라우터 및 SDM으로 Cisco IOS IPS 구성

목차

소개

이 문서에서는 12.4(15)T3 이상 릴리스에서 Cisco IOS® IPS(Intrusion Prevention System)를 구성하기 위해 Cisco 라우터 및 SDM(Security Device Manager) 버전 2.5를 사용하는 방법에 대해 설명합니다.

IOS IPS와 관련된 SDM 2.5의 향상된 기능은 다음과 같습니다.

- 서명 목록 GUI에 표시되는 총 컴파일된 서명 번호
- SDM 서명 파일(zip 파일 형식; 예: sigv5-SDM-S307.zip) 및 CLI 서명 패키지(pkg 파일 형식; 예를 들어, IOS-S313-CLI.pkg)은 하나의 작업으로 함께 다운로드할 수 있습니다.
- 다운로드한 서명 패키지를 옵션으로 라우터에 자동으로 푸시할 수 있습니다.

초기 프로비저닝 프로세스에 포함되는 작업은 다음과 같습니다.

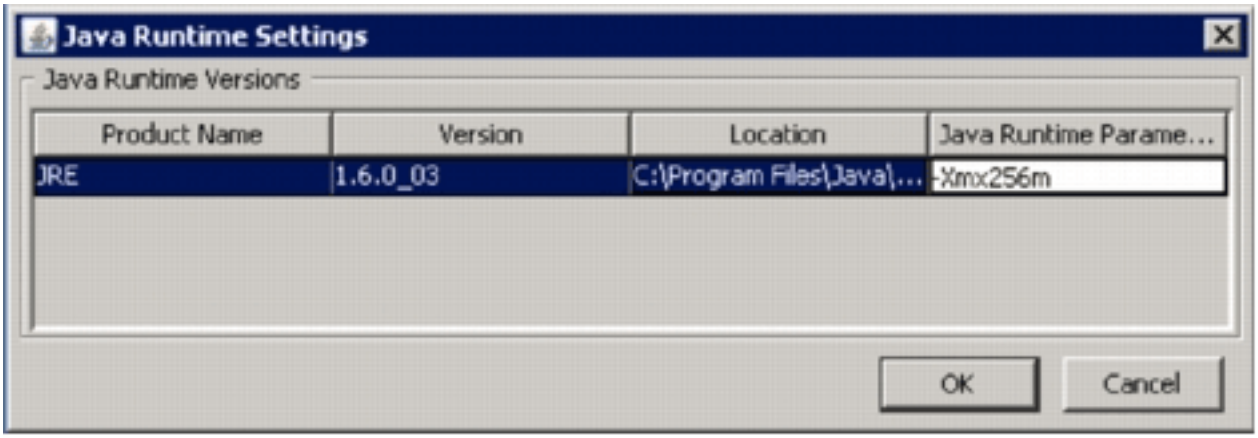
1. SDM 2.5를 다운로드하여 설치합니다.
2. IOS IPS 서명 패키지를 로컬 PC에 다운로드하려면 SDM 자동 업데이트를 사용합니다.
3. IOS IPS를 구성하려면 IPS 정책 마법사를 시작합니다.
4. IOS IPS 컨피그레이션 및 서명이 올바르게 로드되었는지 확인합니다.

Cisco SDM은 스마트 마법사를 통해 라우터 및 보안 구성을 간소화하는 웹 기반 구성 툴로서, CLI(Command Line Interface)에 대한 지식 없이도 고객이 Cisco 라우터를 빠르고 쉽게 구축, 구성 및 모니터링할 수 있도록 지원합니다.

SDM 버전 2.5는 Cisco.com의 http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm에서 다운로드할 수 있습니다(등록된 고객만 해당). 릴리스 노트는 http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html에서 확인할 수 있습니다.

참고: Cisco SDM의 화면 해상도는 1024 x 768 이상이어야 합니다.

참고: Cisco SDM은 IOS IPS를 구성하려면 Java 메모리 힙의 크기가 256MB 이상이어야 합니다. Java 메모리 힙의 크기를 변경하려면 Java 제어판을 열고 **Java** 탭을 클릭한 다음 Java 애플릿 런타임 설정 아래 있는 **보기**를 **클릭한** 다음 Java 런타임 매개변수 열에 -Xmx256m을 입력합니다.



사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 12.4(15)T3 이상 릴리스의 Cisco IOS IPS
- Cisco 라우터 및 SDM(Security Device Manager) 버전 2.5

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.

구성

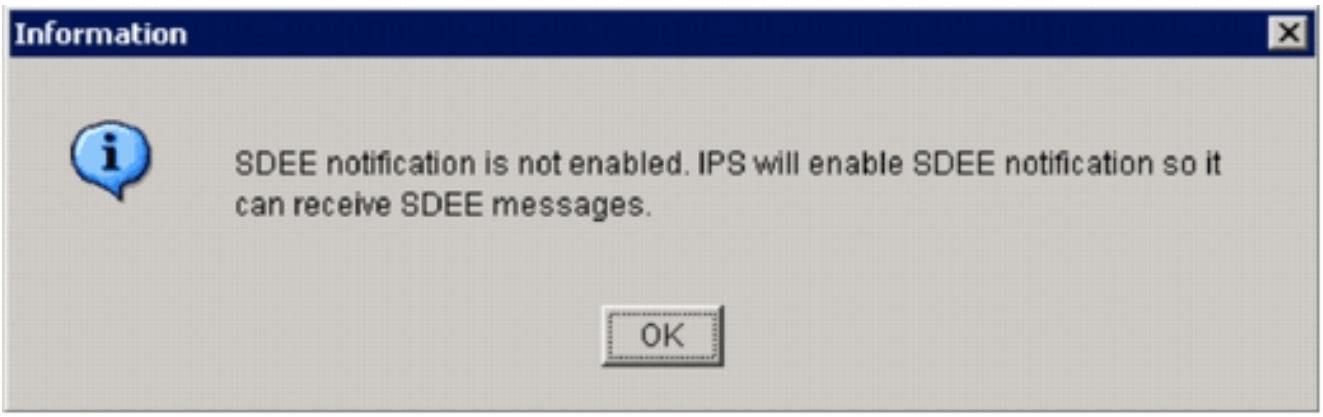
참고: SDM을 사용하여 IOS IPS를 프로비저닝할 때 메시지를 모니터링하려면 라우터에 대한 콘솔 또는 텔넷 세션을 엽니다('용어 모니터'가 켜짐).

1. Cisco.com의 http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm에서 SDM 2.5를 다운로드하여 (등록된 고객만 해당) 로컬 PC에 설치합니다.
2. 로컬 PC에서 SDM 2.5를 실행합니다.
3. IOS IPS Login 대화 상자가 나타나면 라우터에 대한 SDM 인증에 사용하는 것과 동일한 사용

자 이름과 암호를 입력합니다.

