ASDM 6.3 이상에서 IP 옵션 검사 구성

목차

소개

이 문서에서는 특정 IP 옵션이 활성화된 IP 패킷을 전달하기 위해 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 릴리스 버전 8.3 이상을 실행하는 Cisco ASA
- 소프트웨어 릴리스 버전 6.3 이상을 실행하는 Cisco Adaptive Security Manager

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

각 IP 패킷에는 Options 필드가 있는 IP 헤더가 포함되어 있습니다. 일반적으로 IP 옵션이라고 하는 Options 필드는 일부 상황에서는 필요한 제어 기능을 제공하지만 대부분의 일반적인 커뮤니케이션에는 필요하지 않습니다. 특히, IP 옵션에는 타임스탬프, 보안 및 특별 라우팅에 대한 프로비저닝이 포함됩니다. IP 옵션 사용은 선택 사항이며, 필드에는 0, 1 또는 그 이상의 옵션이 포함될 수 있습니다.

IP Options는 보안 위험이며 IP Options 필드가 활성화된 IP 패킷이 ASA를 통해 전달되는 경우 네트워크의 내부 설정에 대한 정보가 외부로 유출됩니다. 따라서 공격자는 네트워크의 토폴로지를 매핑할 수 있습니다. Cisco ASA는 기업에서 보안을 적용하는 디바이스이므로 기본적으로 IP Options 필드가 활성화된 패킷을 삭제합니다. 참조할 수 있도록 샘플 syslog 메시지가 여기에 표시됩니다.

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||10.110.1.34 XX.YY.ZZ.ZZ IP , IP : " "
```

그러나 비디오 트래픽이 Cisco ASA를 통과해야 하는 특정 구축 시나리오에서는 특정 IP 옵션이 있는 IP 패킷을 전달해야 합니다. 그렇지 않으면 화상 회의 통화가 실패할 수 있습니다. Cisco ASA 소프트웨어 릴리스 버전 8.2.2 부터는 "Inspection for IP options"라는 새로운 기능이 도입되었습니다. 이 기능을 사용하면 Cisco ASA를 통해 허용되는 특정 IP 옵션의 패킷을 제어할 수 있습니다.

