Konfigurieren der IP-Optionsüberprüfung auf ASDM 6.3 und höher

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Konfigurieren
ASDM-Konfiguration
Standardverhalten der Cisco ASA, um RSVP-Pakete zuzulassen
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

Dieses Dokument enthält eine Beispielkonfiguration zur Konfiguration der Cisco Adaptive Security Appliance (ASA), um die IP-Pakete mit aktivierten IP-Optionen weiterzuleiten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA mit Softwareversion 8.3 oder höher
- Cisco Adaptive Security Manager mit Softwareversion 6.3 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Jedes IP-Paket enthält einen IP-Header mit dem Feld "Optionen". Das Feld Optionen, gemeinhin als IP-Optionen bezeichnet, stellt Kontrollfunktionen bereit, die in bestimmten Situationen erforderlich sind, aber für die meisten gängigen Kommunikationsvorgänge nicht erforderlich sind. IP-Optionen umfassen insbesondere Bestimmungen für Zeitstempel, Sicherheit und spezielle Weiterleitung. Die Verwendung von IP-Optionen ist optional, und das Feld kann 0, eine oder mehrere Optionen enthalten.

IP-Optionen stellen ein Sicherheitsrisiko dar. Wenn ein IP-Paket mit aktiviertem IP-Optionenfeld über die ASA weitergeleitet wird, werden Informationen über die interne Einrichtung eines Netzwerks an die Außenstellen weitergeleitet. So kann ein Angreifer die Topologie Ihres Netzwerks abbilden. Da Cisco ASA ein Gerät ist, das die Sicherheit im Unternehmen erzwingt, verwirft es standardmäßig die Pakete, bei denen das Feld "IP Options" (IP-Optionen) aktiviert ist. Hier wird eine Beispiel-Syslog-Meldung angezeigt, die als Referenz dient:

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||IP von 10.110.1.34 an XX.YY.ZZ.ZZ verweigern, IP-Optionen:
"Router-Warnung"
```

In bestimmten Bereitstellungsszenarien, in denen der Videodatenverkehr über die Cisco ASA geleitet werden muss, müssen IP-Pakete mit bestimmten IP-Optionen jedoch weitergeleitet werden, da andernfalls das Videokonferenzgespräch fehlschlagen kann. Ab der Cisco ASA-Softwareversion 8.2.2 wurde eine neue Funktion mit dem Namen "Inspection for IP options" eingeführt. Mit dieser Funktion können Sie steuern, welche Pakete mit bestimmten IP-Optionen über die Cisco ASA zugelassen werden.

Standardmäßig ist diese Funktion aktiviert, und die Überprüfung der unten stehenden IP-Optionen ist in der globalen Richtlinie aktiviert. Die Konfiguration dieser Überprüfung weist die ASA an, die Weiterleitung eines Pakets zuzulassen oder die angegebenen IP-Optionen zu löschen und das Paket anschließend weiterzugeben.

- **End of Options List (EOOL)** oder **IP Option 0** - Diese Option wird am Ende aller Optionen angezeigt, um das Ende einer Liste von Optionen zu kennzeichnen.
- **No Operation (NOP)** oder **IP Option 1** - In diesem Optionenfeld wird die Gesamtlänge der Feldvariable festgelegt.
