロキシを使用します。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。
9.6(1)	<b>tls-proxy</b> キーワードが追加されました。

## 使用上のガイドライン

Diameter は、LTE (Long Term Evolution) および IMS (IP Multimedia Subsystem) 用の EPS (Evolved Packet System) などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウントिंग (AAA) プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameter アプリケーションは、課金のユーザ アクセス、サービス認証、QoS、およびレートの設定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロールプレーン インターフェイスで使用されますが、ASA は、次のインターフェイスについてのみ、Diameter コマンド コードおよび属性値ペア (AVP) を検査します。

- S6a: モビリティ マネージメント エンティティ (MME) - ホーム サブスクリプション サービス (HSS)
- S9: PDN ゲートウェイ (PDG) - 3GPP AAA プロキシ/サーバ
- Rx: ポリシー/課金ルール機能 (PCRF) - コールセッション制御機能 (CSCF)

Diameter インスペクションでは、Diameter エンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。TCP/TLS (インスペクションをイネーブルにするときに TLS を指定する場合) および SCTP には使用できませんが、SCTP/DTLS には使用できません。SCTP Diameter セッションにセキュリティを提供するには IPsec を使用します。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、オプションで、Diameter インスペクションポリシー マップを使用し、アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録された Diameter アプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックをきめ細かく設定できます。



(注)

他のインターフェイス上で動作するアプリケーションに対する Diameter メッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によってこれらのアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できますが、これらのサポートされていないアプリケーションに対してコマンドコードまたは AVP に基づいてアクションを指定することはできません。

例

次に、Diameter インスペクションをデフォルト ポート (TCP/3868、TCP/5868、および SCTP/3868) にグローバルに適用する例を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect diameter
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy global_policy global
```

関連コマンド

コマンド	説明
<b>class</b>	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。
<b>inspect sctp</b>	SCTP インスペクションをイネーブルにします。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。
<b>show service-policy inspect diameter</b>	inspect diameter ポリシーのステータスおよび統計情報を表示します。
<b>tls-proxy</b>	TLS プロキシを定義します。

# inspect dns

DNS インспекションをイネーブルにしたり(ディセーブルになっている場合)、DNS インспекションパラメータを設定したりするには、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できます。DNS インспекション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] [dynamic-filter-snoop]
```

```
no inspect dns [map_name] [dynamic-filter-snoop]
```

## 構文の説明

**dynamic-filter-snoop** (オプション)ダイナミック フィルタ スヌーピングをイネーブルにします。これはボットネット トラフィック フィルタでのみ使用されず。ボットネット トラフィック フィルタリングを使用する場合に限り、このキーワードを指定します。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック(内部 DNS サーバへの送信トラフィックを含む)に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。

*map\_name* (任意)DNS マップの名前を指定します。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。ボットネット トラフィック フィルタのスヌーピングは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。
7.2(1)	このコマンドは、DNS インспекションの追加パラメータを設定できるように変更されました。
8.2(1)	<b>dynamic-filter-snoop</b> キーワードが追加されました。

## 使用上のガイドライン

DNS インспекションは、次のような `preset_dns_map` インспекションクラス マップを使用して、デフォルトでイネーブルになっています。

- 最大 DNS メッセージ長は、512 バイトです。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

### DNS リライトに必要な DNS インспекション

DNS インспекションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部の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 サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インспекション エンジンがディセーブルである場合、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 インターフェイスにある場合、DNS 応答のパブリック 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」アドレス) をプライベート アドレス (「実際の」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 アドレスに変換します。

DNS インспекションがイネーブルであれば、NAT の DNS リライトを設定できます。

## 例

次に、DNS メッセージの最大長を設定する例を示します。

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

次に、すべての UDP DNS トラフィック用のクラス マップを作成し、デフォルトの DNS インспекション ポリシー マップで DNS インспекション および ポット ネット トラフィック フィルタのスヌーピングをイネーブルにして、外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>dynamic-filter enable</b>	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのポットネット トラフィック フィルタをイネーブルにします。
<b>policy-map</b>	特定のセキュリティアクションにクラス マップを関連付けます。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上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/ESMTP アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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可能です。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** [*map\_name*]

**no inspect esmtp** [*map\_name*]

## 構文の説明

*map\_name* (任意) ESMTP マップの名前。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドラ イン

ESMTP インспекションは、\_default\_esmtp\_map インспекション ポリシー マップを使用して、デフォルトで有効になります。

- サーバ バナーはマスクされます。
- 暗号化されたトラフィックが検査されます。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。
- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。

- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ESMTP アプリケーション インспекションを使用すると、ASA を通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インспекション処理は、SMTP アプリケーション インспекションに似ており、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ほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インспекションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。は、7つの RFC 821 コマンド(DATA、ASAHELO、MAIL、NOOP、QUIT、RCPT、RSET)をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

その他の拡張 SMTP コマンド(ATRN、ONEX、VERB、CHUNKING など)、およびプライベート拡張はサポートされません。サポートされないコマンドは、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、破棄されます。

ESMTP インспекション エンジンでは、文字「2」、「0」を除くサーバの SMTP バナーの文字をアスタリスクに変更します。復帰(CR)、および改行(LF)は無視されます。

SMTP インспекションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インспекションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インспекションは、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 SMTP コマンドと 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。
- 監査証拠の生成: メールアドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インспекションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端(<CR><LR> で終了していない)
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メールアドレスがスキャンされます。縦棒(|)は削除され(ブランクに変更されます)、「<」および「>」はメールアドレスを定義する場合にのみ許可されます(「>」より前に「<」がある必要があります)。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、ASA 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、サーバが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 チェックサムを再計算または調整が必要になります。

- TCP ストリーム編集
- コマンド パイプライン

例

次に、SMTP インспек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。その後、サービス ポリシーは 外部インターフェイス に適用されます。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>policy-map type inspect</b>	インспекション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。
<b>show conn</b>	SMTP を含む各種接続タイプの接続状態を表示します。

# inspect ftp

ポートを FTP インспекション用に設定したり、拡張インспекションをイネーブルにしたりするには、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できます。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*]]

## 構文の説明

<i>map_name</i>	FTP インспекション マップの名前。
<b>strict</b>	(任意)FTP トラフィックの拡張インспекションをイネーブルにして、RFC 標準への準拠を強制します。

## デフォルト

FTP インспекションはデフォルトでイネーブルになり、ASA は FTP ポート 21 をリッスンします。

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 に設定した場合、ポート 2021 に対して開始されるすべての接続で、データ ペイロードが FTP コマンドとして解釈されます。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。 <i>map_name</i> 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 インспекションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡

- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション インспекションによって、FTP データ転送用にセカンダリ チャネルが用意されます。これらのチャネルのポートは、**PORT** コマンドまたは **PASV** コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイルアップロード、ファイルダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。



(注)

インспекションは FTP コントロール接続のポートだけに適用し、データ接続のポートには適用しないでください。ASA のステートフル インспекション エンジンには、必要に応じてダイナミックにデータ接続を準備します。

**no inspect ftp** コマンドを使用して、FTP インспекション 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。

### 厳密な FTP

厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密な FTP をイネーブルにするには、**inspect ftp** コマンドに **strict** オプションを含めます。

厳密な FTP を使用するときは、オプションで FTP インспекション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

インターフェイスに対して **strict** オプションをオンにすると、FTP インспекションによって次の動作が適用されます。

- FTP コマンドが確認応答されてからでない、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと **PORT** コマンドが、エラー文字列に表示されないように確認されます。



