ASDM 6.3以降でのIPオプションインスペクションの設定

内容

概要

このドキュメントでは、特定の IP オプションがイネーブルの IP パケットを送信するために Cisco 適応型セキュリティ アプライアンス（ASA）を設定する方法について設定例を紹介します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA ソフトウェア リリース バージョン 8.3 以降
- Cisco Adaptive Security Manager ソフトウェア リリース バージョン 6.3 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

各 IP パケットには、Options フィールドのある IP ヘッダーが含まれています。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、この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ます。

IP オプションはセキュリティ リスクであり、ASA から IP オプション フィールドを含む IP パケットが渡された場合、ネットワークの内部設定の詳細が外部に漏れてしまいます。そのため、攻撃者はネットワークのトポロジをマッピングできます。Cisco ASA は企業のセキュリティを強化するデバイスですので、IP オプション フィールドを含むパケットはデフォルトでドロップします。参考のため、syslog メッセージ サンプルを以下に示します。

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny IP from 10.110.1.34 to XX.YY.ZZ.ZZ, IP options:"Router Alert"
```

ただし、ビデオ トラフィックを Cisco ASA 経由で渡す必要がある特定の導入シナリオでは、特定の IP オプションを含む IP パケットを渡す必要があり、そうしないとビデオ会議コールができなくなる可能性があります。Cisco ASA ソフトウェア リリース 8.2.2 以降では、「IP オプションのインスペクション」という新機能が導入されました。この機能を使用すると、特定の IP オプションを含むパケットが Cisco ASA を通過できるように制御できます。