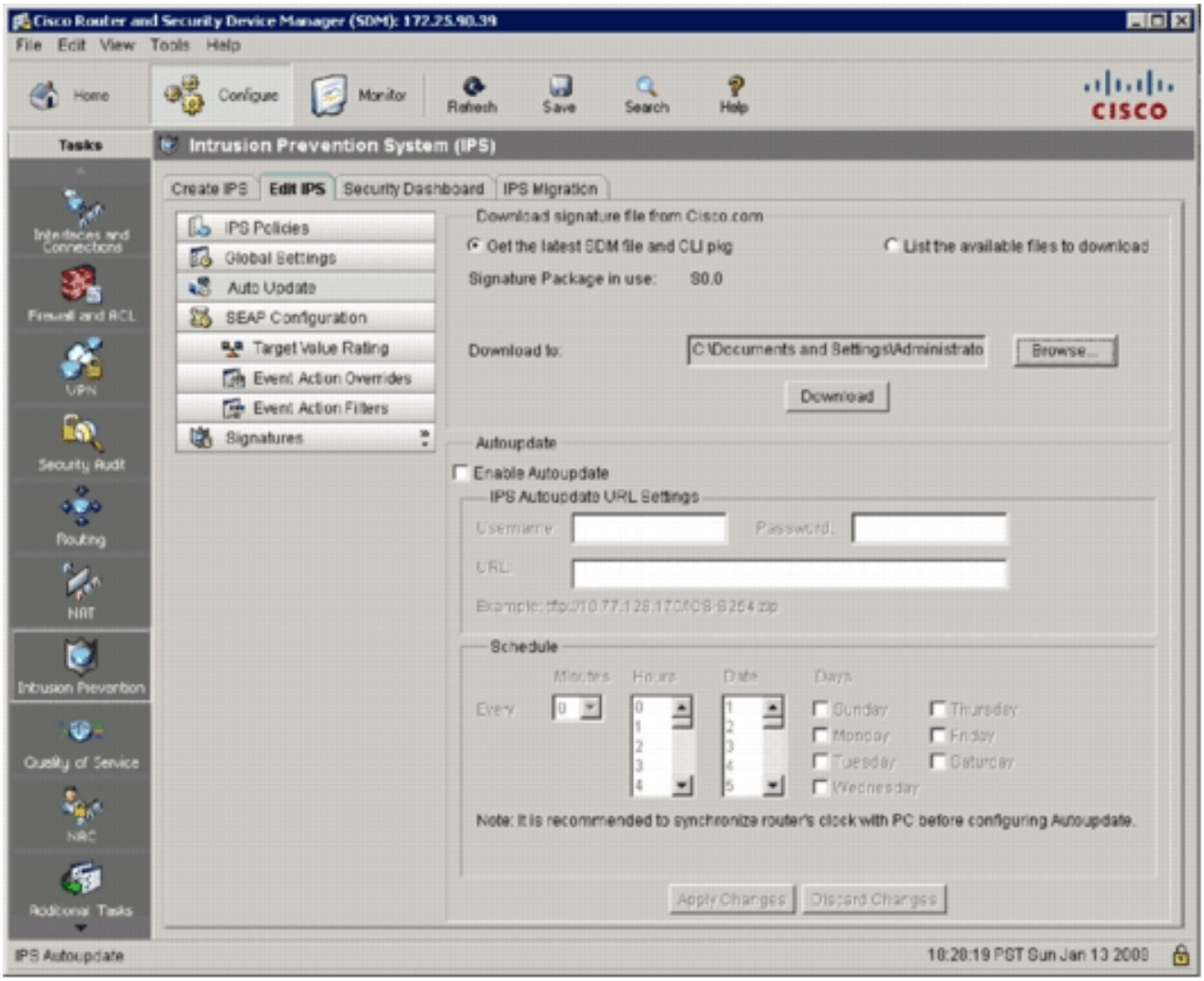
4. SDM 사용자 인터페이스에서 Configure를 클릭한 다음 **Intrusion Prevention**을 클릭합니다.
5. **Edit IPS** 탭을 클릭합니다.
6. 라우터에서 SDEE 알림이 활성화되지 않은 경우 SDEE 알림을 활성화하려면 **OK**를 클릭합니다

.



7. Edit IPS(IPS 편집) 탭의 Download signature file from Cisco.com(Cisco.com에서 서명 파일 다운로드) 영역에서 **Get the latest SDM file and CLI pkg(최신 SDM 파일 가져오기 및 CLI pkg)** 라디오 버튼을 클릭한 다음 **Browse**를 클릭하여 다운로드한 파일을 저장할 로컬 PC의 디렉토리를 선택합니다.TFTP 또는 FTP 서버 루트 디렉토리를 선택할 수 있습니다. 이 디렉토리는 나중에 라우터에 서명 패키지를 구축할 때 사용됩니다.
8. **Download(다운로드)를 클릭합니다**

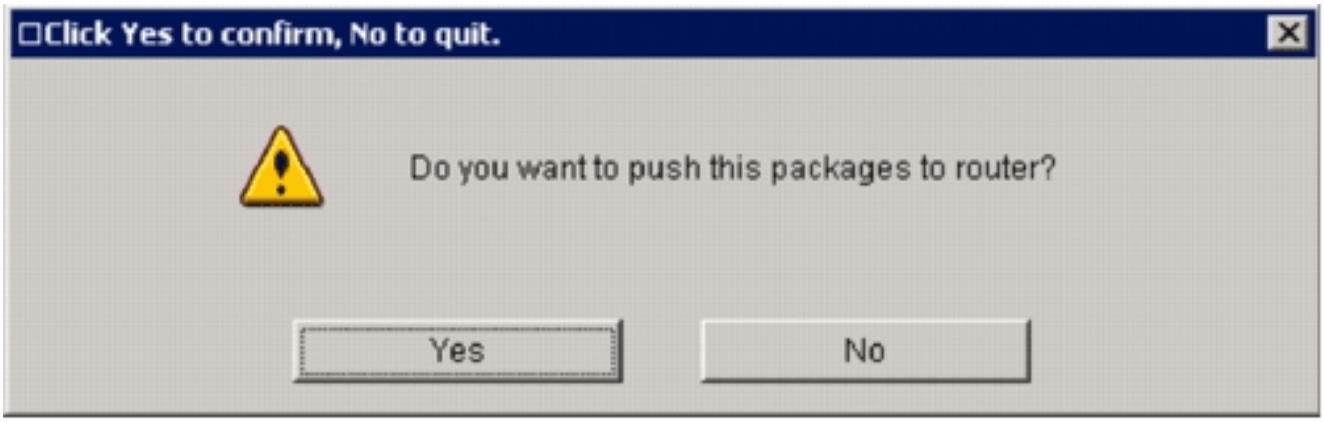
.