기본적으로 이 기능은 활성화되어 있으며 글로벌 정책에서 아래 IP 옵션에 대한 검사가 활성화됩니다. 이 검사를 구성하면 ASA가 패킷이 통과할 수 있도록 하거나, 지정된 IP 옵션을 지운 다음 패킷이 통과할 수 있도록 합니다.

- **옵션 목록 끝(EOOL)** 또는 **IP 옵션 0** - 이 옵션은 옵션 목록의 끝을 표시하기 위해 모든 옵션의 끝에 나타납니다.
- **NOP(No Operation)** 또는 **IP Option 1** - 이 옵션 필드는 필드 변수의 전체 길이를 설정합니다.
- **RTRALT(Router Alert)** 또는 **IP Option 20** - 이 옵션은 패킷이 해당 라우터로 전송되지 않은 경우에도 트랜짓 라우터에 패킷 내용을 검사하도록 알립니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

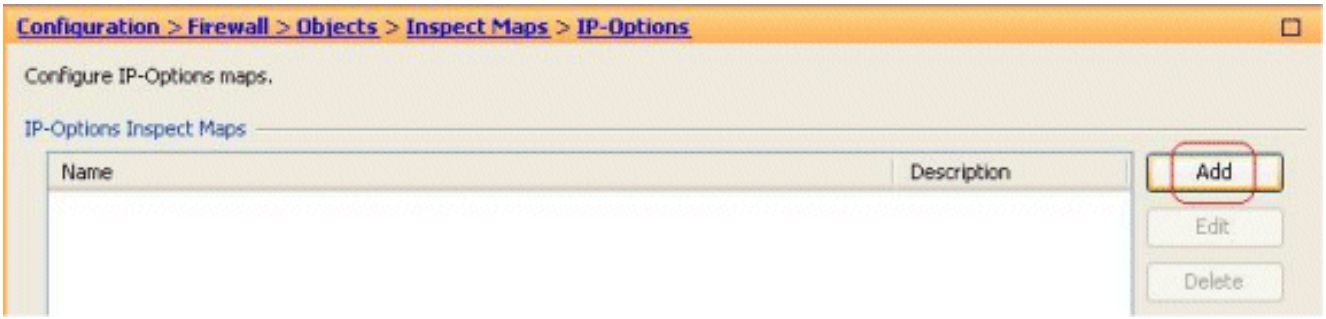
참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

ASDM 컨피그레이션

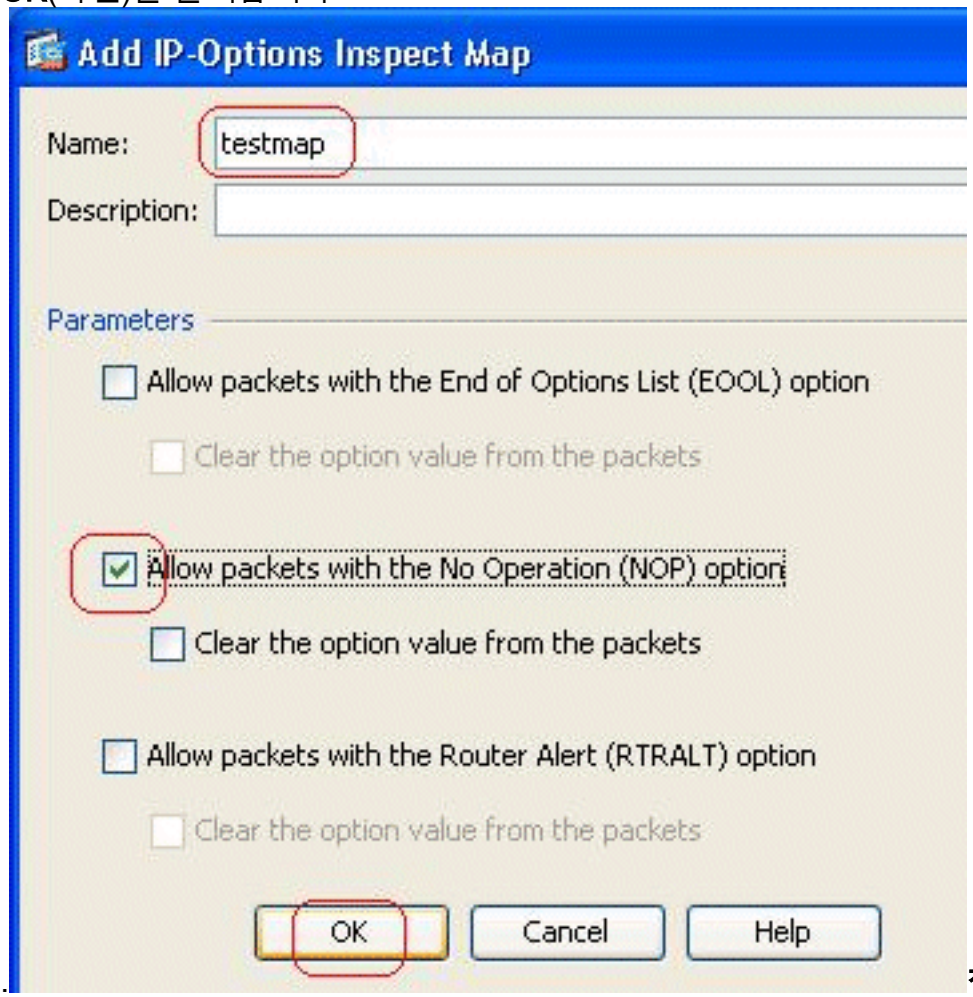
ASDM을 사용하면 IP Options 필드인 NOP가 있는 IP 패킷에 대해 검사를 활성화하는 방법을 확인할 수 있습니다.

IP 헤더의 Options 필드는 0, 1 또는 그 이상의 옵션을 포함할 수 있으며, 이는 필드 변수의 전체 길이를 만듭니다. 그러나 IP 헤더는 32비트의 배수여야 합니다. 모든 옵션의 비트 수가 32비트의 배수가 아닌 경우 32비트 경계에서 옵션을 정렬하기 위해 NOP 옵션을 "내부 패딩"으로 사용합니다.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > Objects(**개체**) > Inspect Maps(검사 맵) > **IP-Options(IP-Options)로 이동하여 Add(추가)를 클릭합니다**
   .