注意

**strict** オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。

**strict** オプションがイネーブルの場合、各 FTP コマンドと応答シーケンスが追跡され、次の異常なアクティビティがないか確認されます。

- 切り捨てられたコマンド: **PORT** コマンドおよび **PASV** 応答コマンドのカンマの数が 5 であるかどうか確認されます。カンマの数が 5 でない場合は、**PORT** コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド: FTP コマンドが、RFC の要求どおりに **<CR><LF>** 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。
- **RETR** コマンドと **STOR** コマンドのサイズ: これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- 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ます。**PORT** コマンドがサーバから送信される場合、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ます。**PASV** 応答コマンドがクライアントから送信される場合、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」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集: ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。

- 無効ポート 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調べられます。1 ~ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン: PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は SYST コマンドに対する FTP サーバの応答を連続した X で置き換えて、サーバのシステム タイプが FTP クライアントに知られないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

### FTP ログ メッセージ

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 取得またはアップロードされたファイルごとに監査レコード 302002 が生成されます。
- メモリ不足によって動的なセカンダリ チャネルの準備に失敗した場合は、監査レコード 201005 が生成されます。

### 例

ユーザ名とパスワードを送信する前に、すべての FTP ユーザに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

### 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>mask-syst-reply</b>	FTP サーバ応答をクライアントに対して非表示にします。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>request-command deny</b>	不許可にする FTP コマンドを指定します。
<b>service-policy</b>	1 つ以上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 インспекション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 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できます。GTP インспекション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 gtp** [*map\_name*]

**no inspect gtp** [*map\_name*]



(注) GTP インспекションには GTP/GPRS または Carrier ライセンスが必要です。

## 構文の説明

*map\_name* (オプション)GTP インспекション ポリシー マップの名前。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	GTPv2 および IPv6 アドレスのサポートが追加されました。

## 使用上のガイドラ イン

GPRS トンネリング プロトコルは、General Packet Radio Service (GPRS) トラフィック用に GSM、UMTS および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザ データ パケットの伝送にもトンネリング メカニズムを使用します。サービス プロバイダー ネットワークは、GTP を使用して、エンドポイント間の GPRS バックボーンを介してマルチプロトコル パケットをトンネリングします。

GTP インспекションはデフォルトではイネーブルになっていません。ただし、ユーザ自身のインспекション マップを指定せずにイネーブルにすると、次の処理を行うデフォルト マップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は 500 です。
- GSN/エンドポイント タイムアウトは 30 分です。
- PDP コンテキストのタイムアウトは 30 分です。GTPv2 では、これはベアラ-コンテキスト タイムアウトです。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答タイムアウトは 20 秒です。
- 未知のメッセージ ID はドロップされ、ログに記録されます。この動作は、3GPP が S5S8 インターフェースについて定義するメッセージに制限されます。他の GPRS インターフェースについて定義されたメッセージは、最小限の検査によって許可される場合があります。

**policy-map type inspect gtp** コマンドを使用して GTP のパラメータを定義します。GTP マップを定義した後、**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**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

GTP の既知のポートは UDP 3386、2123、および 2152 です。

#### シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect gtp** コマンドでメディア エンドポイント (IP 電話など) の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、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 コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、**inspect gtp** コマンドではトンネル 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 ルートを設定しないようにしてください。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、ネットワークのトンネル数を制限する方法を示しています。

```
ciscoasa(config)# policy-map type inspect gtp gmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

## 関連コマンド

コマンド	説明
<b>class</b>	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。
<b>clear service-policy inspect gtp</b>	グローバルな GTP 統計情報をクリアします。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。
<b>show service-policy inspect gtp</b>	<b>inspect gtp</b> ポリシーのステータスおよび統計情報を表示します。

## inspect h323

H.323 アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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 | ras} [map_name]
```

```
no inspect h323 {h225 | ras} [map_name]
```

### 構文の説明

<b>h225</b>	H.225 シグナリング インспекションをイネーブルにします。
<i>map_name</i>	(任意)H.323 マップの名前。
<b>ras</b>	RAS インспекション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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

**inspect h323** コマンドは、Cisco CallManager や VocalTec Gatekeeper などの H.323 に準拠したアプリケーションに対するサポートを提供します。H.323 は国際電気通信連合 (ITU) で定義されている、LAN を介したマルチメディア会議用のプロトコルスイートです。ASA では、H.323 v3 機能の Multiple Calls on One Call Signaling Channel を含め、バージョン 6 までの H.323 をサポートしています。

H.323 インспекションをイネーブルにした場合、ASA は、H.323 Version 3 で追加された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インспекションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

#### シグナリング メッセージのインспекション

シグナリング メッセージのインспекションでは、多くの場合、**inspect h323** コマンドでメディア エンドポイント (IP 電話など) の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、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 コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、**inspect h323** コマンドではトンネル 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 ルートを設定しないようにしてください。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

次に、H.323 インспек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。その後、サービス ポリシーは外部インターフェイスに適用されます。

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

#### 関連コマンド

コマンド	説明
<b>policy-map type inspect</b>	インспекション ポリシー マップを作成します。
<b>show h225</b>	ASA で確立されている H.225 セッションの情報を表示します。
<b>show h245</b>	スロー スタートを使用しているエンドポイントによって ASA 間で確立された H.245 セッションの情報を表示します。
<b>show h323 ras</b>	ASA 間で確立された H.323 RAS セッションの情報を表示します。
<b>timeout {h225   h323}</b>	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 インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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*]

## 構文の説明

*map\_name* (オプション)HTTP インспекション 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。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドラ イン



### ヒント

アプリケーションおよび URL のフィルタリングを実行するサービス モジュールをインストールできます。これには、ASA CX や ASA FirePOWER などの HTTP インспекションが含まれます。ASA 上で実行される HTTP インспекションは、これらのモジュールと互換性がありません。HTTP インспекション ポリシー マップを使用して ASA 上で手作業による設定を試みるより、専用のモジュールを使用してアプリケーション フィルタリングを設定する方がはるかに簡単であることに注意してください。

HTTP インспекション エンジンを使用して、HTTP トラフィックに関する特定の攻撃やその他の脅威から保護します。

HTTP アプリケーション インспекションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

拡張 HTTP インспекション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インспекション ポリシー マップを設定するときには使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。

HTTP アプリケーション インспекションでトンネルアプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバヘッダー タイプのスプーフィングもサポートされています。

拡張 HTTP インспекションは、すべての HTTP メッセージについて次の点を確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

例

この例では、任意のインターフェイスを通過して ASA に入るすべての HTTP 接続(ポート 80 の TCP トラフィック)が HTTP インспекション対象として分類されます。このポリシーはグローバル ポリシーなので、インспекションが発生するのは各インターフェイスにトラフィックが入ったときだけです。

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>policy-map type inspect</b>	インспекション ポリシー マップを作成します。

## 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できます。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、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

ICMP インスペクション エンジンを使用すると、TCP や UDP トラフィックのように ICMP トラフィックを検査できます。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP による ASA の通過を禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンにより、それぞれの要求に対して 1 つの応答しか返されなくなり、正確なシーケンス番号が設定されるようになります。

ICMP インスペクションがディセーブルの場合(デフォルト設定)、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、ICMP エコー要求への応答であっても拒否されます。