9. CCO 로그인 대화 상자가 나타나면 CCO 등록 사용자 이름과 암호를 사용합니다

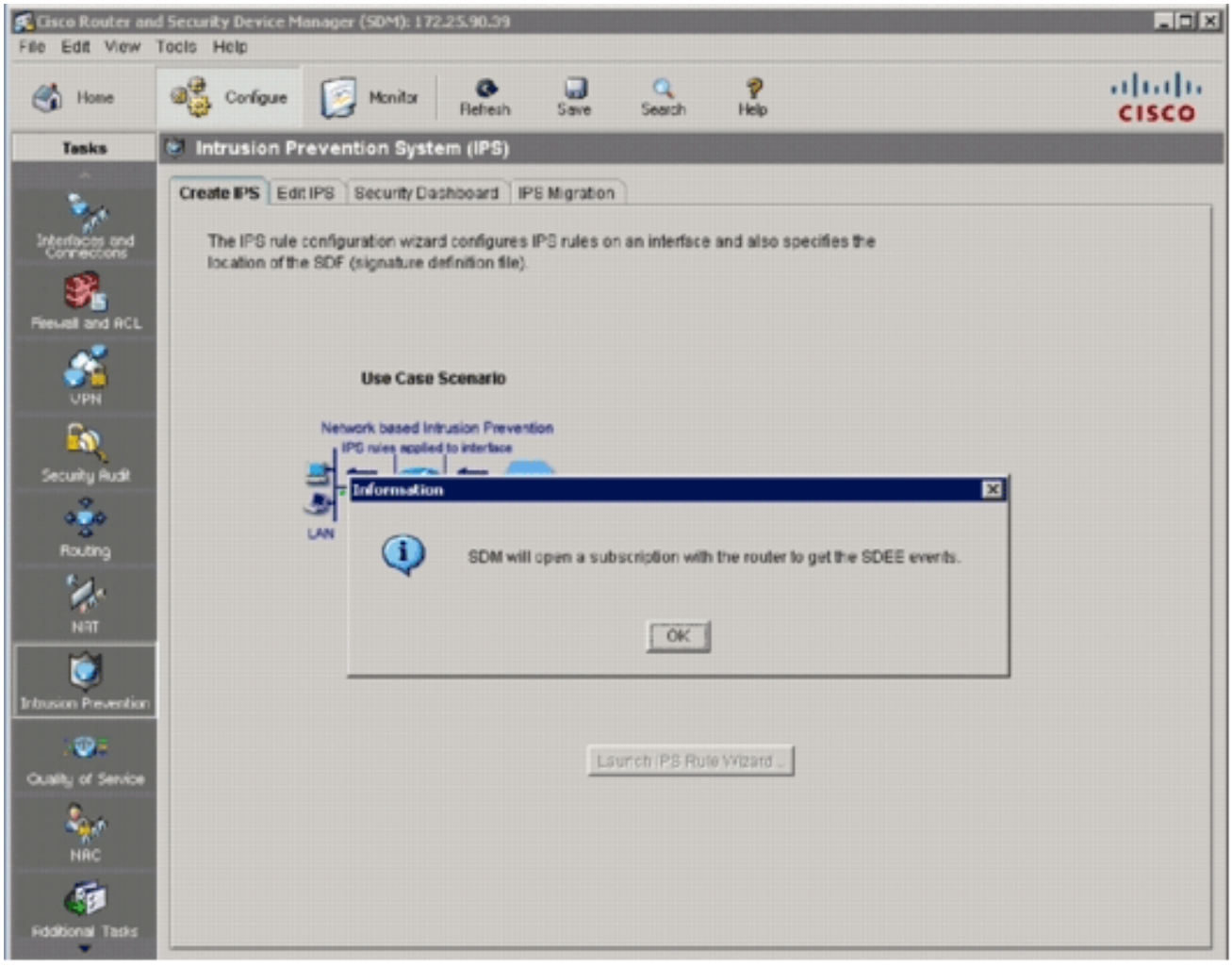
. SDM은 Cisco.com에 연결하여 SDM 파일(예: sigv5-SDM-S307.zip) 및 CLI pkg 파일(예: IOS-S313-CLI.pkg)을 7단계에서 선택한 디렉토리로 다운로드하기 시작합니다.두 파일이 모두 다운로드되면 SDM은 다운로드한 서명 패키지를 라우터로 푸시하라는 메시지를 표시합니다

.



10. IOS IPS가 라우터에 아직 구성되지 않았으므로 No를 클릭합니다.
11. SDM이 최신 IOS CLI 서명 패키지를 다운로드한 후 **Create IPS** 탭을 클릭하여 초기 IOS IPS 컨피그레이션을 생성합니다.
12. 라우터에 변경 사항을 적용하라는 메시지가 표시되면 Apply Changes(변경 사항 적용)를 **클릭합니다**.
13. Launch **IPS Rule Wizard를 클릭합니다**.SDM이 알림을 검색하기 위해 라우터에 대한 SDEE 서브스크립션을 설정해야 함을 알리는 대화 상자가 나타납니다

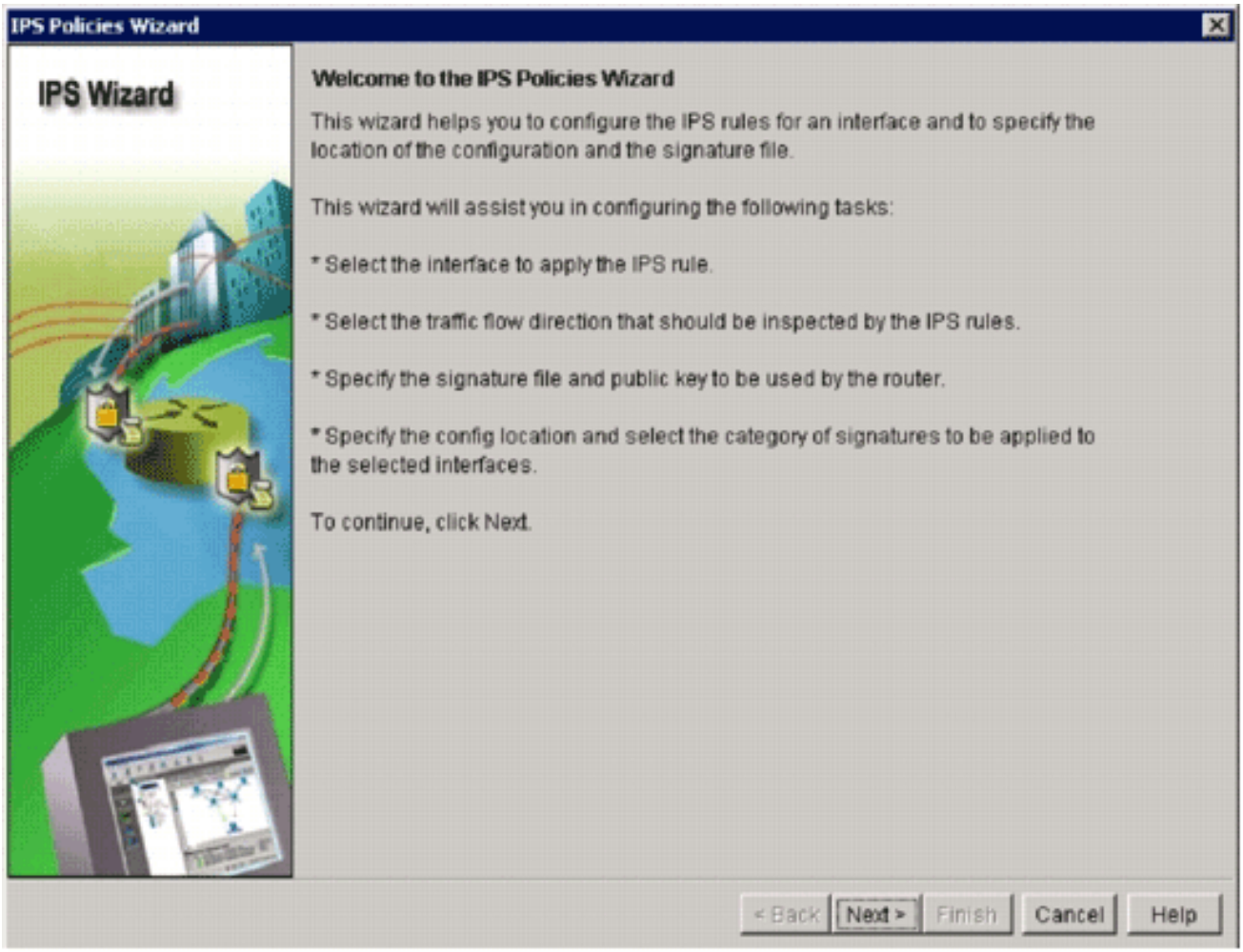
.