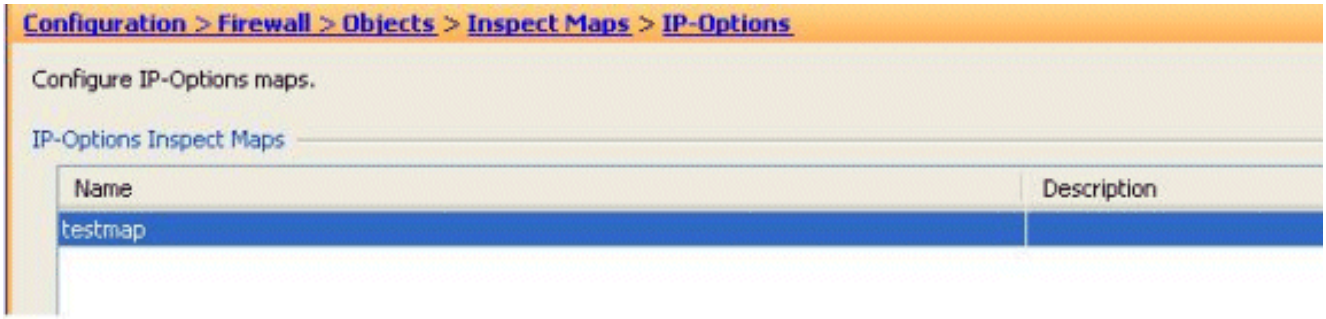


2. Add IP-Options Inspect Map 창이 나타납니다. Inspect Map의 이름을 지정하고 **Allow packets with the No Operation (NOP)(NOP(No Operation) 옵션이 있는 패킷 허용)을** 선택한 다음 **OK**(확인)를 클릭합니다



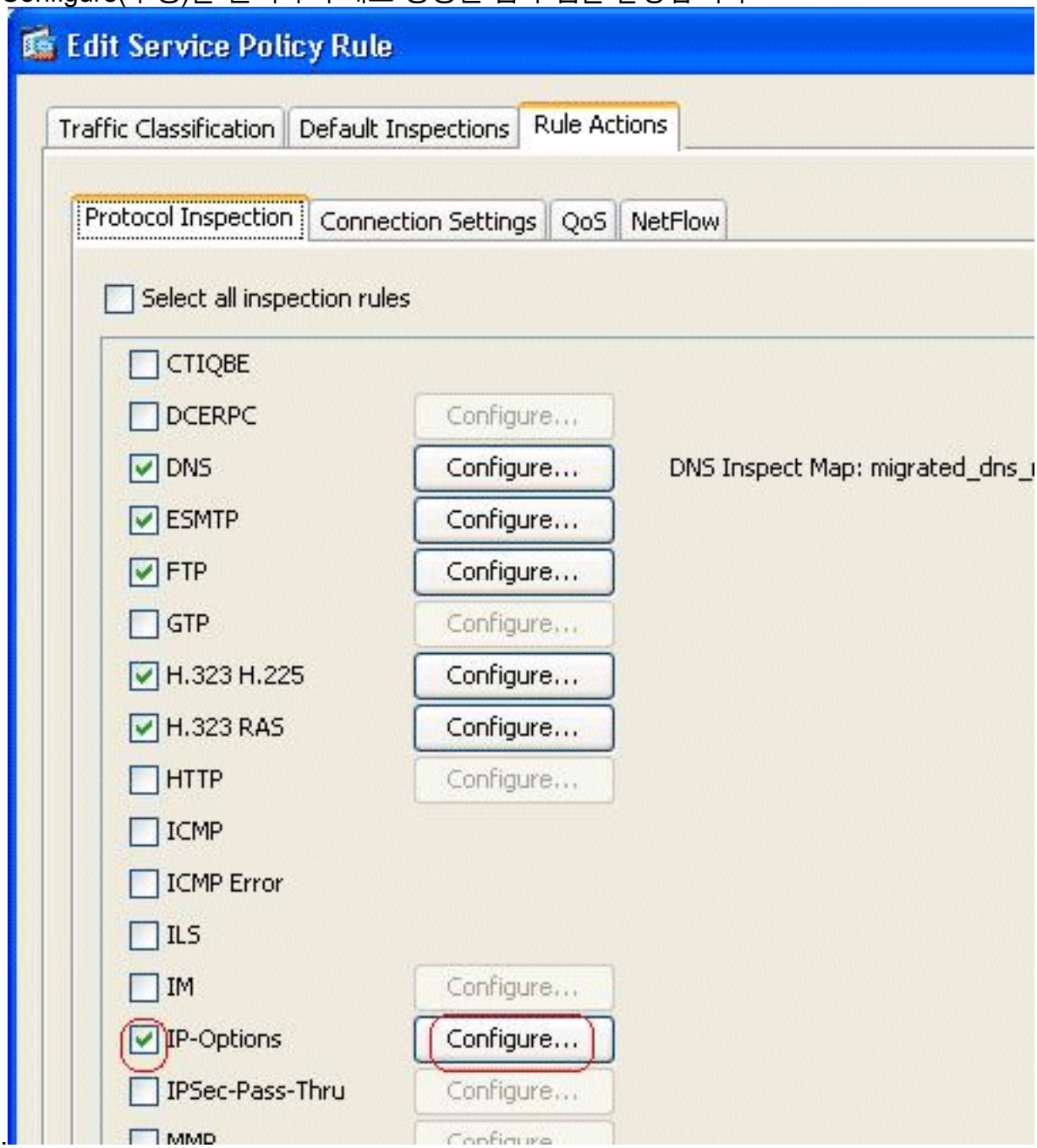