### 例

次の例に示すように、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ます。この例では、ICMP プロトコル ID (IPv4 の場合は 1、IPv6 の場合は 58) を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して ICMP インスペクション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。

```

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>icmp</b>	ASA インターフェイスが終端となる ICMP トラフィックのアクセスルールを設定します。
<b>policy-map</b>	セキュリティアクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
<b>service-policy</b>	1 つ以上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 メッセージに対してアプリケーション インспекション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できます。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、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

ICMP エラー インспекションをイネーブルにすると、ASA は NAT の設定に基づいて、ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASA は、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASA は、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストと ASA の間にある中間ノードによって生成された ICMP エラーメッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが **traceroute** コマンドを使用して ASA の内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASA が中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インспекション エンジンには、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP (宛先アドレス) に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。

- 元のパケットのマッピング IP を実際の IP に変更する。
- 元のパケットのマッピング ポートを実際のポートに変更する。
- 元のパケットの IP チェックサムを再計算する。

例

次に、ICMP エラー アプリケーション インспек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。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して ICMP エラー インспекション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。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>icmp</b>	ASA インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。
<b>inspect icmp</b>	ICMP インспек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。
<b>policy-map</b>	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
<b>service-policy</b>	1 つ以上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 インспекション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。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、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

**inspect ils** コマンドは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品に対する NAT のサポートを提供します。

ASA は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、PAT はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に **xlate** が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0 (NAT なし) を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインспекション エンジンをおフにすることを勧めます。

ILS サーバが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート (通常は TCP 389) の LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャンネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ (ADD、DEL、SEARCH、MODIFY など) が交換される場合があります。ADD REQUEST PDU 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 アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インспекションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- 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、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の 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の増分を調整する。

ILS インспекションには、次の制限事項があります。

- 照会要求や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複数の ID を持っている単一のユーザは NAT には認識されません。



(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 チャンネル上のみのため、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、この間隔は 60 分に設定されています。

## 例

次の例に示すように、ILS インспекション 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 トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して ILS インспекション 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。

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

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティアクションにクラス マップを関連付けます。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上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

インスタント メッセージング トラフィックのインスペクション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。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 im** *map\_name*

**no inspect im** *map\_name*

## 構文の説明

*map\_name* IM マップの名前。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

**inspect im** コマンドは、IM プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。インスタント メッセージ (IM) インスペクション エンジンを使用すると、IM のネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

## 例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
ciscoasa(config)# regex loginname1 "user1@example.com"
ciscoasa(config)# regex loginname2 "user2@example.com"
ciscoasa(config)# regex loginname3 "user3@example.com"
ciscoasa(config)# regex loginname4 "user4@example.com"
ciscoasa(config)# regex yahoo_version_regex "1\.0"
ciscoasa(config)# regex gif_files "\.gif"
ciscoasa(config)# regex exe_files "\.exe"
```

```

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

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

ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

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

ciscoasa(config)# class-map im inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic

ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all

```

## 関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。
<b>match protocol</b>	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

# inspect ip-options

パケット内の IP オプションのインスペクションをイネーブルにするには、クラスまたはポリシー マップ タイプ インスペクション コンフィギュレーション モードで **inspect ip-options** 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できます。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 ip-options** [*map\_name*]

**no inspect ip-options** *map\_name*

## 構文の説明

*map\_name* (任意) IP オプション マップの名前。

## デフォルト

このコマンドは、グローバル ポリシーでデフォルトでイネーブルになっています。デフォルトのインスペクション マップでは、ルータ アラート オプションを持つパケットは許可されますが、その他のオプションを持つパケットはドロップされます。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペ アレント	シングル	マルチ	
				コンテキ スト	システム
ポリシーまたはクラス マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

## コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。サポートされているオプションは、 <b>ecool</b> オプション、 <b>nop</b> オプション、および <b>router-alert</b> オプションです。IP ヘッダーに <b>EOOL</b> 、 <b>NOP</b> 、または <b>RTRALT</b> 以外のオプションがさらに含まれている場合、これらのオプションを許可するように <b>ASA</b> が設定されているかどうかに関係なく、 <b>ASA</b> はそのパケットをドロップします。
9.5(1)	すべての IP オプションのサポートが追加されました。

## 使用上のガイドライン

パケットの IP ヘッダーには **Options** フィールドが含まれています。**Options** フィールドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、一般的な通信では必要ありません。具体的には、IP オプションにはタイムスタンプ、セキュリティ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、フィールドにはゼロまたは 1 つ以上の数のオプションを含めることができます。

IP オプション インспекションを設定して、パケット ヘッダーの [IP Options] フィールドのコンテンツに基づいてどの IP パケットを許可するかについて制御できます。望ましくないオプションがあるパケットをドロップしたり、オプションをクリア (してパケットを許可) したり、変更なしでパケットを許可したりできます。

デフォルト以外の処理を行うには、IP オプション インспекション ポリシー マップを作成し、**parameter** コマンドを入力して、さまざまなオプションに対して実行するアクションを指定します。次のオプションを検査できます。いずれの場合も、**allow** アクションはそのオプションを含むパケットを変更なしで許可し、**clear** アクションはパケットを許可しますがヘッダーからそのオプションを除去します。

マップからオプ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。パケットに他の許可されているオプションまたはクリアされたオプションが含まれている場合でも、マップで指定されていないオプションを含むパケットはすべてドロップされます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ (<http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml>) を参照してください。

- **default action {allow | clear}**: マップに明示的に含まれていないオプションに対するデフォルトのアクションを設定します。許可またはクリアのデフォルトアクションを設定しないと、許可されていないオプションを持つパケットはドロップされます。
- **basic-security action {allow | clear}**: セキュリティ (SEC) オプションを許可またはクリアします。
- **commercial-security action {allow | clear}**: 商用セキュリティ (CIPSO) オプションを許可またはクリアします。
- **ool action {allow | clear}**: End of Options List オプションを許可またはクリアします。ゼロ バイトが 1 つだけ含まれたこのオプションは、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
- **exp-flow-control action {allow | clear}**: 実験的フロー制御 (FINN) オプションを許可またはクリアします。
- **exp-measurement action {allow | clear}**: 実験的測定 (ZSU) オプションを許可またはクリアします。
- **extended-security action {allow | clear}**: 拡張セキュリティ (E-SEC) オプションを許可またはクリアします。
- **imi-traffic-descriptor action {allow | clear}**: IMI トラフィック記述子 (IMITD) オプションを許可またはクリアします。
- **nop action {allow | clear}**: No Operation オプションを許可またはクリアします。IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合、NOP オプションは、オプションを 32 ビット境界上に揃えるために、「内部パディング」として使用されます。
- **quick-start action {allow | clear}**: クリックスタート (QS) オプションを許可またはクリアします。
- **record-route action {allow | clear}**: レコードルート (RR) オプションを許可またはクリアします。

- **router-alert action {allow | clear}**: ルータ アラート (RTRALT) オプションを許可またはクリアします。このオプションは、デフォルトの IP オプション インспекション ポリシー マップで許可されます。このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインспекションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。
- **timestamp action {allow | clear}**: タイムスタンプ (TS) オプションを許可またはクリアします。
- **{0-255} action {allow | clear}**: オプション タイプ番号によって識別されるオプションを許可またはクリアします。番号は全オプション タイプのオクテット (コピー、クラス、およびオプション番号) で、オクテットのオプションの番号部分だけではありません。これらのオプション タイプは、実際のオプションに表示されない可能性があります。非標準オプションは、インターネット プロトコル RFC 791 (<http://tools.ietf.org/html/rfc791>) で定義されている、想定される「タイプ/長さ/値」形式である必要があります。