14. **확인**을 **클릭합니다**.Authentication Required 대화 상자가 나타납니다

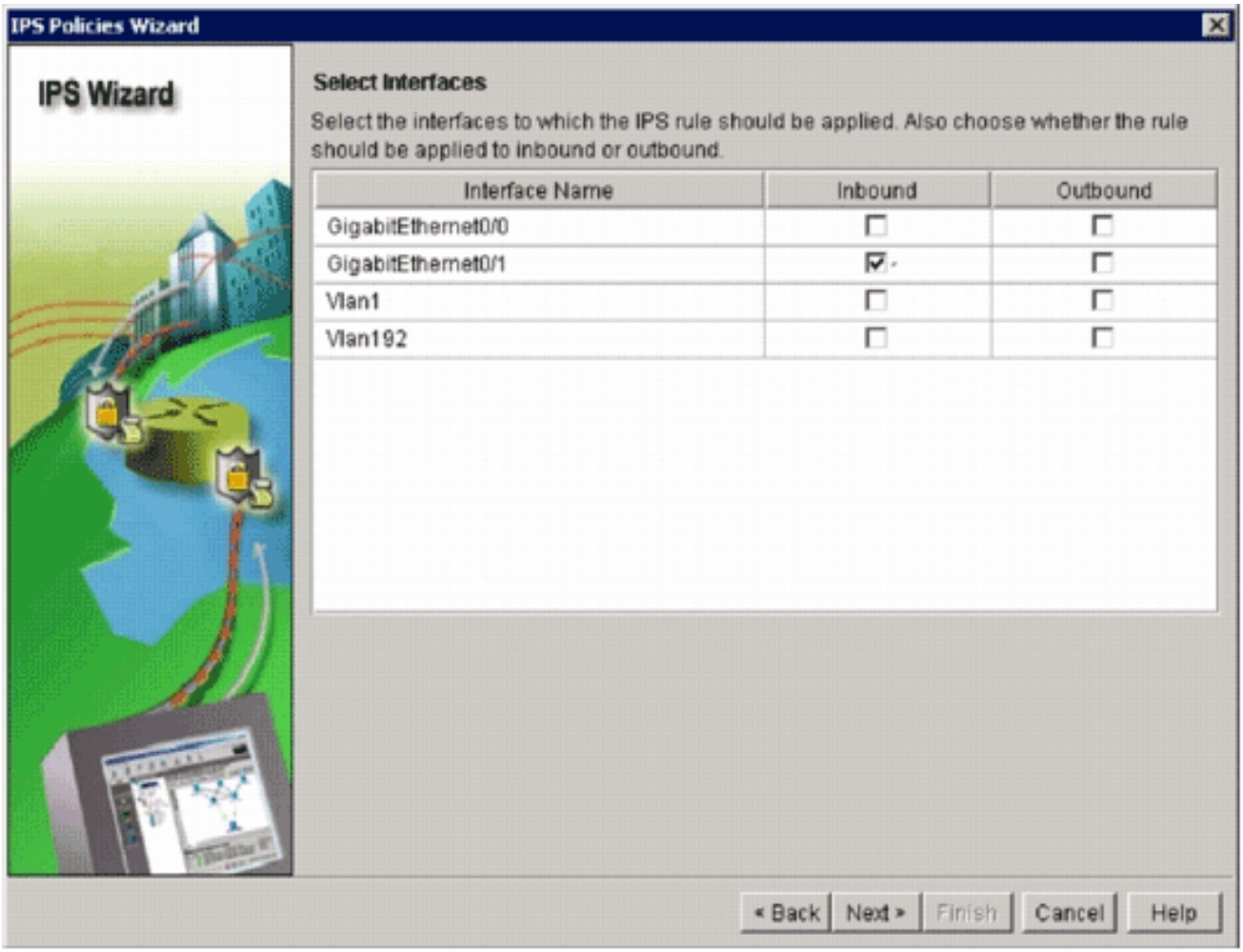
15. SDM이 라우터에 인증하는 데 사용한 사용자 이름과 암호를 입력하고 **OK**를 클릭합니다.IPS Policies Wizard 대화 상자가 나타납니다

.



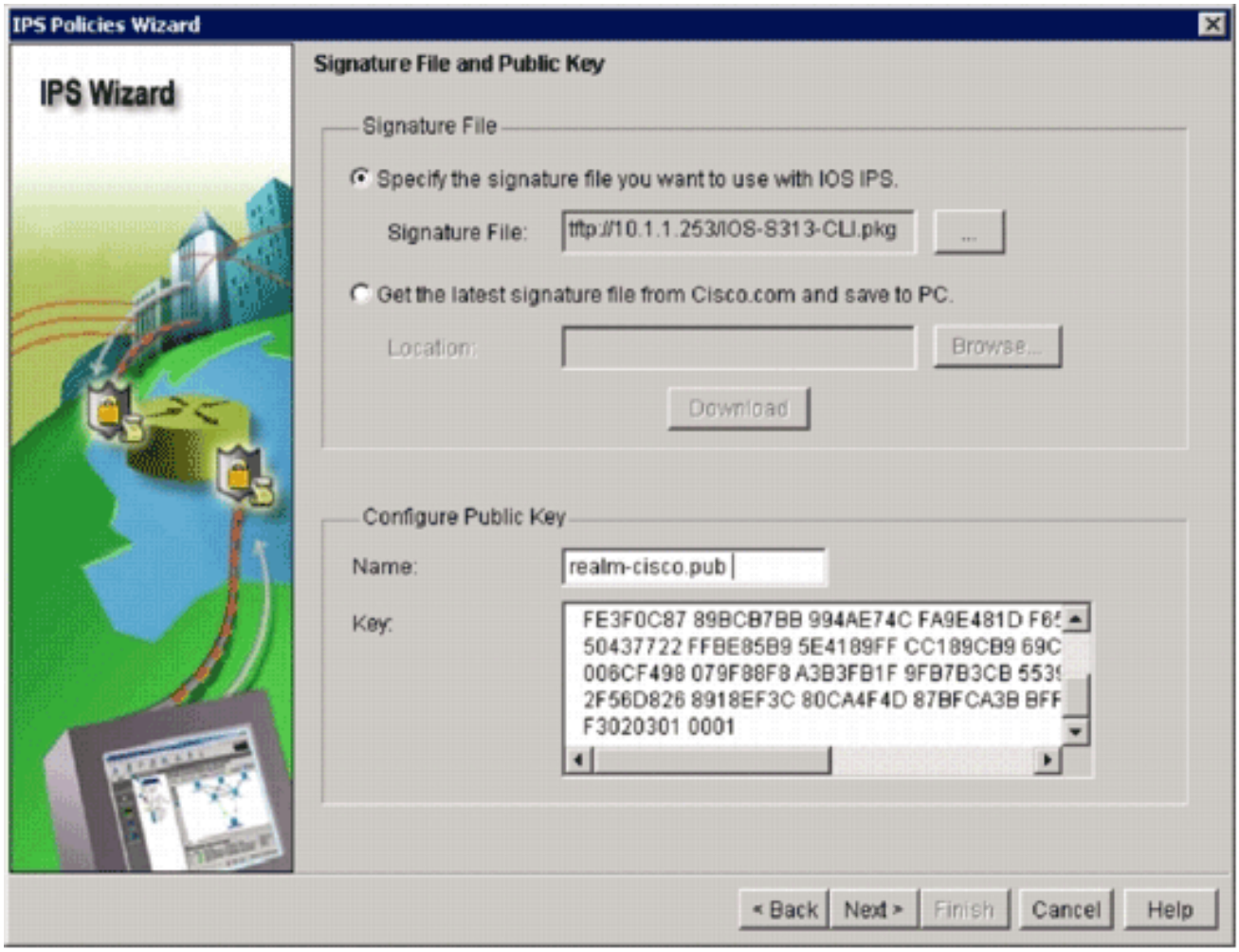
16. Next(**다음)를 클릭합니다**

.