참고: 또한 Clear the **option value from the packets** 옵션을 선택하여 IP 패킷의 이 필드가 비활성화되고 패킷이 Cisco ASA를 통과하도록 할 수 있습니다.

3. testmap이라는 새 검사 맵**이** 생성됩니다. Apply를 **클릭합니다**

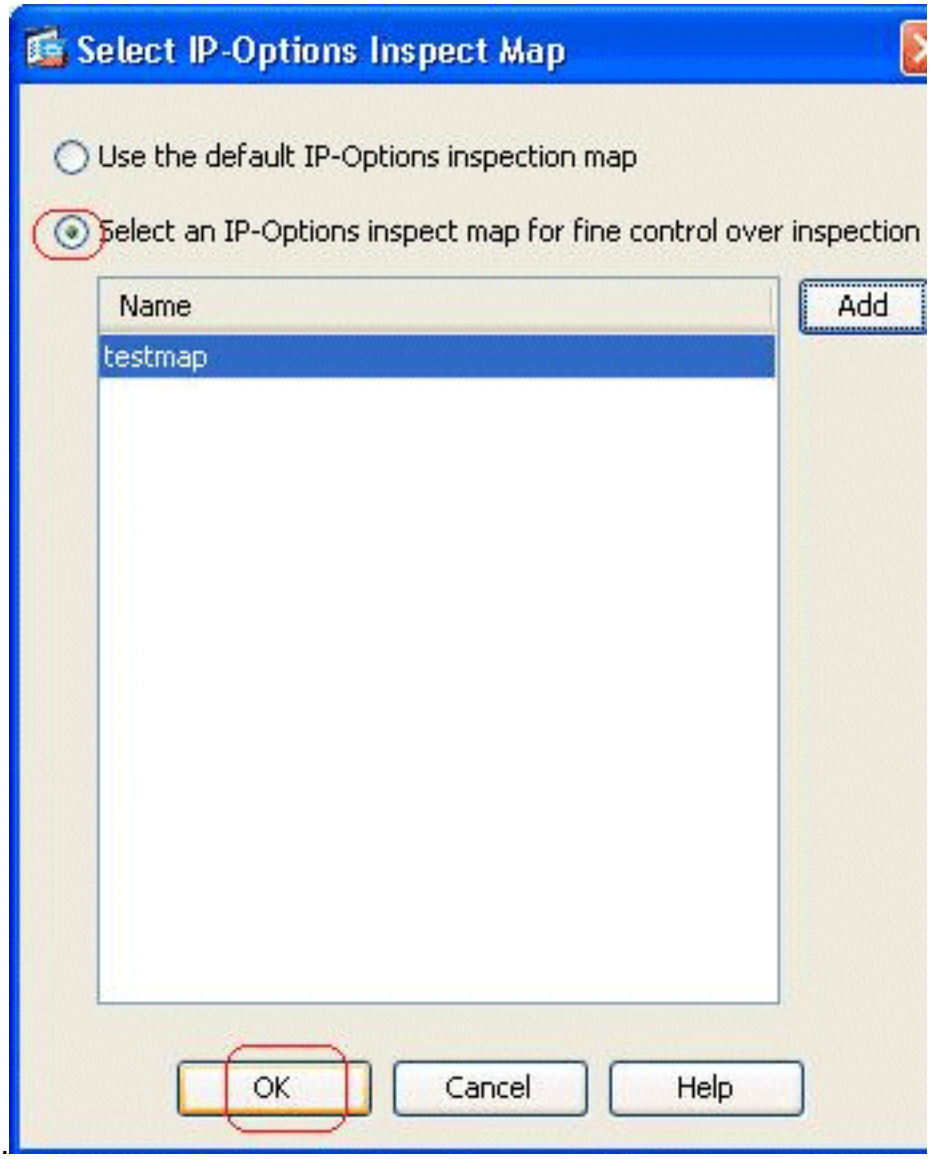


4. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > Service Policy Rules(**서비스 정책 규칙**)로 