例

次に、パケット ヘッダーに EOOL、NOP、および RTRALT オプションを含むパケットを ASA が通過させるように IP オプション インспекション ポリシー マップを定義する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

次に、任意の IP オプションを持つパケットを許可する新しいデフォルト アクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action allow
```

関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>policy-map type inspect</b>	インспекション ポリシー マップを作成します。

## inspect ipsec-pass-thru

IPsec パススルー インспекション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。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 ipsec-pass-thru [map_name]
```

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

### 構文の説明

*map\_name* (オプション)IPsec パススルー マップの名前。

### デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 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 インспекションをイネーブルまたはディセーブルにします。IPsec パススルー アプリケーション インспекションによって、IKE UDP ポート 500 接続に関連付けられた ESP (IP プロトコル 50) トラフィックか AH (IP プロトコル 51) トラフィックまたはその両方の便利なトラバーサルが提供されます。このインспекションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

インспекションの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、IPsec パススルー 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。このコンフィギュレーションで、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーション モードでは、クライアントあたりの最大接続数と、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て、ポリシーを 1 つまたは複数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** コマンドで使用されたときにイネーブルになります。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。



(注)

ASA 7.0(1) では、**inspect ipsec-pass-thru** コマンドは ESP トラフィックの通過のみ許可していましたが、最新バージョンで同じ動作を保持するために、**inspect ipsec-pass-thru** コマンドが引数なしで指定されている場合は、ESP を許可するデフォルト マップが作成され、付加されます。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

次に、アクセス リストを使用して IKE トラフィックを識別し、IPsec パススルー パラメータ マップを定義して、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。

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

関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>class-map type inspect</b>	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インスペクション クラス マップを作成します。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。
<b>match protocol</b>	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

## inspect ipv6

IPv6 インспекション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 ipv6** 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。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 ipv6** [*map\_name*]

**no inspect ipv6** [*map\_name*]

### 構文の説明

*map\_name* (任意)IPv6 インспекション ポリシー マップの名前。

### デフォルト

IPv6 インспекションは、デフォルトでディセーブルになっています。

IPv6 インспекションをイネーブルにし、インспекション ポリシー マップを指定しないと、デフォルトの IPv6 インспекション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランス アレント	シングル	マルチ	
				コン テキ スト	シ ス テ ム
クラス コンフィギュ レーション	• 対応	• 対応	• 対応	• 対応	—

### コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

### 使用上のガイド ライン

IPv6 インспекションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、IPv6 インспекションでは、IPv6 パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかを確認できます。

例

次に、ヘッダーが hop-by-hop、destination-option、routing-address、および routing type 0 である IPv6 トラフィックをすべて削除する例を示します。

```

policy-map type inspect ipv6 ipv6-pm
  parameters
    match header hop-by-hop
      drop
    match header destination-option
      drop
    match header routing-address count gt 0
      drop
    match header routing-type eq 0
      drop
policy-map global_policy
  class class-default
    inspect ipv6 ipv6-pm
!
service-policy global_policy global
    
```

関連コマンド

コマンド	説明
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>match header</b>	IPv6 インスペクション ポリシー マップで IPv6 ヘッダーを照合します。
<b>policy-map type inspect ipv6</b>	IPv6 のインスペクション ポリシー マップを作成します。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>verify-header</b>	IPv6 インスペクション パラメータを設定します。

## inspect lisp

LISP インспекション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 lisp** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを入力します。LISP インспекション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 lisp [inspect_map_name]
```

```
no inspect lisp [inspect_map_name]
```

### 構文の説明

<i>inspect_map_name</i>	EID を制限する場合または LISP メッセージの事前共有キーを指定する必要がある場合は、LISP インспекション マップ名を指定します ( <b>policy-map type inspect lisp</b> )。
-------------------------	--

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

### 使用上のガイドライン

ASA は、ファースト ホップ ルータと ITR または ETR の間で送信される EID 通知メッセージの LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。

#### クラスタ フロー モビリティの LISP インспекションについて

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

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

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

例

次に、192.168.50.89(内部)にある LISP ルータと 192.168.10.8(別の ASA インターフェイス上)にある ITR または ETR ルータの間の LISP トラフィック (UDP 4342)を検査する例を示します。

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

関連コマンド

コマンド	説明
<b>allowed-eids</b>	IP アドレスに基づいて検査される EID を限定します。
<b>clear cluster info</b> <b>flow-mobility counters</b>	フロー モビリティ カウンタをクリアします。
<b>clear lisp eid</b>	ASA EID テーブルから EID を削除します。
<b>cluster flow-mobility lisp</b>	サービス ポリシーのフロー モビリティを有効にします。
<b>flow-mobility lisp</b>	クラスタのフロー モビリティを有効にします。
<b>policy-map type inspect lisp</b>	LISP 検査をカスタマイズします。

コマンド	説明
<b>site-id</b>	クラスターシャーシのサイト ID を設定します。
<b>show asp table classify domain inspect-lisp</b>	LISP 検査用の ASP テーブルを表示します。
<b>show cluster info flow-mobility counters</b>	フロー モビリティ カウンタを表示します。
<b>show conn</b>	LISP フロー モビリティの対象となるトラフィックを表示します。
<b>show lisp eid</b>	ASA EID テーブルを表示します。
<b>show service-policy</b>	サービス ポリシーを表示します。
<b>validate-key</b>	LISP メッセージを検証するための事前共有キーを入力します。

# inspect m3ua

M3UA インспекション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 m3ua** 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できます。M3UA インспекション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 m3ua** [*map\_name*]

**no inspect m3ua** [*map\_name*]



(注) M3UA インспекションには Carrier ライセンスが必要です。

## 構文の説明

*map\_name* (オプション)M3UA インспекション ポリシー マップの名前。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

## 使用上のガイドラ イン

MTP3 User Adaptation (M3UA) は、SS7 Message Transfer Part 3 (MTP3) レイヤと連動する IP ベース アプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバ プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザ パート (ISUP など) を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 が想定されるポートですが、異なるポートを使用するようにシグナリング ゲートウェイを設定することもできます。

MTP3 レイヤは、ルーティングおよびノード アドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード (OPC) および宛先ポイント コード (DPC) を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UA インスペクションは、限定されたプロトコル準拠を提供します。

オプションで、M3UA インスペクション ポリシー マップを作成し、ポイント コードまたはサービス インジケータ (SI) に基づいてアクセス ポリシーを適用することができます。また、メッセージ クラスおよびタイプに基づいてレート制限を適用することもできます。

## 例

次に、M3UA インスペクション ポリシー マップおよびインスペクション ポリシーの例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasahostname(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect m3ua m3ua-map

ciscoasa(config)# service-policy global_policy global
```

## 関連コマンド

コマンド	説明
<b>class</b>	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。
<b>policy-map type inspect</b>	インスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。
<b>show service-policy inspect m3ua</b>	<b>inspect m3ua</b> ポリシーのステータスおよび統計情報を表示します。

# inspect mgcp

MGCP アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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*]

構文の説明	<i>map_name</i>	(任意)MGCP マップの名前。
-------	-----------------	------------------