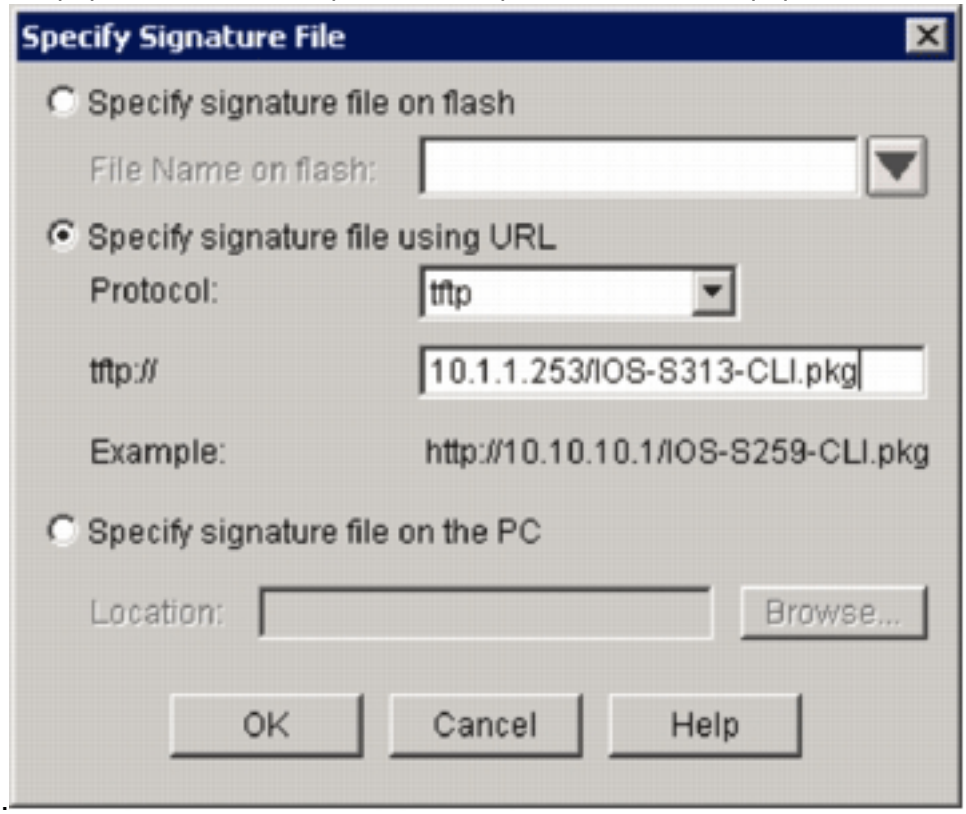


17. Selected Interfaces(선택한 인터페이스) 창에서 해당 IOS IPS를 적용할 인터페이스 및 방향을 선택한 다음 **Next(다음)**를 클릭하여 계속합니다

.



18. Signature File and Public Key 창의 Signature File 영역에서 **Specify the signature file you want to use with IOS IPS** 라디오 버튼을 클릭한 다음 **Signature File** 버튼(...)을 클릭하여 7단계에서 지정한 디렉토리로 시그니처 패키지 파일의 위치를 지정합니다



19. Specify signature file using **URL(URL을 사용하여 서명 파일 지정)** 라디오 버튼을 클릭하고 Protocol(프로토콜) 드롭다운 목록에서 프로토콜을 선택합니다.**참고:** 이 예에서는 TFTP를 사

용하여 서명 패키지를 라우터에 다운로드합니다.

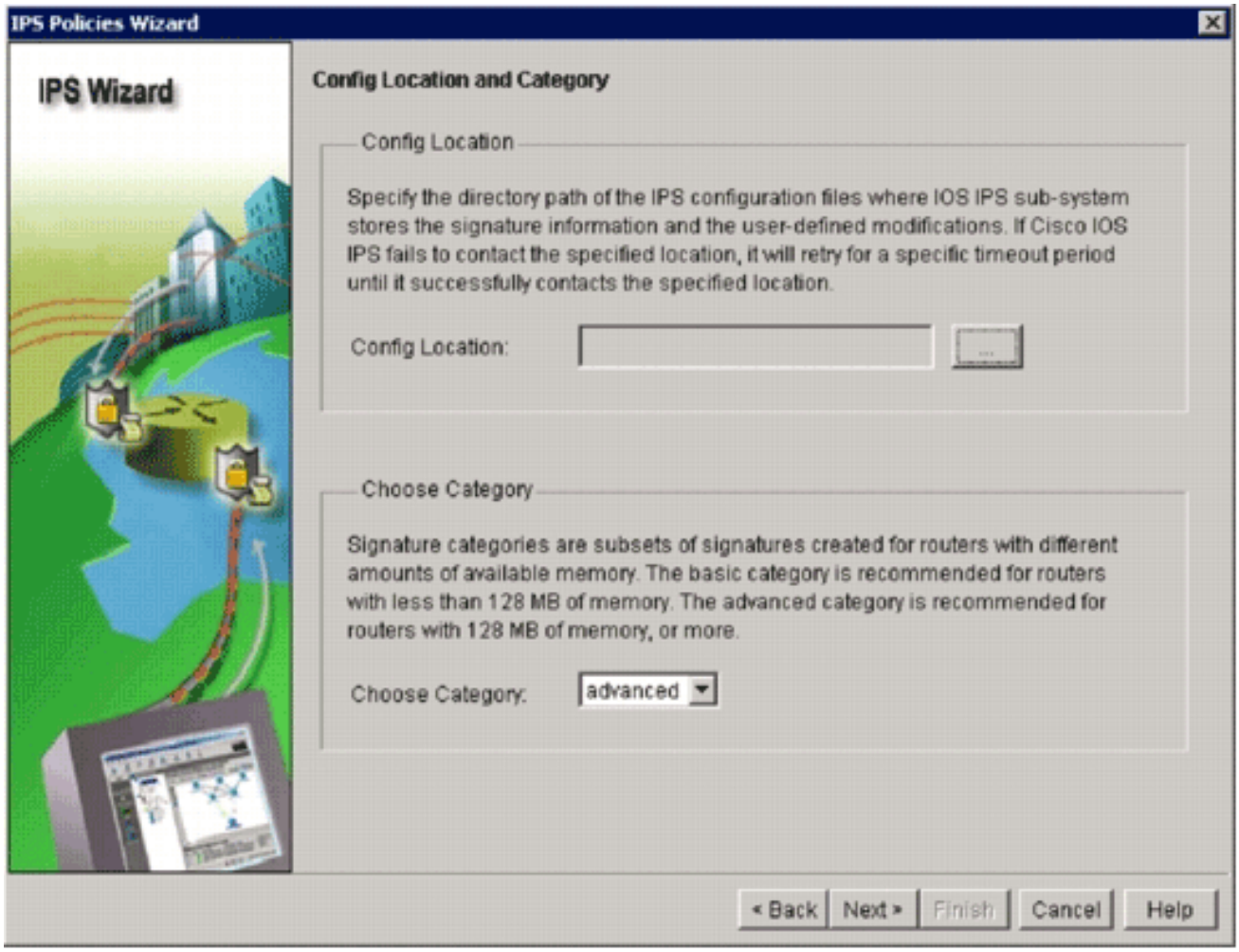
20. 서명 파일의 URL을 입력하고 **확인**을 클릭합니다.
21. Signature File and Public Key 창의 Configure Public Key 영역에서 Name 필드에 **realm-cisco.pub**를 입력한 다음 이 공개 키를 복사하여 Key 필드에 붙여넣습니다.