デフォルトでこの機能は有効であり、以下の IP オプション インスペクションは、グローバル ポリシーで有効にされています。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションをクリアした後にパケットの転送を許可することを ASA に指示します。

- **End of Options List（EOOL）または IP オプション 0 - 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最後に置かれます。**
- **No Operation（NOP）または IP オプション 1 - フィールド変数全体の長さを示します。**
- **Router Alert（RTRALT）または IP オプション 20 - 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。**

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

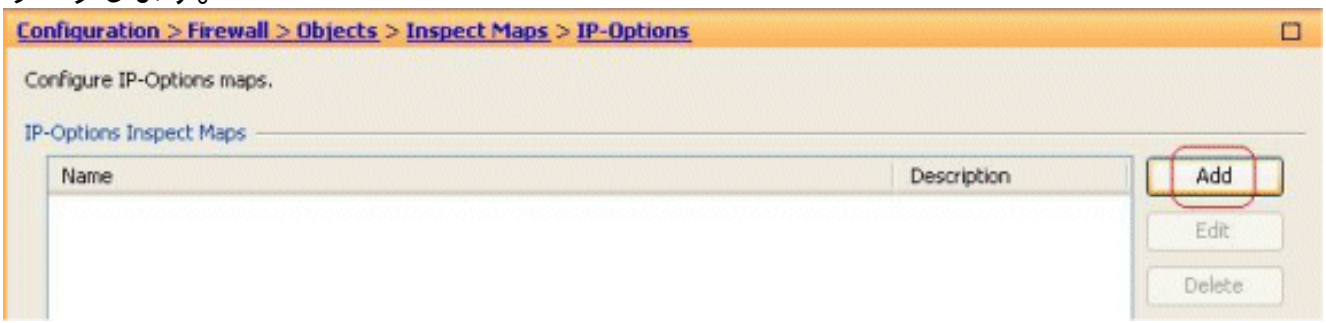
注：このセクションで使用されるコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ASDM の設定

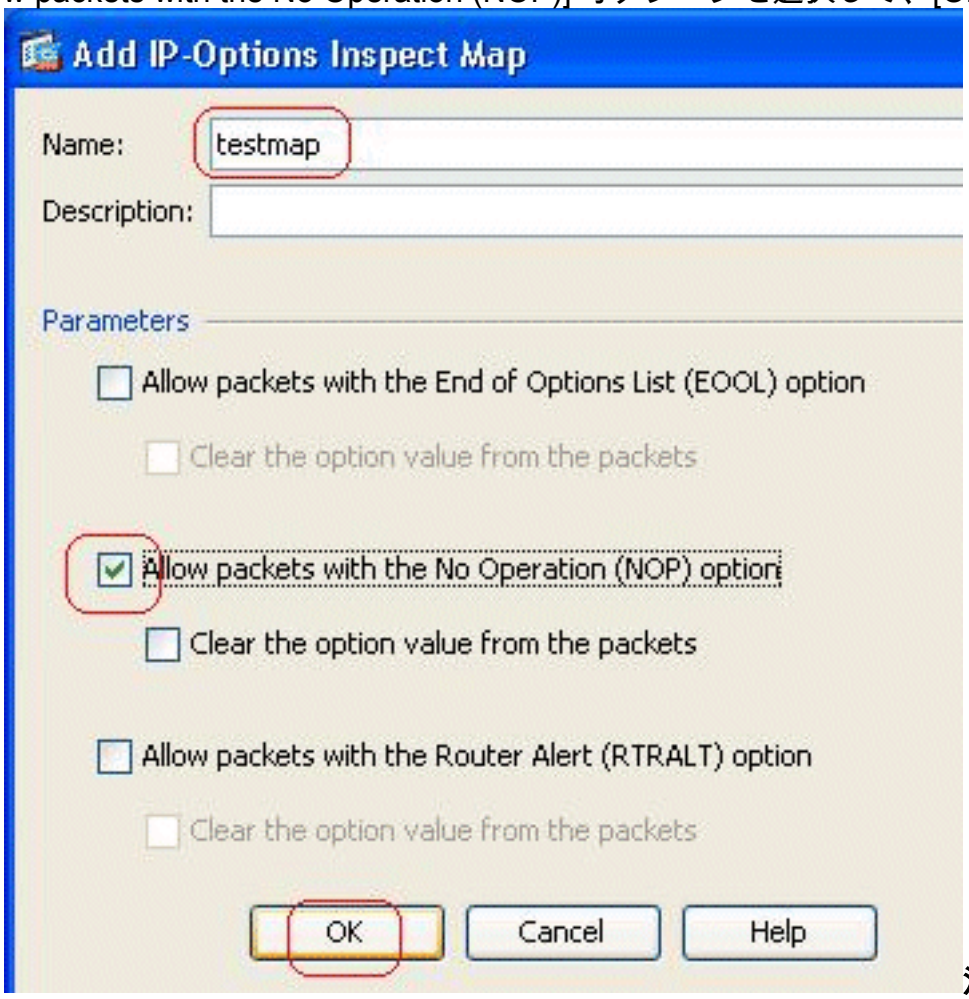