デフォルト このコマンドは、デフォルトでディセーブルになっています。

コマンドモード 次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

MGCP を使用するには、通常、2 つ以上の **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。一般的に、コール エージェントはゲートウェイのデフォルト 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 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に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部(グローバル)アドレスのセットで、内部ネットワークの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。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ (RJ11) インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブルモデムや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 デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX (構内交換機) インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス (IP アドレスと UDP ポート番号) に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、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ているときに、コマンドを受信したコール エージェントが制御をバックアップコール エージェントに引き渡し、バックアップコール エージェントが応答を送信する場合に起こる可能性があります。



(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定します。これによって、ASA を通過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** および **gateway** コマンドを使用します。コマンドキューで一度に許可される 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 メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect mgcp** コマンドでメディア エンドポイント (IP 電話など) の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect mgcp** コマンドではトンネル 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 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 ルートを設定しないようにしてください。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。

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。

例

次に、MGCP トラフィックを指定し、MGCP インスペクション 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。この例では、デフォルトポート (2427 および 2727) 上の MGCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。このコンフィギュレーションでは、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、10.10.10.116 と 10.10.10.117 の両方のゲートウェイを制御できるようにします。すべてのインターフェイスに対して MGCP インスペクション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。

```

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

```

#### 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map type inspect mgcp</b>	MGCP のインスペクション ポリシー マップを作成します。
<b>show mgcp</b>	ASA を介して確立された MGCP セッションの情報を表示します。
<b>timeout</b>	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 mmp

MMP インспек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 mmp** コマンドを使用します。MMP インспек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 mmp tls-proxy** [*name*]

**no inspect mmp tls-proxy** [*name*]

### 構文の説明

<i>name</i>	TLS プロキシインスタンス名を指定します。
<b>tls-proxy</b>	MMP インспекションに対して TLS プロキシをイネーブルにします。MMP プロトコルではさらに TCP トランスポートも使用できますが、CUMA クライアントでは TLS トランスポートしかサポートしていません。そのため、MMP インспекションをイネーブルにするには <b>tls-proxy</b> キーワードが必要です。

### デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。

### 使用上のガイドライン

ASA には、CUMA Mobile Multiplexing Protocol (MMP) を検証するインспекション エンジンが含まれています。MMP は、CUMA クライアントとサーバ間でデータ エンティティを送信するためのデータ トランスポート プロトコルです。ASA が CUMA クライアントとサーバの間に配置されており、MMP パケットのインспекションが必要な場合は、**inspect mmp** コマンドを使用します。

MMP トラフィックは TLS 接続でしか転送できないため、MMP インспекションは TLS プロキシとともにイネーブルにする必要があります。



(注)

MMP インспекション エンジンを設定するときは、デフォルト以外のインспекション クラスでしか追加できないことに注意してください。

例

次に、**inspect mmp** コマンドを使用して MMP トラフィックを検査する例を示します。

```
ciscoasa(config)# class-map mmp
ciscoasa(config-cmap)# match port tcp eq 5443
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map mmp-policy
ciscoasa(config-pmap)# class mmp
ciscoasa(config-pmap-c)# inspect mmp tls-proxy myproxy
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy mmp-policy interface outside
```

関連コマンド

コマンド	説明
<b>tls-proxy</b>	TLS プロキシ インスタンスを設定します。

# inspect netbios

NetBIOS アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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** [*map\_name*]

**no inspect netbios** [*map\_name*]

## 構文の説明

*map\_name* (任意) NetBIOS マップの名前。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

**inspect netbios** コマンドは、NetBIOS プロトコルに対するアプリケーション インспекションをイネーブルまたはディセーブルにします。NETBIOS インспекションはデフォルトでイネーブルになっています。NetBIOS インспекション エンジン は、ASA の NAT コンフィギュレーションに基づいて、NetBIOS ネーム サービス (NBNS) パケット内の IP アドレスを変換します。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。

## 例

次に、NetBIOS インспекション ポリシー マップを定義する例を示します。

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

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>policy-map type inspect netbios</b>	NetBIOS のインスペクション ポリシー マップを作成します。
<b>service-policy</b>	1 つ以上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 インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 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トと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 インспекションは、イネーブルになると、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ために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で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 制御チャネル上で修正バージョンの GRE (RFC 2637) がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE (RFC 1701、RFC 1702) には実行されません。

具体的には、ASA は、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャンネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されません。接続と xlate は、後続のセカンダリ 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 インスペクション エンジン は、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャンネルで修正バージョンの GRE (RFC 2637) がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE (RFC 1701、RFC 1702) には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PAC (PPTP アクセス コンセントレータ) から開始されたヘッドエンド PNS (PPTP ネットワーク サーバ) への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザ PC です。

すべてのインターフェイスに対して PPTP インスペクション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。

例

次の例に示すように、PPTP インスペクション 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 トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上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-accounting

RADIUS アカウンティング インспекションをイネーブルまたはディセーブルにしたり、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したりするには、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。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 radius-accounting** *map\_name*

**no inspect radius-accounting** [*map\_name*]

### 構文の説明

*map\_name* 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、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

### 使用上のガイドラ イン

RADIUS アカウンティング インспекションの目的は、RADIUS サーバを使用した GPRS ネットワークの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インспекションを実行するには、GTP/GPRS または Carrier ライセンスは必要ありませんが、GTP インспекションを実行し、GPRS セットアップをセットアップしない限り、意味がありません。

**policy-map type inspect radius-accounting** コマンドを使用して、RADIUS アカウンティングのパラメータの定義に使用するインспекション マップを作成します。parameters コマンドを入力した後、**send response**、**host**、**validate-attribute**、**enable gprs**、および **timeout users** の各コマンドを使用してインспекションの特性や動作を定義できます。

さらに、**class-map type management**、**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、クラスに **inspect radius-accounting** コマンドを適用して、1 つ以上のインターフェイスにポリシーを適用します。



(注) **inspect radius-accounting** コマンドは、**class-map type management** コマンドとのみ使用できます。

例

次に、RADIUS アカウンティング インспекション マップを設定し、インспекションをグローバルにイネーブルにする例を示します。

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

関連コマンド

コマンド	説明
パラメータ	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。
<b>class-map type management</b>	アクションを適用する ASA 宛てのレイヤ 3 またはレイヤ 4 管理トラフィックを識別します。
<b>policy-map type inspect radius-accounting</b>	RADIUS アカウンティングのインспекション ポリシー マップを作成します。
<b>show service-policy</b> および <b>clear service-policy</b>	サービス ポリシー設定の表示とクリアを行います。
<b>service-policy</b>	1 つ以上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 インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

RSH プロトコルは、TCP ポート 514 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** 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インспекションは、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

次に、RSH インспек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。その後、サービス ポリシーは外部 インターフェイスに適用されます。すべてのインターフェイスに対して RSH インспекション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。

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy
```

```
ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティアクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上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 インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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。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** [*map\_name*]

**no inspect rtsp** [*map\_name*]

## 構文の説明

*map\_name* (任意)RTSP マップの名前。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