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001
```

참고: 이 공개 키는 다음 Cisco.com에서 다운로드할 수 있습니다. http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup(등록된 고객만 해당)

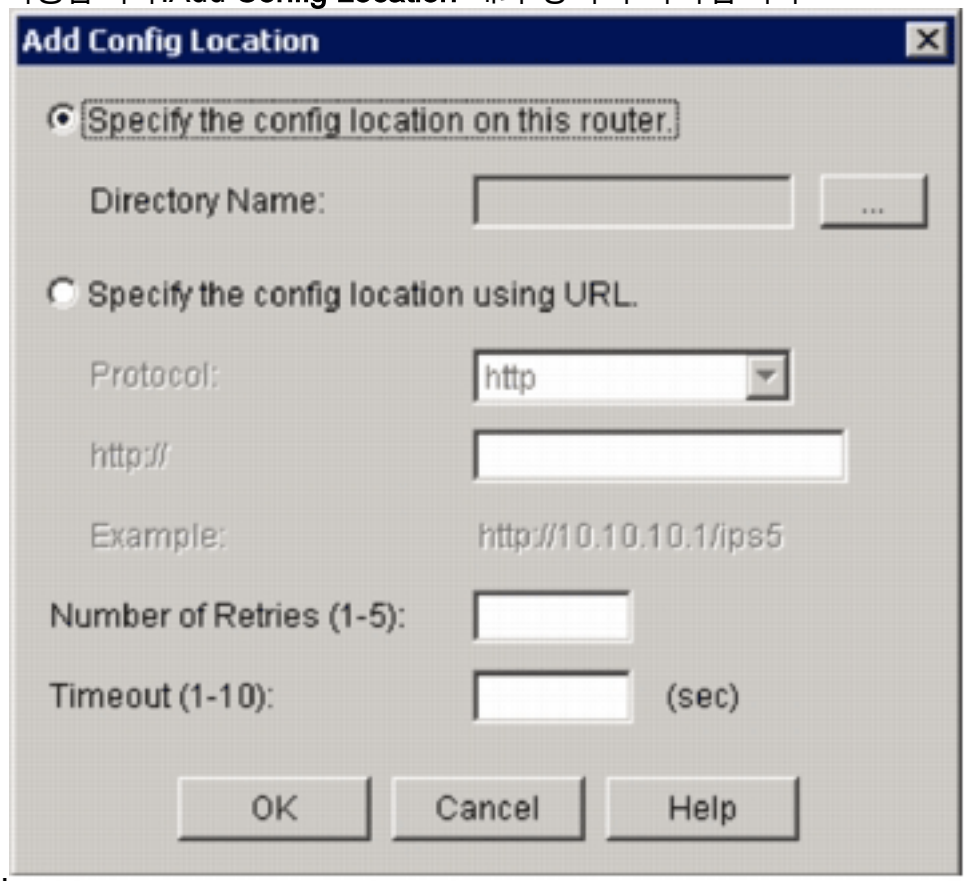
22. **Next(다음)**를 클릭하여 계속합니다

.



23. Config Location and Category(컨피그레이션 위치 및 카테고리) 창에서 **Config Location(컨피그레이션 위치)** 버튼(...)을 클릭하여 시그니처 정의 및 컨피그레이션 파일을 저장할 위치를

지정합니다.Add **Config Location** 대화 상자가 나타납니다



.

24. Add Config Location(컨피그레이션 위치 추가) 대화 상자에서 **Specify the config location on this router(이 라우터에서 컨피그레이션 위치 지정)** 라디오 버튼을 클릭한 다음 **Directory Name(디렉토리 이름)** 버튼(...)