- **Router Alert (RTRALT)** oder **IP Option 20** - Diese Option benachrichtigt Transit-Router, um den Inhalt des Pakets zu überprüfen, selbst wenn das Paket nicht für diesen Router bestimmt ist.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere

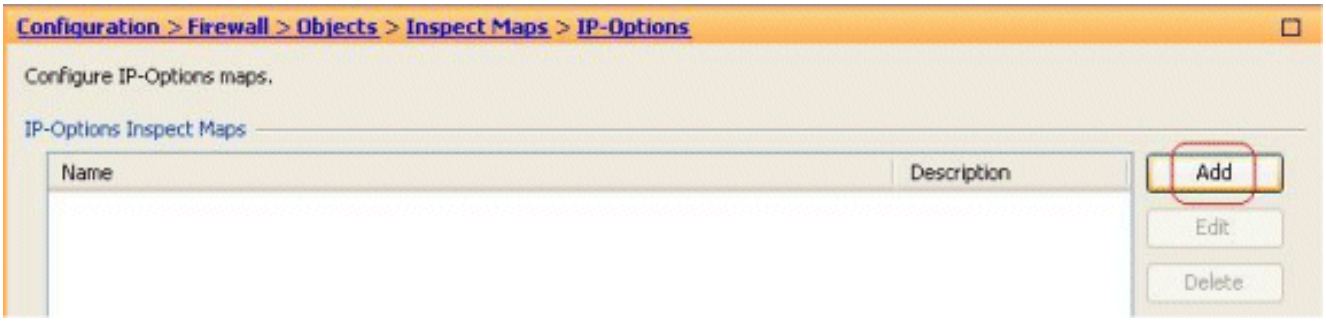
Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

ASDM-Konfiguration

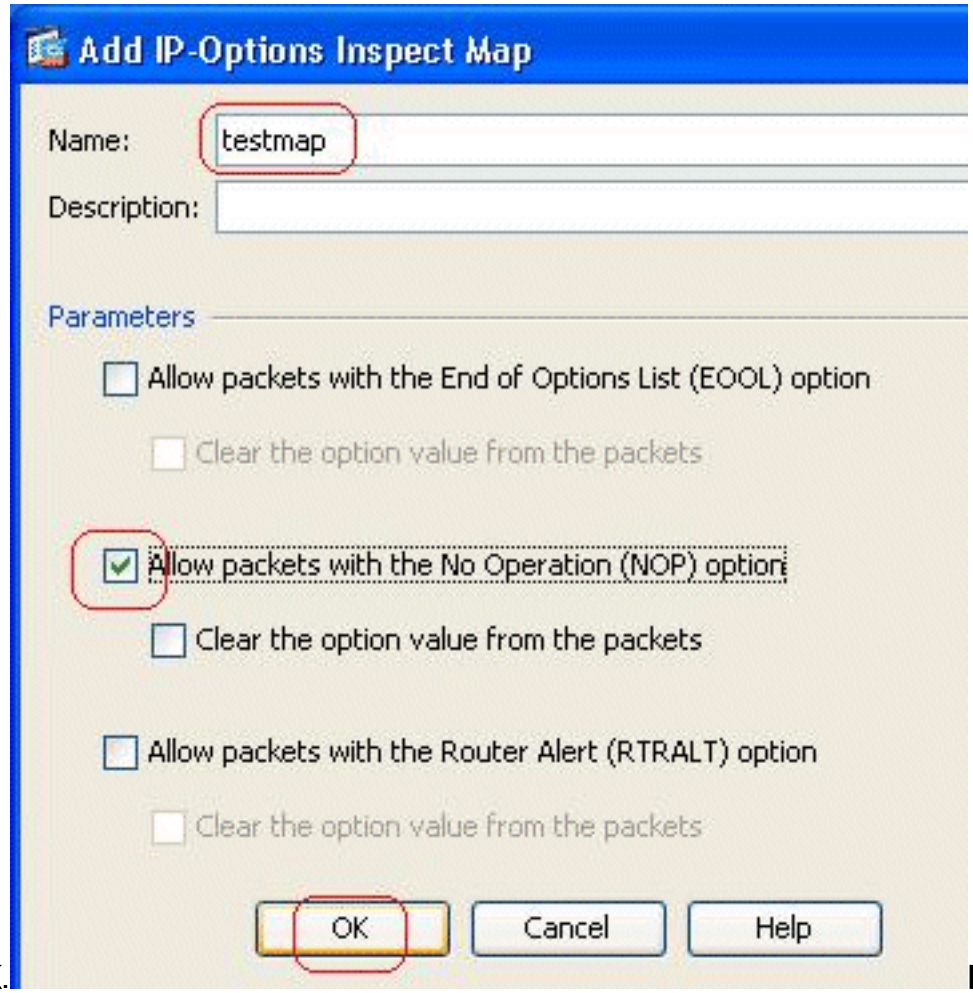
Mithilfe des ASDM können Sie sehen, wie die Überprüfung für die IP-Pakete aktiviert wird, die das Feld "IP Options" (IP-Optionen) enthalten.

Das Feld Optionen im IP-Header kann 0, eine oder mehrere Optionen enthalten, wodurch die Gesamtlänge der Feldvariablen berechnet wird. Beim IP-Header muss es sich jedoch um ein Vielfaches von 32 Bit handeln. Wenn die Anzahl der Bits aller Optionen kein Vielfaches von 32 Bit ist, wird die NOP-Option als "internes Padding" verwendet, um die Optionen an einer 32-Bit-Grenze auszurichten.