**inspect rtsp** コマンドを使用すると、ASA 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 の各接続で使用されます。



(注) Cisco IP/TV では、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、制御チャネルとしての TCP(例外的に UDP)とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP コントロール チャネルは、クライアントに設定されているトランスポート モードに応じて、オーディオ/ビデオ トラフィックの送信に使用されるデータ チャネルをネゴシエートするために使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA 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。SETUP 応答メッセージが、着信方向に移動している場合、サーバは ASA との相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、ASA は、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、クライアントとサーバのポートを SETUP 応答メッセージ内に含める必要があるとは規定していないため、ASA で状態を保持し、SETUP メッセージに含まれているクライアント ポートを記憶しておく必要があります。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、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 を使用するときには、転送モードを正しく設定することが重要です。ASA では、サーバからクライアントまたはその逆の **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] の順に選択して、トランスポート モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] および [Attempt to use TCP for all content] のチェックボックスを選択します。ASA 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 で UDP モードを使用する場合は、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] のチェックボックスを選択します。マルチキャスト経由でライブ コンテンツは利用できません。ASA で、**inspect rtsp port** コマンド ステートメントを追加します。

### 制約事項と制限

RTSP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA 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。
- 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 ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化できますが、ASA ではフラグメント化されたパケットに対して NAT を実行することはできません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、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。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

### 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。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic
ciscoasa(config-cmap)# match access-list rtsp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy
ciscoasa(config-pmap)# class rtsp-traffic
```

```
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティアクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。

# inspect scansafe

クラスのトラフィックに対するクラウド Web セキュリティ インспекション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 scansafe** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを入力します。インспекション アク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 scansafe** *scansafe\_policy\_name* [**fail-open** | **fail-close**]

**no inspect scansafe** *scansafe\_policy\_name* [**fail-open** | **fail-close**]

## 構文の説明

<i>scansafe_policy_name</i>	<b>policy-map type inspect scansafe</b> コマンドで定義するインспекション クラス マップの名前を指定します。
<b>fail-open</b>	(オプション)クラウド Web セキュリティ サーバを使用できない場合に ASA を通過するトラフィックを許可します。
<b>fail-close</b>	(オプション)クラウド Web セキュリティ サーバを使用できない場合にすべてのトラフィックをドロップします。 <b>fail-close</b> がデフォルトです。

## コマンドデフォルト

**fail-close** がデフォルトです。

## 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。

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

## コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

Cisco クラウド Web セキュリティ では、Software as a Service (SaaS) による Web セキュリティおよび Web フィルタリング サービスが提供されます。ネットワークで ASA を使用している企業は、追加ハードウェアをインストールせずにクラウド Web セキュリティ サービスを使用できます。



(注)

この機能は「ScanSafe」とも呼ばれていますので、ScanSafe という名前が表示されるコマンドがあります。

モジュラ ポリシー フレームワークを使用してこのコマンドを設定する手順は次のとおりです。

1. **policy-map type inspect scansafe** コマンドを使用してインスペクション ポリシー マップを作成します。HTTP と HTTPS の両方を検査する場合、各トラフィックについて少なくとも1つずつ設定する必要があります。
2. (オプション)**class-map type inspect scansafe** コマンドを使用してホワイトリストを設定します。
3. **class-map** コマンドを使用して、検査するトラフィックを定義します。HTTP と HTTPS のトラフィックについて、それぞれクラス マップを設定する必要があります。
4. **policy-map** コマンドを入力してポリシーを定義します。
5. HTTP の場合、**class** コマンドを入力して HTTP クラス マップを参照します。
6. **inspect scansafe** コマンドを入力して HTTP インスペクション ポリシー マップを参照します。
7. HTTPS の場合、**class** コマンドを入力して HTTPS クラス マップを参照します。
8. **inspect scansafe** コマンドを入力して HTTPS インスペクション ポリシー マップを参照します。
9. 最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。

## 例

次に、2つのクラス(HTTPに1つ、HTTPSに1つ)を設定する例を示します。各ACLはwww.cisco.comとtools.cisco.com、DMZネットワーク、およびHTTPとHTTPSの両方に対するトラフィックを免除します。他のすべてのトラフィックは、複数のホワイトリストに記載されたユーザおよびグループを除き、クラウド Web セキュリティに送信されます。ポリシーは、内部インターフェイスに適用されます。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0

ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
```

```

ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS

ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside
    
```

関連コマンド

コマンド	説明
<b>class-map type inspect scansafe</b>	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
<b>default user group</b>	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
<b>http[s]</b> (パラメータ)	インスペクション ポリシー マップのサービス タイプ (HTTP または HTTPS) を指定します。
<b>license</b>	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
<b>match user group</b>	ユーザまたはグループをホワイトリストと照合します。
<b>policy-map type inspect scansafe</b>	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
<b>retry-count</b>	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
<b>scansafe</b>	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
<b>scansafe general-options</b>	汎用クラウド Web セキュリティ サーバ オプションを設定します。
<b>server {primary   backup}</b>	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
<b>show conn scansafe</b>	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ 接続を表示します。
<b>show scansafe server</b>	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
<b>show scansafe statistics</b>	合計と現在の http 接続を表示します。
<b>user-identity monitor</b>	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
ホワイトリスト	トラフィックのクラスでホワイトリスト アクションを実行します。

# inspect sctp

Stream Control Transmission Protocol (SCTP) インспекションをイネーブルまたはディセーブルにするには、クラス コンフィギュレーション モードで **inspect sctp** 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できます。SCTP インспекション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 sctp** [*map\_name*]

**no inspect sctp** [*map\_name*]



(注)

SCTP インспекションには Carrier ライセンスが必要です。

## 構文の説明

*map\_name* (オプション) SCTP インспекション ポリシー マップの名前。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

## 使用上のガイドライン

SCTP (Stream Control Transmission Protocol) は、テレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャのいくつかのインターフェイス用のトランスポート プロトコルでもあります。デバイスを通過するモバイル ネットワーク トラフィックがある場合は、SCTP インспекションを GTP および Diameter インспекションとともに使用します。

オプションで、SCTP ポリシー マップを指定できます。これにより、SCTP アプリケーションでフィルタ処理を実行して、さまざまなサービスを提供できます。また、ペイロード プロトコル ID (PPID) に基づいて SCTP トラフィック クラスを選択的にドロップしたり、ログに記録したり、それらにレート制限を適用したりすることができます。 **policy-map type inspect sctp** コマンドを使用してポリシー マップを作成します。

例

次の例では、未割り当ての PPID (この例の作成時点で未割り当て) をドロップし、PPID 32 ~ 40 をレート制限し、Diameter PPID をログに記録するインスペクションポリシーマップを作成します。このサービスポリシーは、すべての SCTP トラフィックを照合する inspection\_default クラスにインスペクションを適用します。

```

policy-map type inspect sctp sctp-pmap
  match ppid 58 4294967295
    drop
  match ppid 26
    drop
  match ppid 49
    drop
  match ppid 32 40
    rate-limit 1000
  match ppid diameter
    log

policy-map global_policy
  class inspection_default
    inspect sctp sctp-pmap
  !
service-policy global_policy global
    
```

関連コマンド

コマンド	説明
<b>class</b>	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。
<b>clear service-policy inspect sctp</b>	グローバルな SCTP 統計情報をクリアします。
<b>policy-map type inspect</b>	インスペクションポリシーマップを作成します。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシーマップを適用します。
<b>show service-policy inspect sctp</b>	<b>inspect sctp</b> ポリシーのステータスおよび統計情報を表示します。

## inspect sip

SIP アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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 [sip_map] [tls-proxy proxy_name] [phone-proxy proxy_name] [uc-ime proxy_name]
```

```
no inspect sip [sip_map] [tls-proxy proxy_name] [phone-proxy proxy_name] [uc-ime proxy_name]
```