을 클릭하여 컨피그레이션 파일을 찾습니다.기존 디렉토리를 선택하거나 라우터 플래시에 새 디렉토리를 생성하여 서명 정의 및 컨피그레이션 파일을 저장할 수 있도록 Choose Folder 대화 상자가 나타납니다

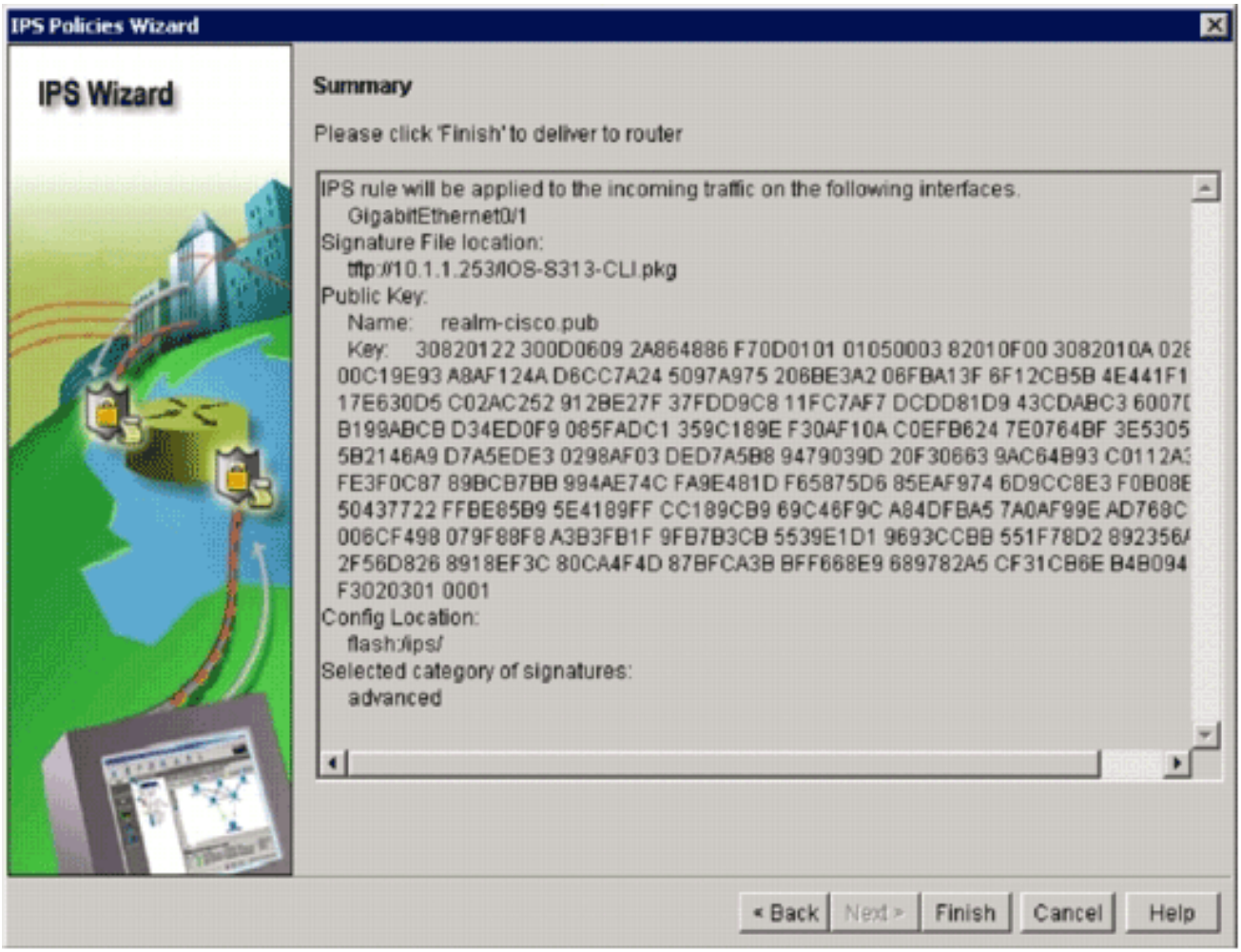
.

25. 새 디렉토리**를** 만들려면 대화 상자 맨 위에 있는 새 폴더를 클릭합니다.
26. 디렉토리를 선택한 후 **확인**을 클릭하여 변경 사항을 적용한 다음 **확인**을 클릭하여 Add

Config Location 대화 상자를 닫습니다.

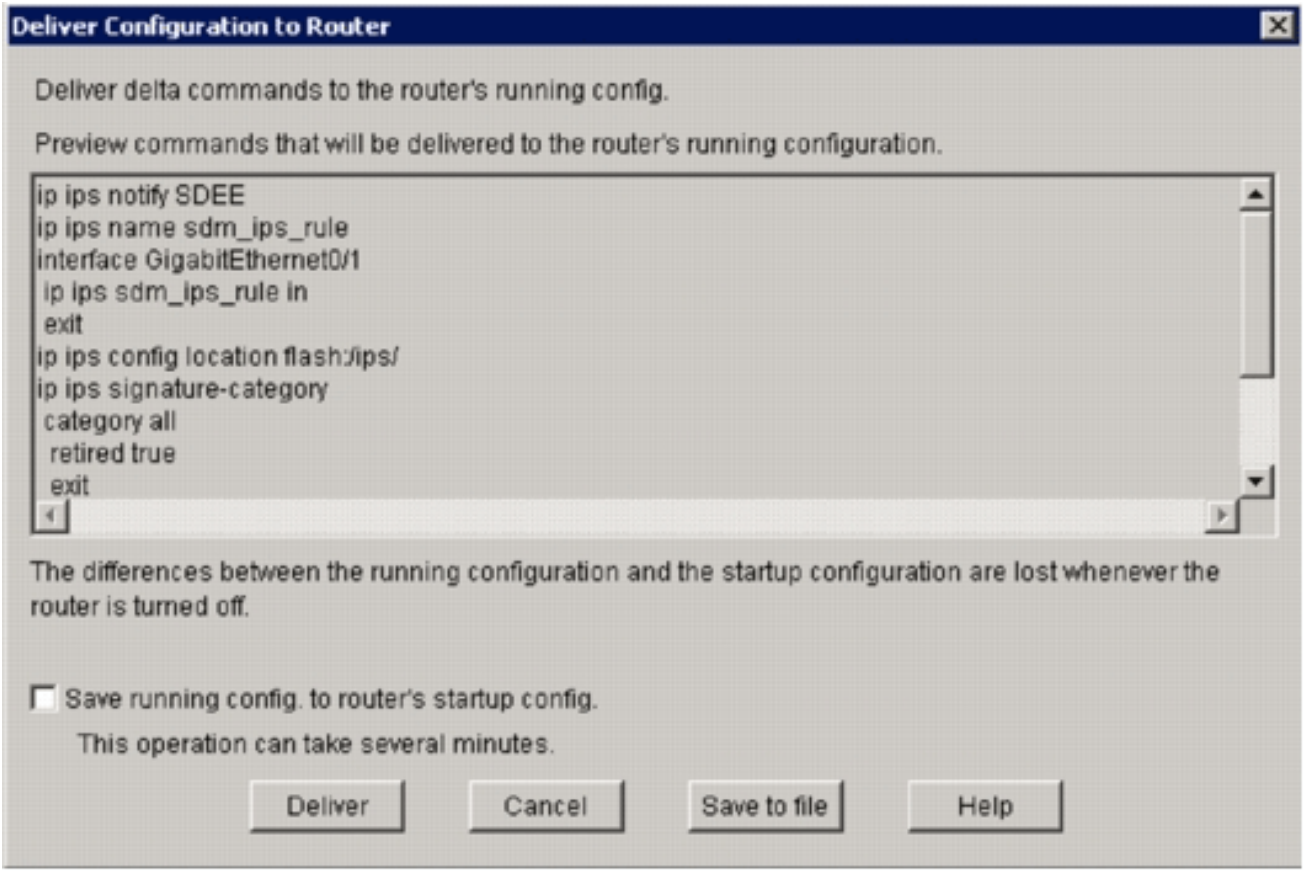
27. IPS Policies Wizard(IPS 정책 마법사) 대화 상자에서 라우터에 설치된 메모리 양에 따라 서명 카테고리를 선택합니다. SDM에서 선택할 수 있는 두 가지 서명 범주가 있습니다. 기본 및 고급라우터에 128MB DRAM이 설치되어 있는 경우 메모리 할당 오류를 방지하기 위해 기본 범주를 선택하는 것이 좋습니다. 라우터에 256MB 이상의 DRAM이 설치된 경우 두 카테고리를 선택할 수 있습니다.