ASDM を使用すると、IP オプション フィールド（NOP）を含む IP パケットのインスペクションを有効にする方法がわかります。

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。

1. [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IP-Options] に移動し、[Add] をクリックします。

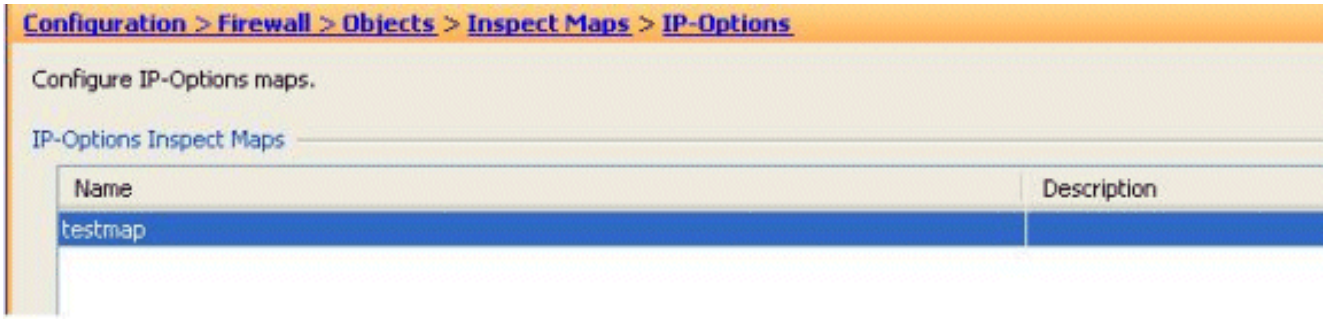


2. [Add IP-Options Inspect Map] ウィンドウが表示されます。インスペクション マップの名前を指定し、[Allow packets with the No Operation (NOP)] オプションを選択して、[OK] をクリックします。

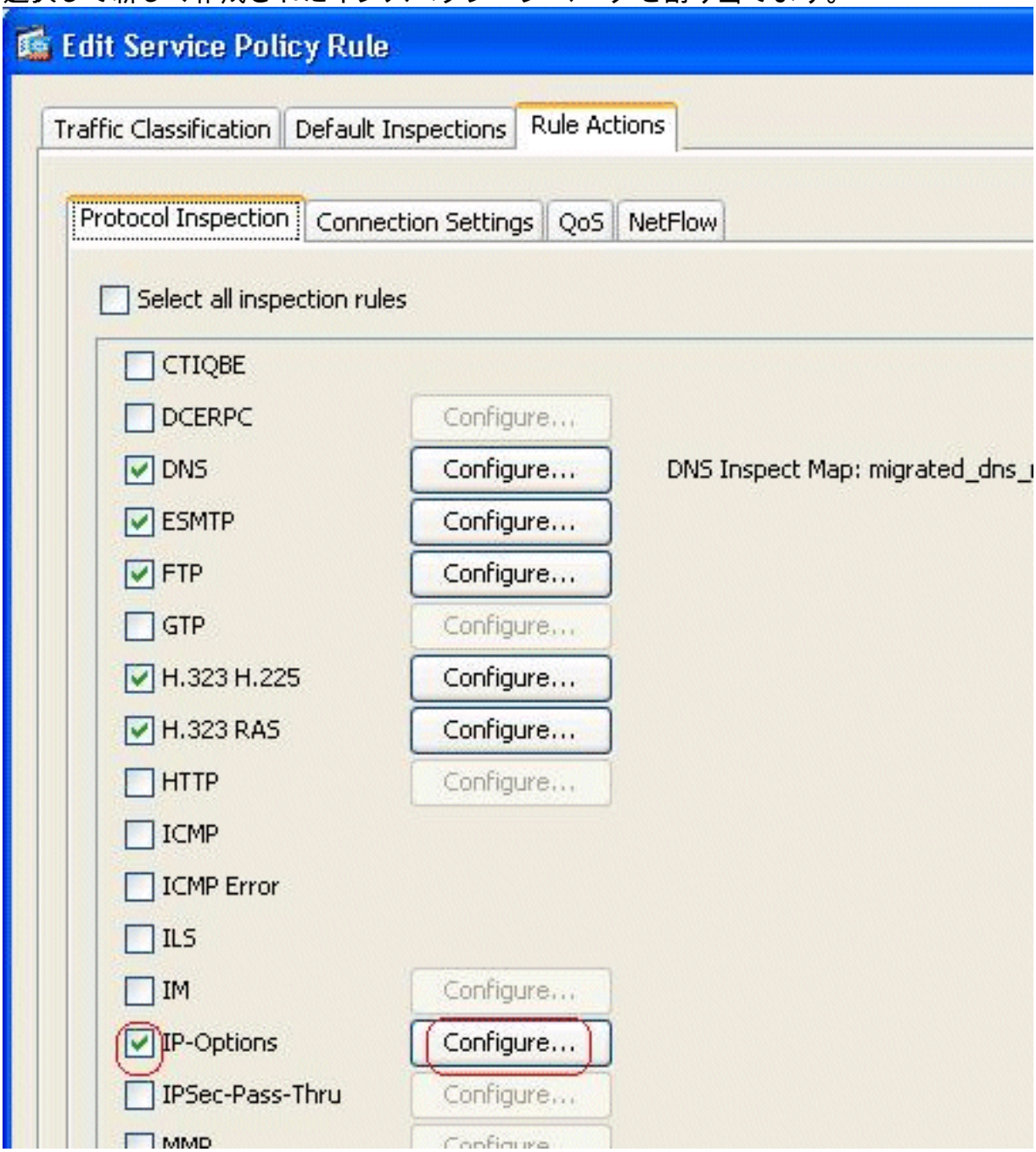


注：[Clear the option value from the packets]オプションを選択しても、IPパケットのこのフィールドが無効になり、パケットがCisco ASAを通過するようにすることができます。

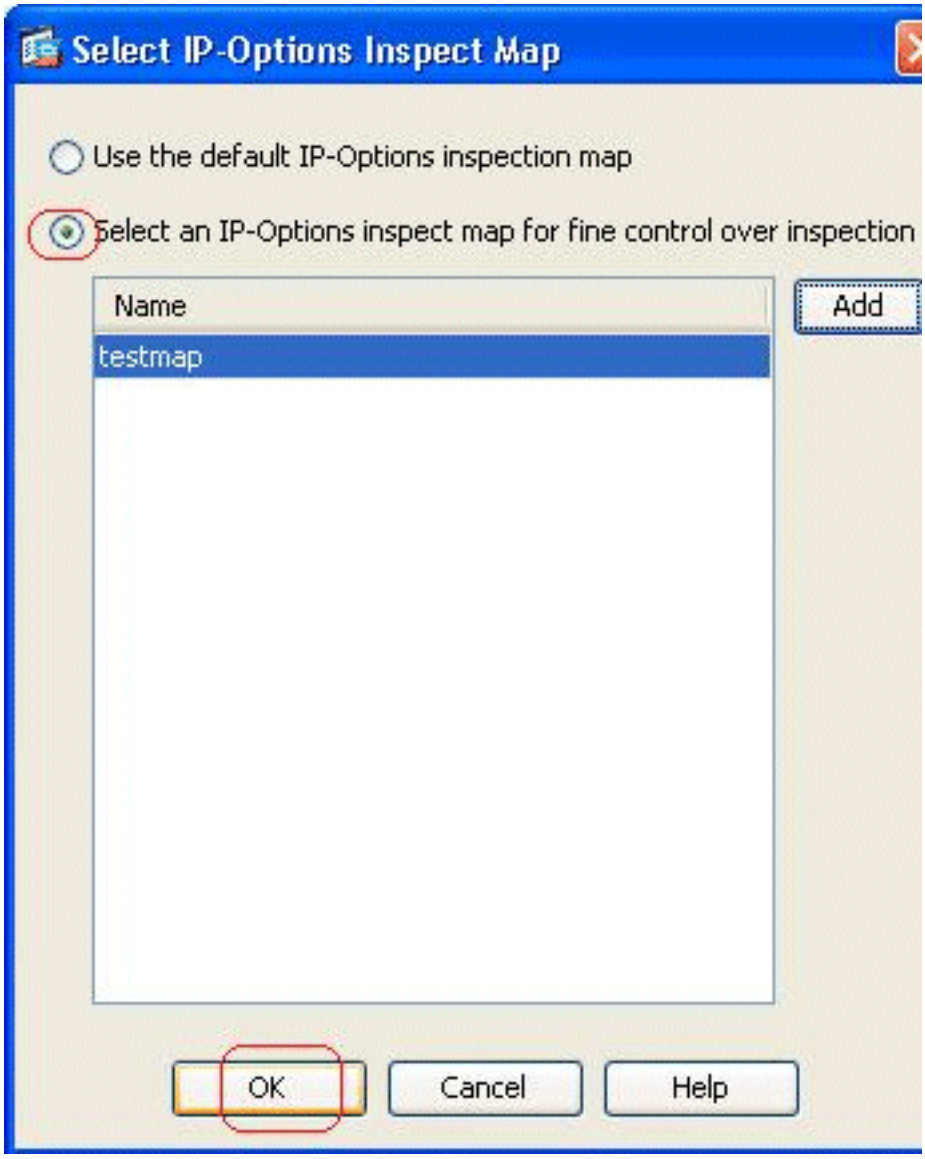