### 構文の説明

<b>phone-proxy</b> <i>proxy_name</i>	指定したインспекションセッションの Phone Proxy をイネーブルにします。
<i>sip_map</i>	SIP ポリシー マップ名を指定します。
<b>tls-proxy</b> <i>proxy_name</i>	指定されたインспекションセッションで TLS プロキシをイネーブルにします。キーワード <b>tls-proxy</b> をレイヤ 7 ポリシー マップ名として使用することはできません。
<b>uc-ime</b> <i>proxy_name</i>	SIP インспекションの Cisco Intercompany Media Engine プロキシをイネーブルにします。

### デフォルト

SIP インспекションはデフォルトでイネーブルになっており、次を含むデフォルトのインспекション ポリシー マップを使用します。

- SIP インスタント メッセージ (IM) の拡張機能: イネーブル
- SIP トラフィック以外の SIP ポート使用: 許可
- サーバとエンドポイントの IP アドレスの非表示: ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク: ディセーブル
- 1 以上の宛先ホップ カウントを保証: イネーブル
- RTP 準拠: 適用強制しない
- SIP 準拠: ステート チェックとヘッダー検証を実行しない

暗号化されたトラフィックのインспекションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP のデフォルトのポート割り当ては 5060 です。

**コマンドモード** 次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。
8.0(2)	<b>tls-proxy</b> キーワードが追加されました。
9.4(1)	<b>phone-proxy</b> キーワードと <b>uc-ime</b> キーワードが追加されました。

**使用上のガイドラ  
イン**

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インспекションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インспекションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインспекションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。

ASA 経由の SIP コールをサポートする場合は、シグナリングメッセージは予約済みの宛先ポート (UDP/TCP 5060) 経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレス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。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 インспекションは、それらの埋め込まれた IP アドレスに NAT を適用します。

**SIP インспекションの制限事項**

SIP インспекションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス (「trying」応答メッセージの SIP ヘッダー内の「from」) は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。

- SDP 部分の所有者/作成者フィールド(o=)の IP アドレスが接続フィールド(c=)の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。
- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

#### シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、**inspect sip** コマンドでメディアエンドポイント(IP 電話など)の場所を特定する必要があります。

この情報は、メディアトラフィックのアクセスコントロールと NAT 状態を準備して、手動で設定を行わずにメディアトラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect sip** コマンドで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ルートを設定しないようにしてください。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。その後、サービスポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して SIP インスペクション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。

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

#### 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map type inspect sip</b>	SIP のインスペクションポリシーマップを作成します。
<b>show sip</b>	ASA を通じて確立された SIP セッションに関する情報を表示します。
<b>show conn</b>	さまざまな接続タイプの接続状態を表示します。
<b>timeout</b>	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。
<b>tls-proxy</b>	TLS プロキシインスタンスを定義し、最大セッション数を設定します。

# inspect skinny

SCCP (Skinny) アプリケーション インспекションをイネーブルにするには、クラス設定モードで **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できます。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** [*skinny\_map*] [**tls-proxy** *proxy\_name*] [**phone-proxy** *proxy\_name*]

**no inspect skinny** [*skinny\_map*] [**tls-proxy** *proxy\_name*] [**phone-proxy** *proxy\_name*]

## 構文の説明

<b>phone-proxy</b> <i>proxy_name</i>	インспекションセッションの phone proxy をイネーブルにします。
<i>skinny_map</i>	skinny ポリシー マップ名を指定します。
<b>tls-proxy</b> <i>proxy_name</i>	インспекションセッションで TLS プロキシをイネーブルにします。

## デフォルト

SCCP インспекションは、次のデフォルト値を使用してデフォルトでイネーブルになっています。

- 登録: 適用強制しない
- メッセージの最大 ID: 0x181
- プレフィックスの長さの最小値: 4
- メディア タイムアウト: 00:05:00
- シグナリング タイムアウト: 01:00:00
- RTP 準拠: 適用強制しない

暗号化されたトラフィックのインспекションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。
8.0(2)	キーワード <b>tls-proxy</b> が追加されました。

リリース	変更内容
9.4(1)	<b>phone-proxy</b> キーワードは廃止されました。
9.13(1)	<b>tls-proxy</b> キーワードは廃止されました。このキーワードは今後のリリースで削除される予定です。

## 使用上のガイドライン

Skinny (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 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インспекション は、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インспекションによって処理されます。ASA は、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。



(注)

ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインспекションをサポートします。

### Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングはスタティックである必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスを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です。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようになります。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック 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 アドレスと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 と比べて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 が接続を開始できるようにするために、ACL やスタティック エントリは必要ありません。

### 制約事項と制限

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、ASA 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。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された 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た Cisco CallManager の IP アドレスとポートを変換することはできません。



(注) ASA では、コール セットアップ中であるコール以外の SCCP 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。

#### シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect skinny** コマンドでメディア エンドポイント (IP 電話など) の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect skinny** コマンドで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 ルートを設定しないようにしてください。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。その後、サービス ポリシーは外部 インターフェイスに適用されます。すべてのインターフェイスに対して SCCP インスペクション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。

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

#### 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map type inspect skinny</b>	SCCP のインスペクション ポリシー マップを作成します。
<b>show skinny</b>	ASA 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。
<b>show conn</b>	さまざまな接続タイプの接続状態を表示します。
<b>timeout</b>	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。
<b>tls-proxy</b>	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

## inspect snmp

SNMP アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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*

### 構文の説明

*map\_name* SNMP マップ名です。

### デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

**inspect snmp** コマンドを使用し、**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 はセキュリティが低いため、SNMP トラフィックをバージョン 2 に制限するようにセキュリティ ポリシーで要求する場合があります。SNMP の特定のバージョンを拒否するには、**snmp-map** コマンドを使用して作成する SNMP マップで、**deny version** コマンドを使用します。SNMP マップを設定した後、**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 つ以上のインターフェイスにこのマップを適用します。

すべてのインターフェイスに対してストリクト snmp アプリケーション インспекション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。

例

次に、SNMP トラフィックを識別し、SNMP マップを定義して、ポリシーを定義し、SNMP インスタレーションをイネーブルにして、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。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>deny version</b>	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
<b>snmp-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上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 インспекション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できます。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**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

このコマンドは、デフォルトで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

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

SQL\*Net プロトコルは、さまざまなパケット タイプで構成されています。ASA はこれらのパケットを処理して、ASA のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL\*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL\*Net 用に使用している値ですが、構造化照会言語 (SQL) の IANA ポート割り当てとは一致しません。SQL\*Net インспекションを一連のポート番号に適用するには、**class-map** コマンドを使用します。



(注)

SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL\*Net のインспекションをディセーブルにします。SQL\*Net インспекションがイネーブルになっていると、ASA はプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

ASA は、すべてのアドレスの NAT を実行し、パケット内のすべての埋め込みポートを検索して、SQL\*Net バージョン 1 用に開きます。

SQL\*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート 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 の各 TNSFrame タイプ (Connect, Accept, Refuse, Resend, Marker) は、NAT 対象のアドレスがあるかどうかをスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くことありません。

SQL\*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかをスキャンされます。データ長がゼロの Redirect メッセージが ASA を通過すると、後続の Data または Redirect メッセージの NAT が実行され、ポートがダイナミックに開かれることを想定するフラグが接続データ構造に設定されます。先行するパラグラフの 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 インスペクションエンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL\*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ (Connect, Accept, Refuse, Resend, Marker, Redirect, Data) とすべてのパケットは、ポートおよびアドレスがあるかどうかをスキャンされます。アドレスの NAT が実行され、ポート接続が開かれます。