1. Gehen Sie zu **Configuration > Firewall > Objects > Inspect Maps > IP-Options, und klicken Sie auf Add.**

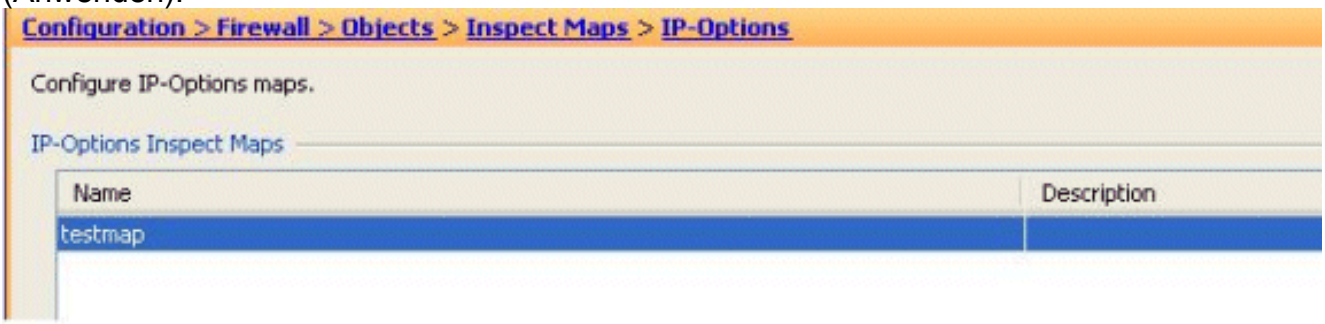


2. Das Fenster Add IP-Options Inspect Map (IP-Optionen-Analyseübersicht hinzufügen) wird angezeigt. Geben Sie den Namen der Inspect Map an, wählen Sie die **Option Allow packages with the No Operation (NOP) (Pakete ohne Vorgang zulassen) aus**, und klicken

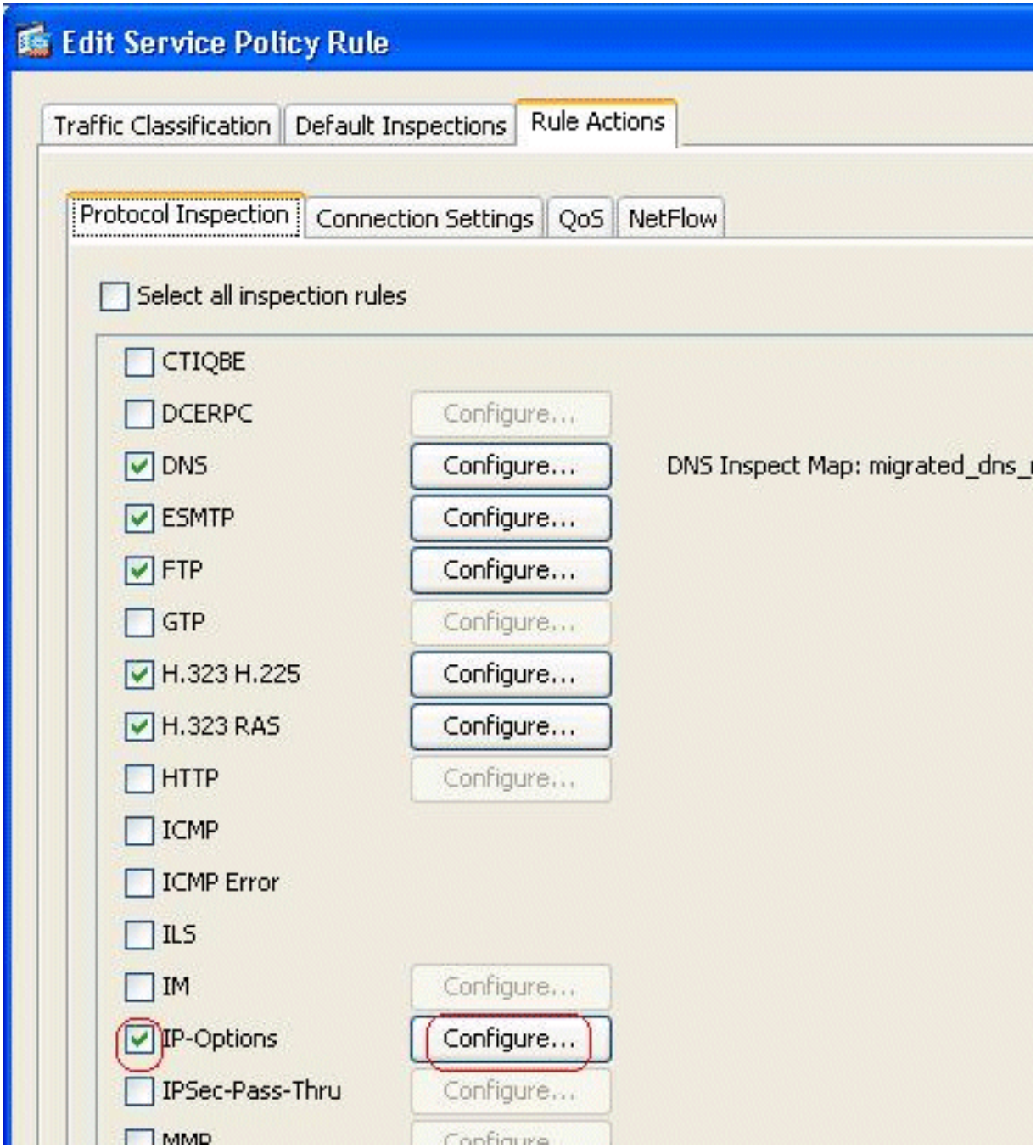
Sie auf **OK**. 

Hinweis: Sie können auch die Option **Clear the option value from the packages** auswählen, sodass dieses Feld im IP-Paket deaktiviert und die Pakete über die Cisco ASA übertragen werden.