3. **testmap という名前の新しいインスペクション マップが作成されます。**[Apply] をクリックします。



4. [Configuration] > [Firewall] > [Service Policy Rules] に移動し、既存のグローバル ポリシーを選択して、[Edit] をクリックします。[Edit Service Policy Rule] ウィンドウが表示されます。[Rule Actions] タブを選択し、[IP-Options] アイテムにチェックマークを入れ、[Configure] を選択して新しく作成されたインスペクション マップを割り当てます。

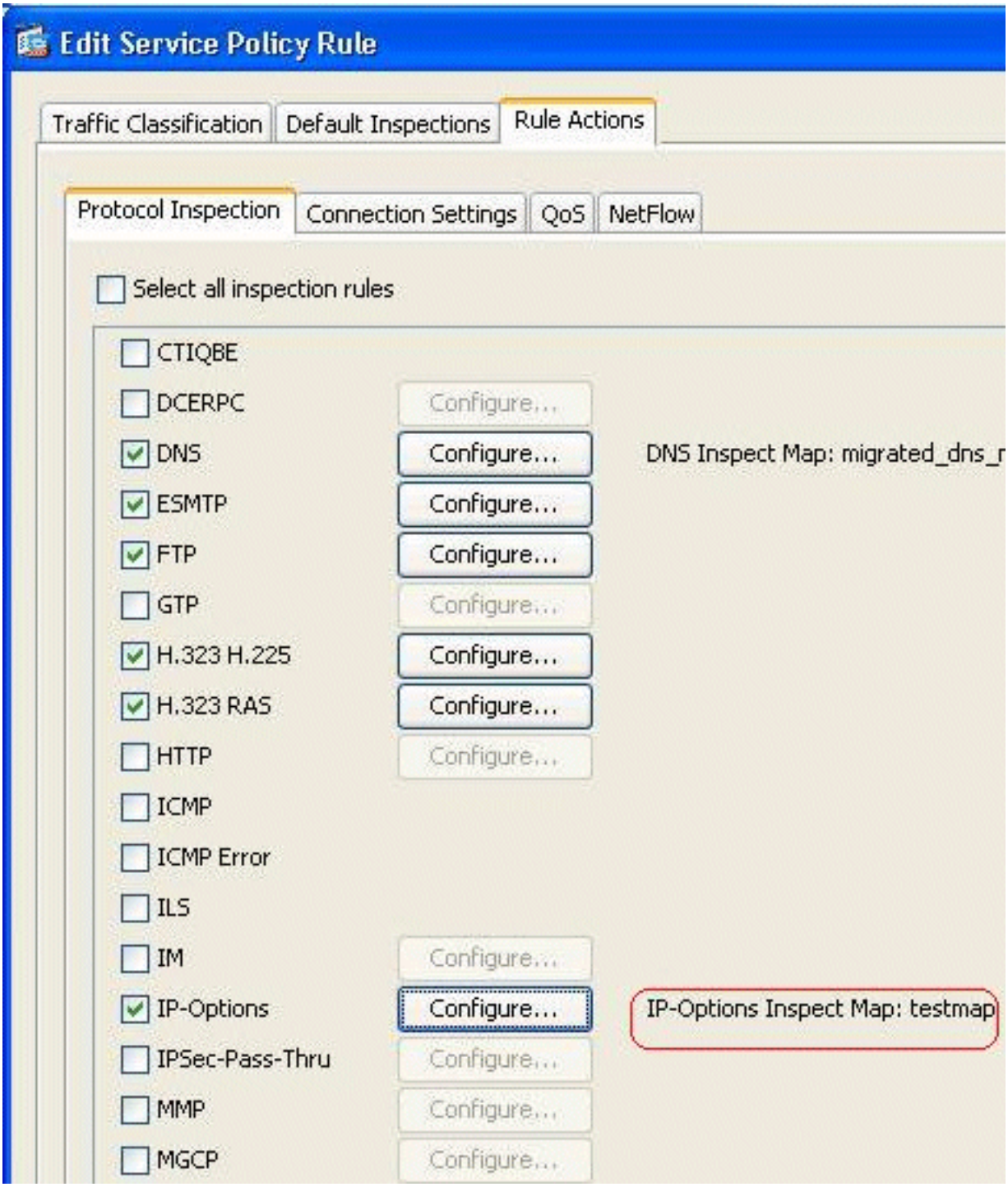


5. [Select an IP-Options inspect map for fine control over inspection] > [testmap] を選択し、

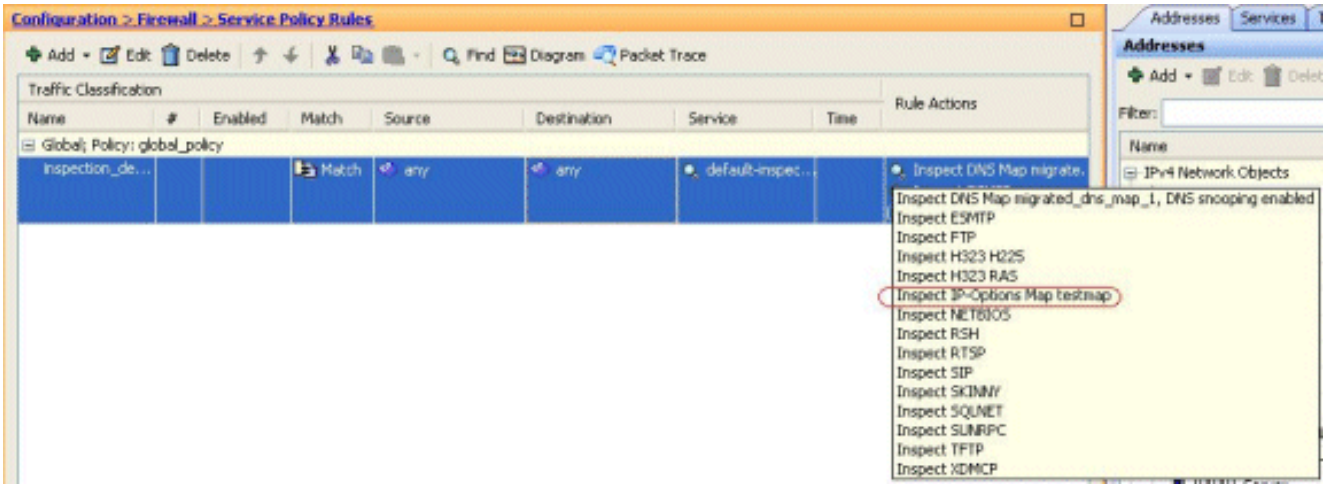


[OK] をクリックします。

6. 選択したインスペクション マップは、[IP-Options] フィールドに表示されます。[OK] をクリックして [Service Policy Rules] タブに戻ります。