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。その後、サービスポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して SQL\*Net インスペクション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。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティアクションにクラスマップを関連付けます。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシーマップを適用します。
<b>show conn</b>	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 stun

Session Traversal Utilities for NAT (STUN) アプリケーション インспекション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 stun** 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できます。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 stun**

**no inspect stun**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。  
デフォルトのポート割り当ては TCP/3478 および UDP/3478 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。

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

## コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

## 使用上のガイドライン

RFC 5389 で定義されている Session Traversal Utilities for NAT (STUN) は、プラグインが不要になるように、ブラウザベースのリアルタイム コミュニケーション用に WebRTC クライアントによって使用されます。WebRTC クライアントは、多くの場合、クラウド STUN サーバを使用してパブリック IP アドレスおよびポートを学習します。WebRTC は、Interactive Connectivity Establishment (ICE、RFC 5245) を使用してクライアント間の接続を確認します。これらのクライアントは、TCP やその他のプロトコルを使用することもできますが、通常、UDP を使用します。

ファイアウォールは、多くの場合、発信 UDP トラフィックをブロックするため、Cisco Spark などの WebRTC 製品が接続を完了できないことがあります。STUN インспекションでは、STUN エンドポイント用のピンホールが開かれ、STUN と ICES の基本コンプライアンスが適用されます。これにより、両側で接続チェックが確認応答された場合にクライアントの通信が許可されます。このため、これらのアプリケーションをイネーブルにするためにアクセスルールで新しいポートを開く必要がなくなります。

デフォルトのインスペクションクラスで STUN インスペクションをイネーブルにすると、STUN トラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。

STUN インスペクションには NAT に関するいくつかの制限があります。WebRTC トラフィックについては、スタティック NAT/PAT44 がサポートされます。Cisco Spark はピンホールを必要としないので、Spark は追加のタイプの NAT をサポートできます。Cisco Spark では NAT/PAT64 (ダイナミック NAT/PAT を含む) も使用できます。

ピンホールが複製される時、STUN インスペクションはフェールオーバー モードとクラスタモードでサポートされます。ただし、トランザクション ID はユニット間で複製されません。STUN 要求の受信後にユニットに障害が発生し、別のユニットが STUN 応答を受信した場合、STUN 応答はドロップされます。

**例**

次に、STUN インスペクションをデフォルト グローバル インスペクション ルールの一部としてイネーブルにする例を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect stun
ciscoasa(config)# service-policy global_policy global
```

**関連コマンド**

コマンド	説明
<b>class</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。
<b>show conn</b>	STUN を含む各種接続タイプの接続状態を表示します。
<b>show service-policy inspect diameter</b>	inspect diameter ポリシーのステータスおよび統計情報を表示します。

## inspect sunrpc

Sun RPC アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

このコマンドは、デフォルトでイネーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

Sun RPC アプリケーション インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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。このモードにアクセスするには、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 プロトコルに対するアプリケーション インспекションをイネーブルまたはディセーブルにします。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の任意のポートで実行できます。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には、サービスが実行されているポートを検出する必要があります。これを行うには、既知のポート 111 でポートマッパー プロセスを照会します。

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。この時点より、クライアント プログラムは Sun RPC クエリーをその新しいポートに送信します。サーバから応答が送信されると、ASA はこのパケットを代行受信し、そのポートで TCP と 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

次に、RPC インспек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。その後、サービス ポリシーは外部 インターフェイスに適用されます。すべてのインターフェイスに対して RPC インспекション 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。

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

関連コマンド

コマンド	説明
<b>clear configure sunrpc_server</b>	<b>sunrpc-server</b> コマンドを使用して実行されているコンフィギュレーションを削除します。
<b>clear sunrpc-server active</b>	Sun RPC アプリケーション インспекションによって、NFS または NIS などの特定のサービス用に開けられているピンホールをクリアします。
<b>show running-config sunrpc-server</b>	Sun RPC サービス テーブル コンフィギュレーションの情報を表示します。
<b>sunrpc-server</b>	NFS または NIS などの Sun RPC サービス用に、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。
<b>show sunrpc-server active</b>	Sun RPC サービス用に開けられているピンホールを表示します。

## inspect tftp

TFTP アプリケーション インспекションをディセーブルにしたり、ディセーブルになっている場合にイネーブルにしたりするには、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できます。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**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

このコマンドは、デフォルトで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

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

### 使用上のガイドライン

RFC 1350 に規定されている Trivial File Transfer Protocol (TFTP) は、TFTP サーバとクライアント間でファイルを読み書きするための簡易プロトコルです。

ASA は、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インспекション 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。

有効な読み取り要求 (RRQ) または書き込み要求 (WRQ) 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、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インспекションをイネーブルにする必要があります。

例

次に、TFTP インспек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。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して TFTP インспекション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。

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

関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。

# inspect vxlan

Virtual Extensible Local Area Network (VXLAN) アプリケーション インспекション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 vxlan** 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可能です。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 vxlan**

**no inspect vxlan**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

デフォルトのポート割り当ては UDP/4789 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。

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

## コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

## 使用上のガイドライン

Virtual Extensible Local Area Network (VXLAN) インспекションは、ASA を通過する VXLAN のカプセル化されたトラフィックで機能します。VXLAN ヘッダー フォーマットが標準に準拠し、不正な形式の packets をドロップすることを確認します。VXLAN インспекションは、ASA が VXLAN トンネル エンド ポイント (VTEP) または VXLAN ゲートウェイとして機能するトラフィックでは行われません。これは、それらのチェックが VXLAN パケットの通常の非カプセル化の一部として行われるためです。

VXLAN パケットは通常、ポート 4789 の UDP です。このポートは、default-inspection-traffic クラスの一部であるため、inspection\_default グローバル サービス ポリシー ルールに VXLAN インспекションを追加するだけです。または、それに対してポートまたは ACL マッチングを使用してクラスを作成することもできます。

## 例

次に、VXLAN インспекションをグローバル インспекションのデフォルト ルールの一部としてイネーブルにする例を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect vxlan
```

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上のインターフェイスにポリシー マップを適用します。

# inspect waas

WAAS アプリケーション インспекション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 waas** 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可能です。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 waas**

**no inspect waas**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 例

次に、デフォルトのインспекション クラスで WAAS アプリケーション インспекションをイネーブルにする例を示します。

```
policy-map global_policy
class inspection_default
inspect waas
```

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティ アクションにクラス マップを関連付けます。
<b>service-policy</b>	1 つ以上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 インспекションをイネーブルにしたり、ASA がリッスンするポートを変更したりするには、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できます。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**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでイネーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた <b>fixup</b> コマンドは廃止されました。

## 使用上のガイドライン

**inspect xdmcp** コマンドは、XDMCP プロトコルに対するアプリケーション インспекションをイネーブルまたはディセーブルにします。

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 セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、ASA 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、この戻り接続を許可すべきかどうかを確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver: n
```

$n$  はディスプレイ番号です。

XDMCP が使用されている場合、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。IP アドレスは、ASA が必要に応じて NAT を行うことができます。XDMCP インスペクションでは、PAT はサポートされません。

## 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。その後、サービスポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して XDMCP インスペクション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。

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

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>policy-map</b>	特定のセキュリティアクションにクラスマップを関連付けます。
<b>service-policy</b>	1つ以上のインターフェイスにポリシーマップを適用します。