이동하여 기존 글로벌 정책을 선택하고 Edit(수정)를 **클릭합니다**. Edit Service Policy Rule 창이 나타납니다. Rule Actions(**규칙 작업**) 탭을 선택하고 **IP-Options** 항목을 선택한 다음

Configure(구성)를 선택하여 새로 생성된 검사 맵을 할당합니다

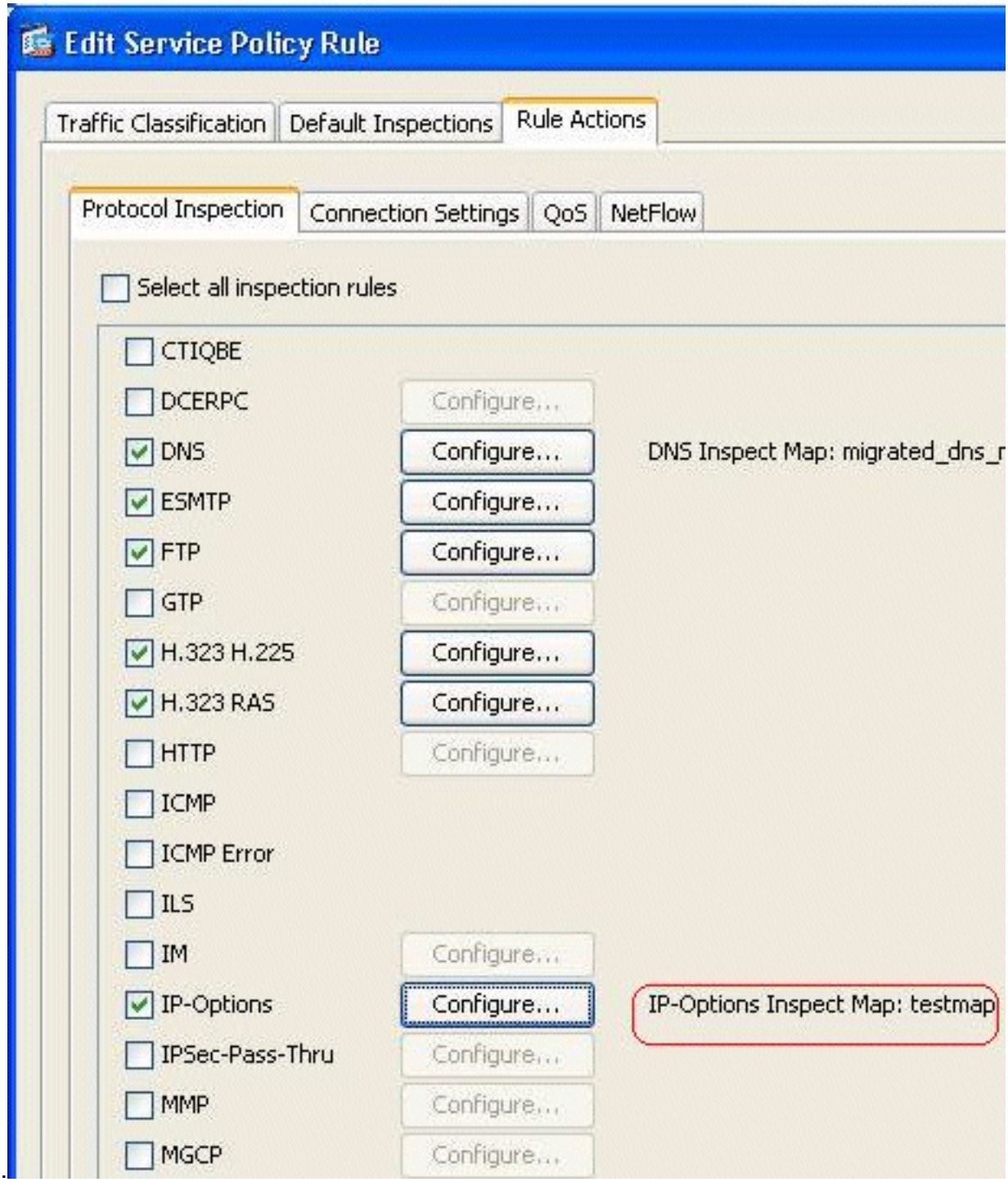


5. Select an **IP-Options inspect map for fine control over inspection > testmap을 선택하고 OK를**