7. [Rule Actions] タブにカーソルを合わせると、このグローバル マップに関連付けられているすべての使用可能なプロトコル インスペクション マップが見つかります。

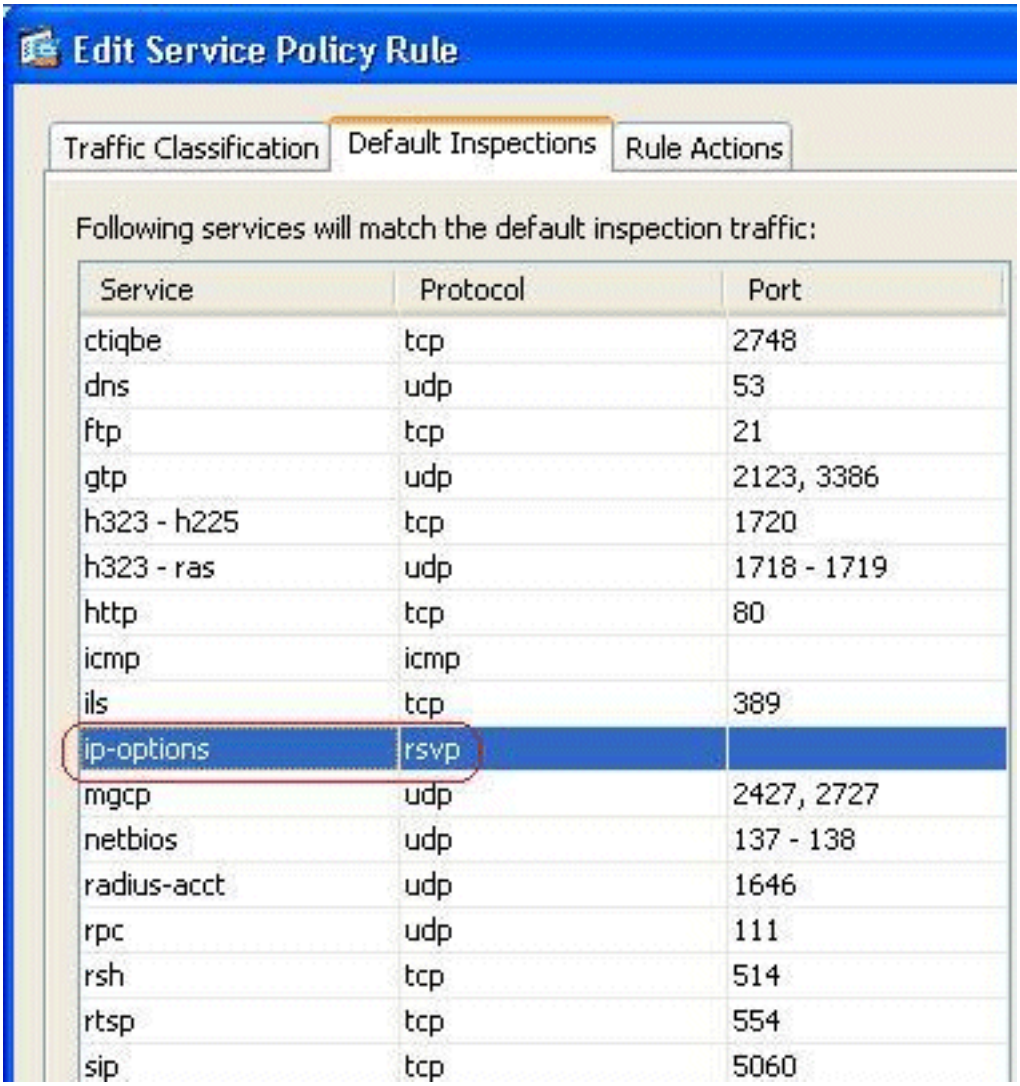


以下は、同等の CLI 設定の参考用のサンプル スニペットです。

Cisco ASA
ciscoasa(config)#policy-map type inspect ip-options testmap ciscoasa(config-pmap)#parameters ciscoasa(config-pmap-p)#nop action allow ciscoasa(config-pmap-p)#exit ciscoasa(config)#policy-map global_policy ciscoasa(config-pmap)#class inspection_default ciscoasa(config-pmap-c)#inspect ip-options testmap ciscoasa(config-pmap-p)#exit ciscoasa(config)#write memory

RSVP パケットを許可するための Cisco ASA のデフォルト動作

IP オプション インスペクションはデフォルトでイネーブルになっています。[Configuration] > [Firewall] > [Service Policy Rules] に移動します。[Global Policy] を選択し、[Edit] をクリックして [Default Inspections] タブを選択します。ここでは、[IP-Options] フィールド内の RSVP プロトコルが表示されます。これにより、RSVP プロトコルが確実に検査され、Cisco ASA を通じて許可されます。その結果、エンドツーエンドのビデオ通話が問題なく確立されます。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show service-policy inspect ip-options - 設定したサービス ポリシー ルールに従って、ドロップ/許可されたパケットの数を表示します。**

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのテクニカルサポート
- テクニカル サポートとドキュメント – Cisco Systems