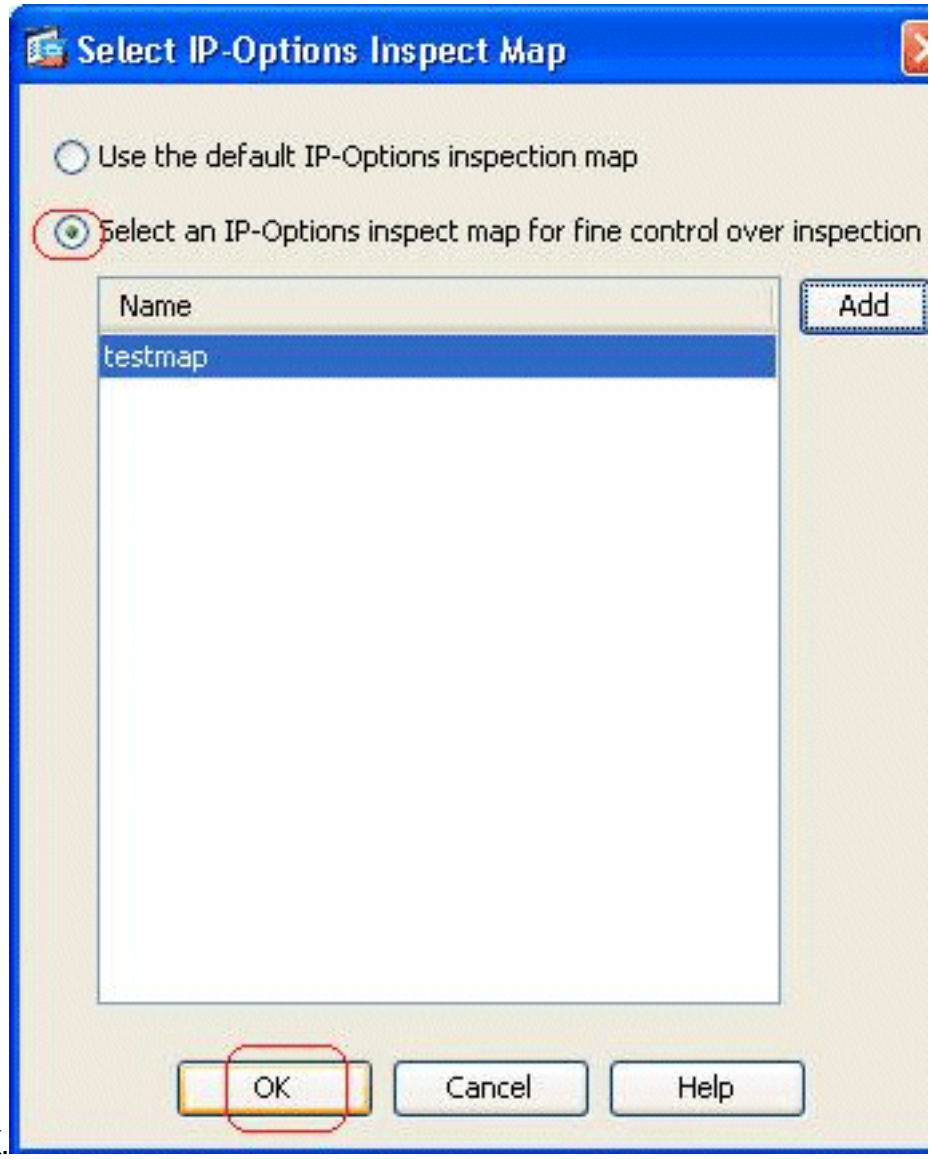
3. Eine neue inspect map namens **testmap** wird erstellt. Klicken Sie auf **Apply** (Anwenden).



4. Gehen Sie zu **Konfiguration > Firewall > Service Policy Rules**, wählen Sie die vorhandene globale Richtlinie aus, und klicken Sie auf **Edit**. Das Fenster "Service Policy bearbeiten" wird angezeigt. Wählen Sie die Registerkarte **Regelaktionen**, markieren Sie das **IP-Optionen-**Element, und wählen Sie **Konfigurieren** aus, um die neu erstellte Inspektionsübersicht zuzuweisen.

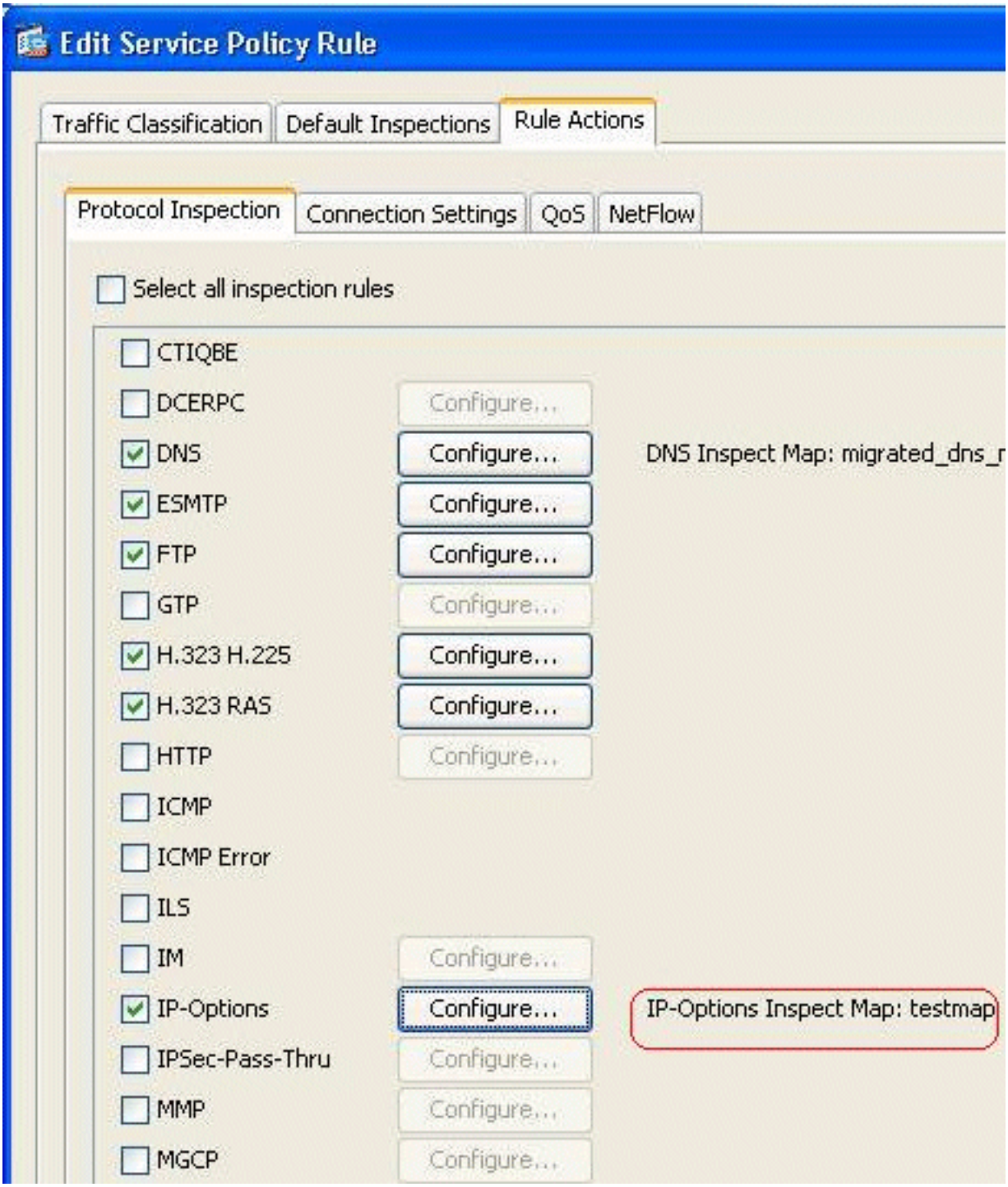


5. Wählen Sie **Eine IP-Optionen-Prüfzuordnung für eine genaue Kontrolle über Inspektion > Testmap auswählen** aus, und klicken Sie auf

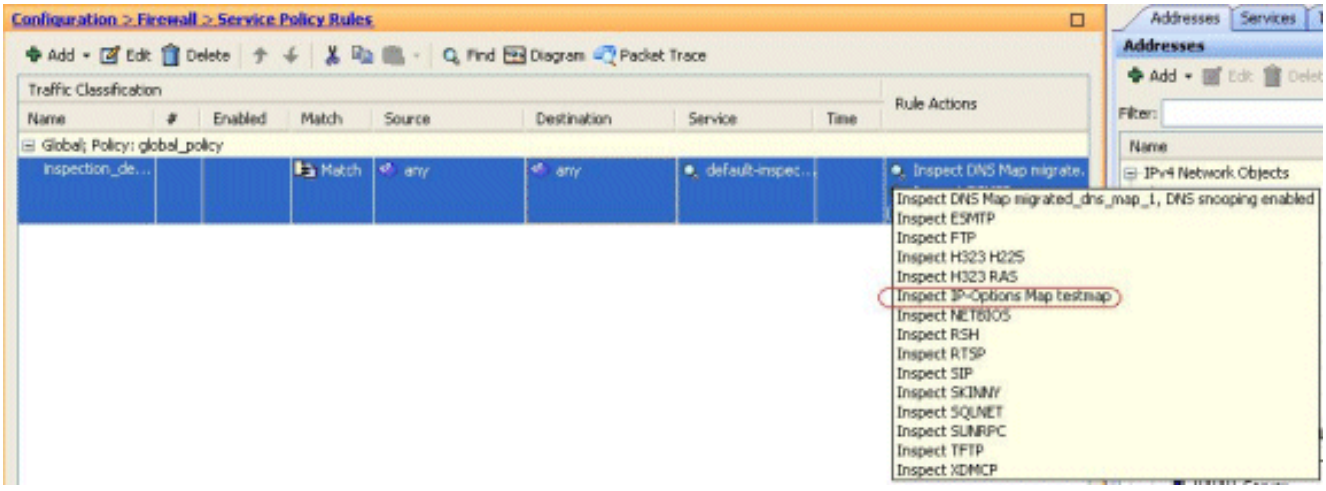


OK.

6. Die ausgewählte Prüfzuordnung kann im Feld **IP-Optionen** angezeigt werden. Klicken Sie auf **OK**, um zur Registerkarte "Service Policy Rules" (Servicebestimmungen) zurückzukehren.



7. Bewegen Sie den Mauszeiger über die Registerkarte **Regelaktionen**, damit Sie alle verfügbaren Protokollprüfungszuordnungen für diese globale Karte finden.