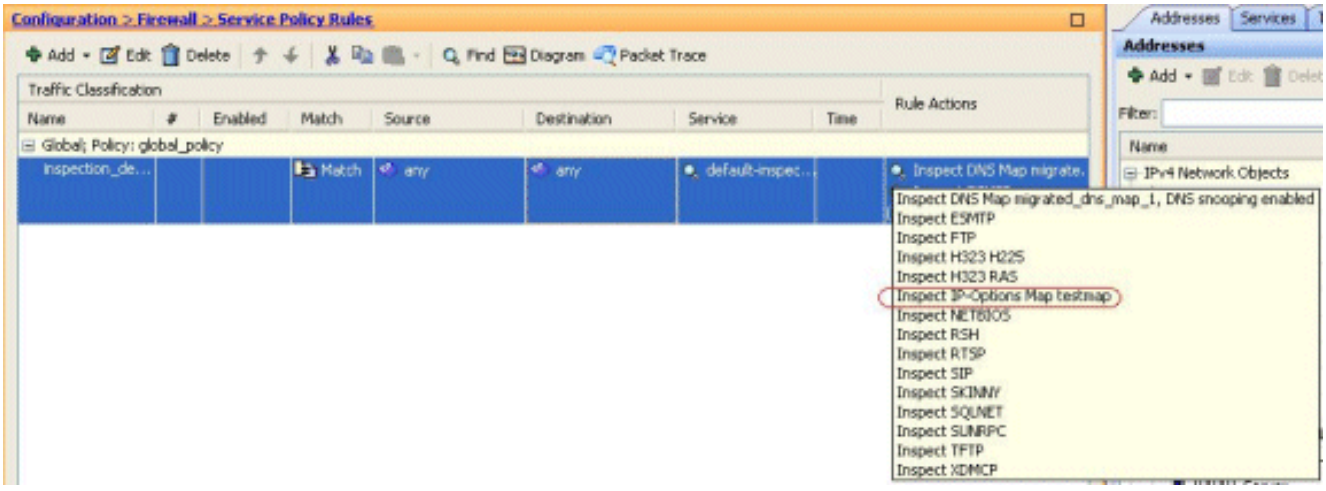
클릭합니다.

6. 선택한 검사 맵은 **IP-Options** 필드에서 볼 수 있습니다. OK(**확인**)를 클릭하여 Service Policy Rules(서비스 정책 규칙) 탭으로 돌아갑니다



7. 마우스를 사용하여 **Rule Actions** 탭 위에 마우스를 올려 이 전역 맵과 연결된 사용 가능한 모든 프로토콜 검사 맵을 찾을 수 있습니다

.