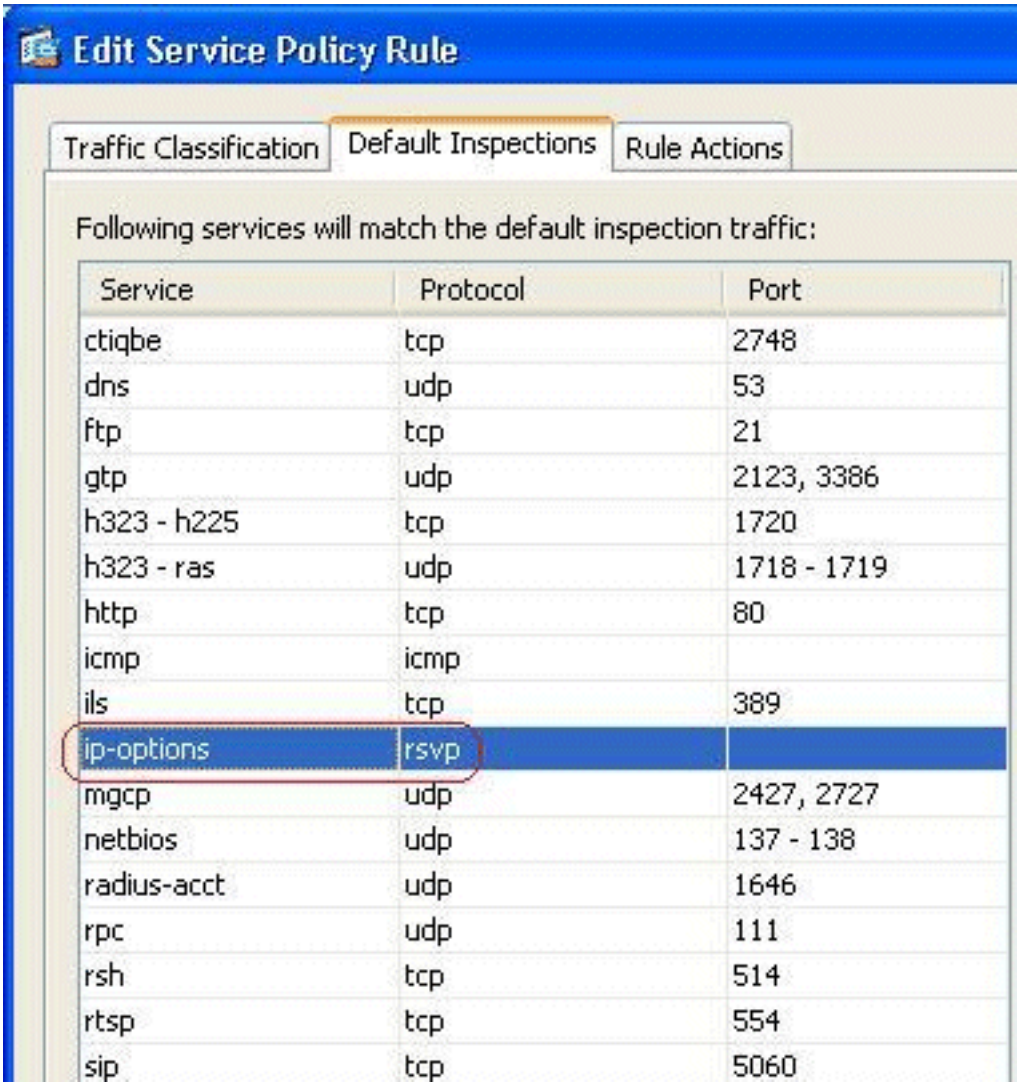
Im Folgenden finden Sie einen Beispielausschnitt der entsprechenden CLI-Konfiguration, der als Referenz dient:

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
```

Standardverhalten der Cisco ASA, um RSVP-Pakete zuzulassen

Die IP Options Inspection ist standardmäßig aktiviert. Gehen Sie zu **Konfiguration > Firewall > Service Policy Rules**. Wählen Sie die globale Richtlinie aus, klicken Sie auf **Bearbeiten**, und wählen Sie die Registerkarte **Standardinspektionen aus**. Hier finden Sie das RSVP-Protokoll im Feld **IP-Optionen**. Dadurch wird sichergestellt, dass das RSVP-Protokoll geprüft und über die Cisco ASA zugelassen wird. So wird ein End-to-End-Videoanruf problemlos eingerichtet.



Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show service-policy inspect ip-options** - Zeigt die Anzahl der verworfenen und/oder zulässigen Pakete gemäß der konfigurierten Service-Richtlinienregel an.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation für Cisco Systeme