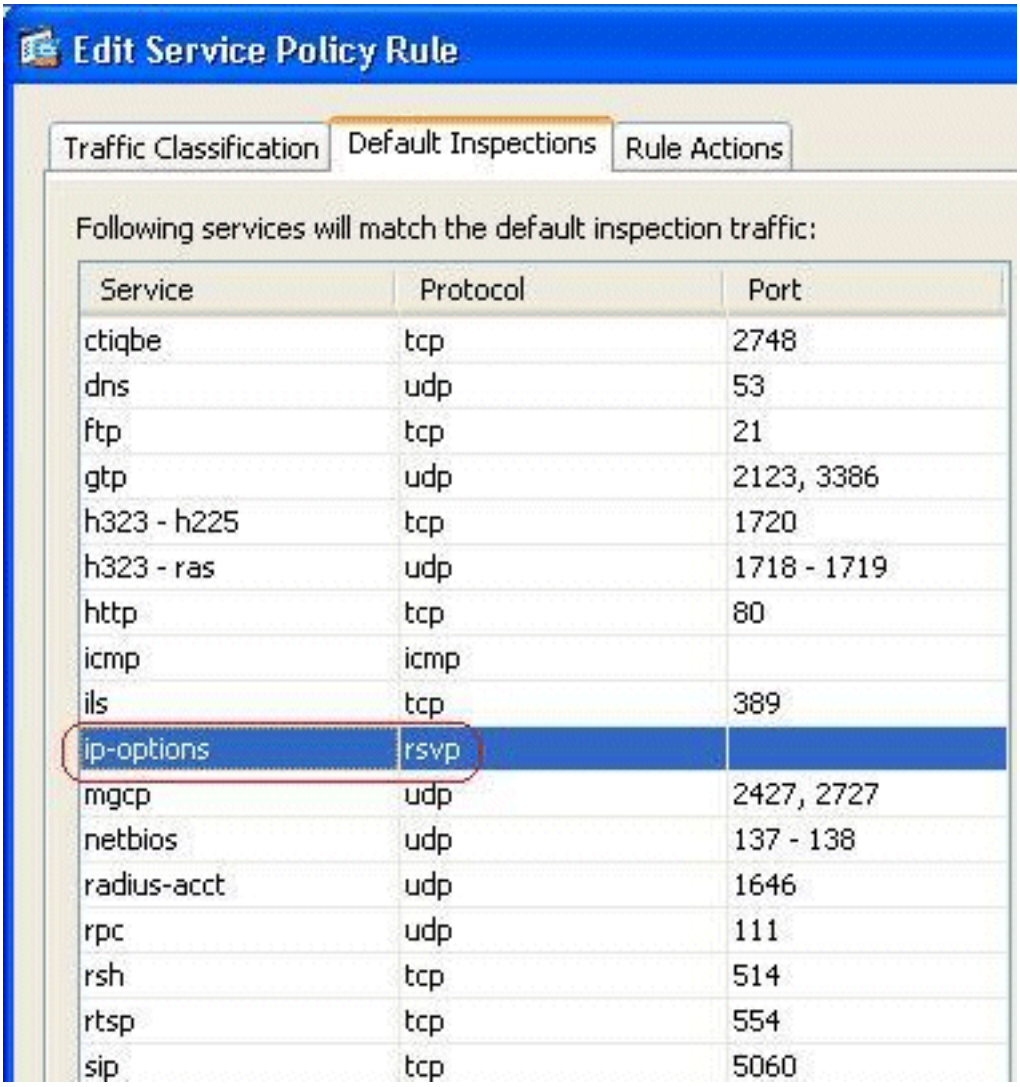
다음은 참조용 등가 CLI 컨피그레이션의 샘플 조각입니다.

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 패킷을 허용하기 위한 Cisco ASA의 기본 동작

IP 옵션 검사는 기본적으로 활성화되어 있습니다. Configuration(컨피그레이션) > Firewall(방화벽) > **Service Policy Rules(서비스 정책 규칙)로 이동합니다**. Global Policy(전역 정책)를 선택하고 **Edit(편집)**를 클릭한 다음 **Default Inspections(기본 검사)** 탭을 선택합니다. 여기서 **IP-Options** 필드에서 RSVP 프로토콜을 찾을 수 있습니다. 이렇게 하면 RSVP 프로토콜이 Cisco ASA를 통해 검사 및 허용됩니다. 따라서 문제 없이 엔드 투 엔드 비디오 통화가 설정됩니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show service-policy inspect ip-options** - 구성된 서비스 정책 규칙에 따라 삭제 및/또는 허용되는 패킷 수를 표시합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances 기술 지원
- 기술 지원 및 문서 – Cisco Systems