28. 사용할 범주를 선택한 후 **Next(다음)**를 클릭하여 요약 페이지로 이동합니다.요약 페이지는 IOS IPS 초기 컨피그레이션 작업에 대한 간략한 설명을 제공합니다

.

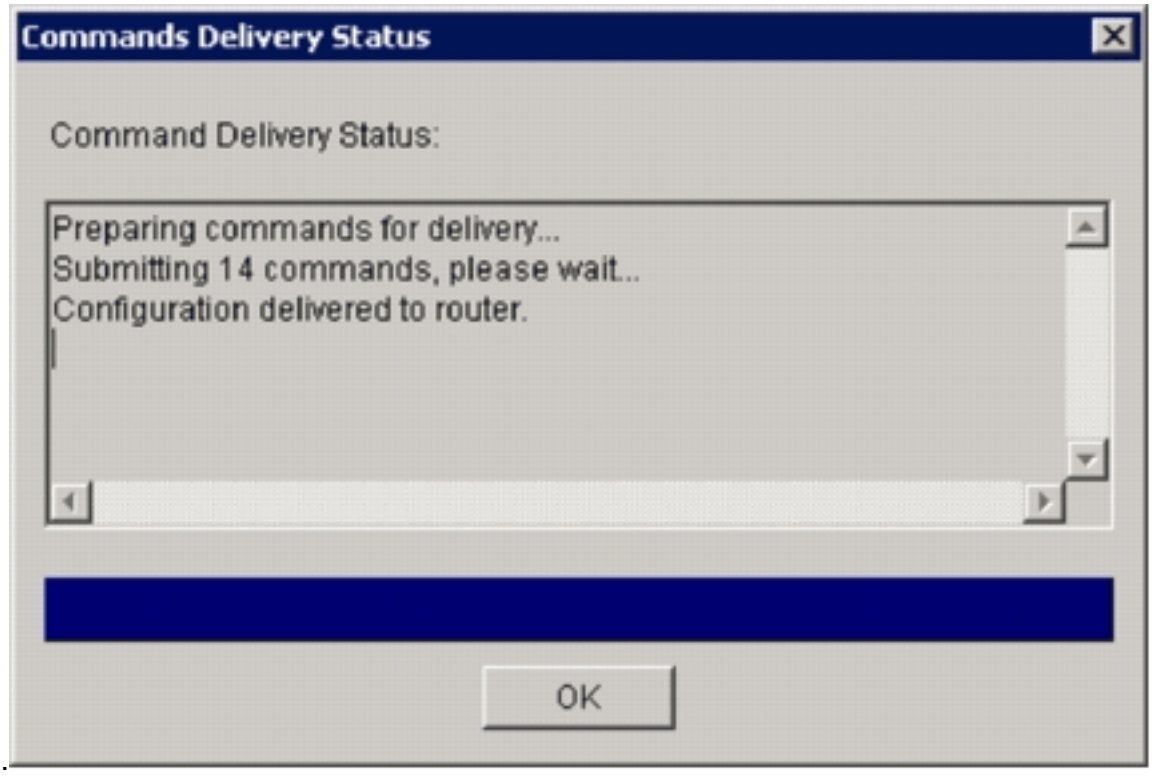


29. 구성 및 서명 패키지를 라우터에 전달하려면 요약 페이지에서 **Finish**를 클릭합니다.SDM의 Preferences 설정에서 미리 보기 명령 옵션이 활성화된 경우 SDM은 SDM이 라우터에 전달하는 CLI 명령의 요약을 보여 주는 Deliver Configuration to Router 대화 상자를 표시합니다

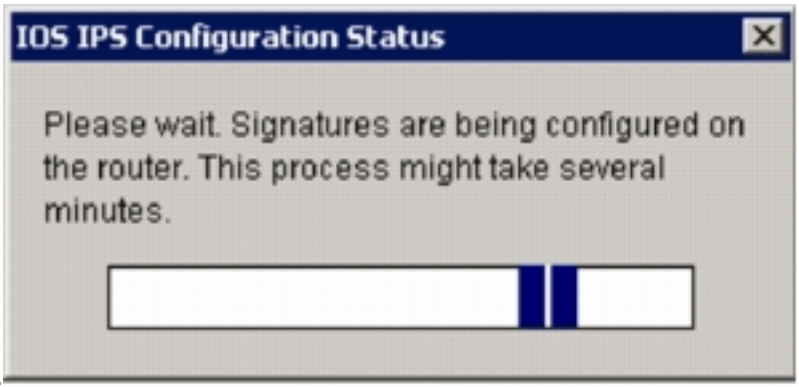
.



30. 계속하려면 Deliver를 클릭합니다.명령 전달 상태를 표시하는 명령 전달 상태 대화 상자가 나타납니다.



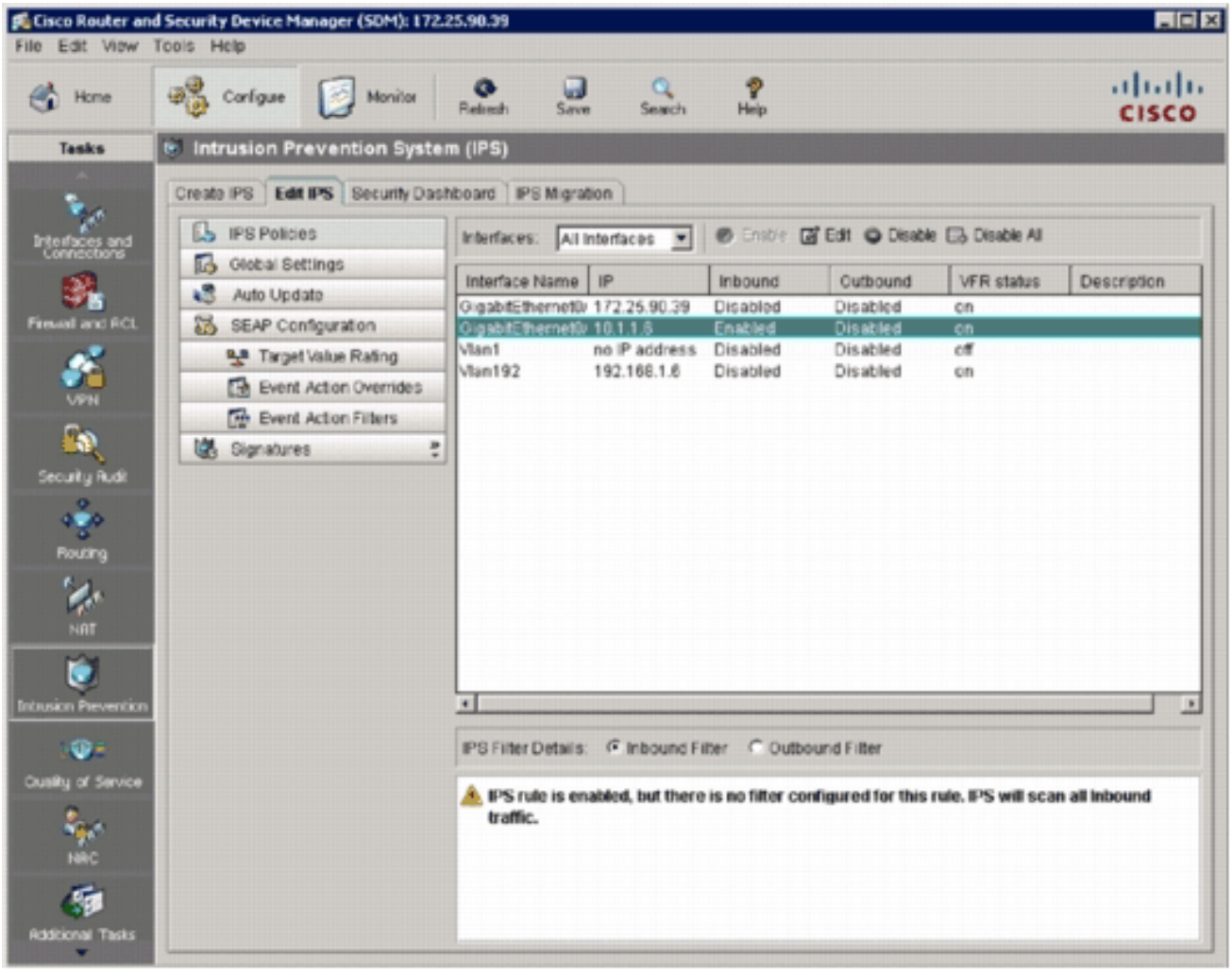
31. 명령이 라우터에 전달되면 **OK**를 클릭하여 계속합니다.IOS IPS Configuration Status(IOS IPS 컨피그레이션 상태) 대화 상자에는 라우터에서 시그니처가 로드되고 있음을 보여 줍니



다.

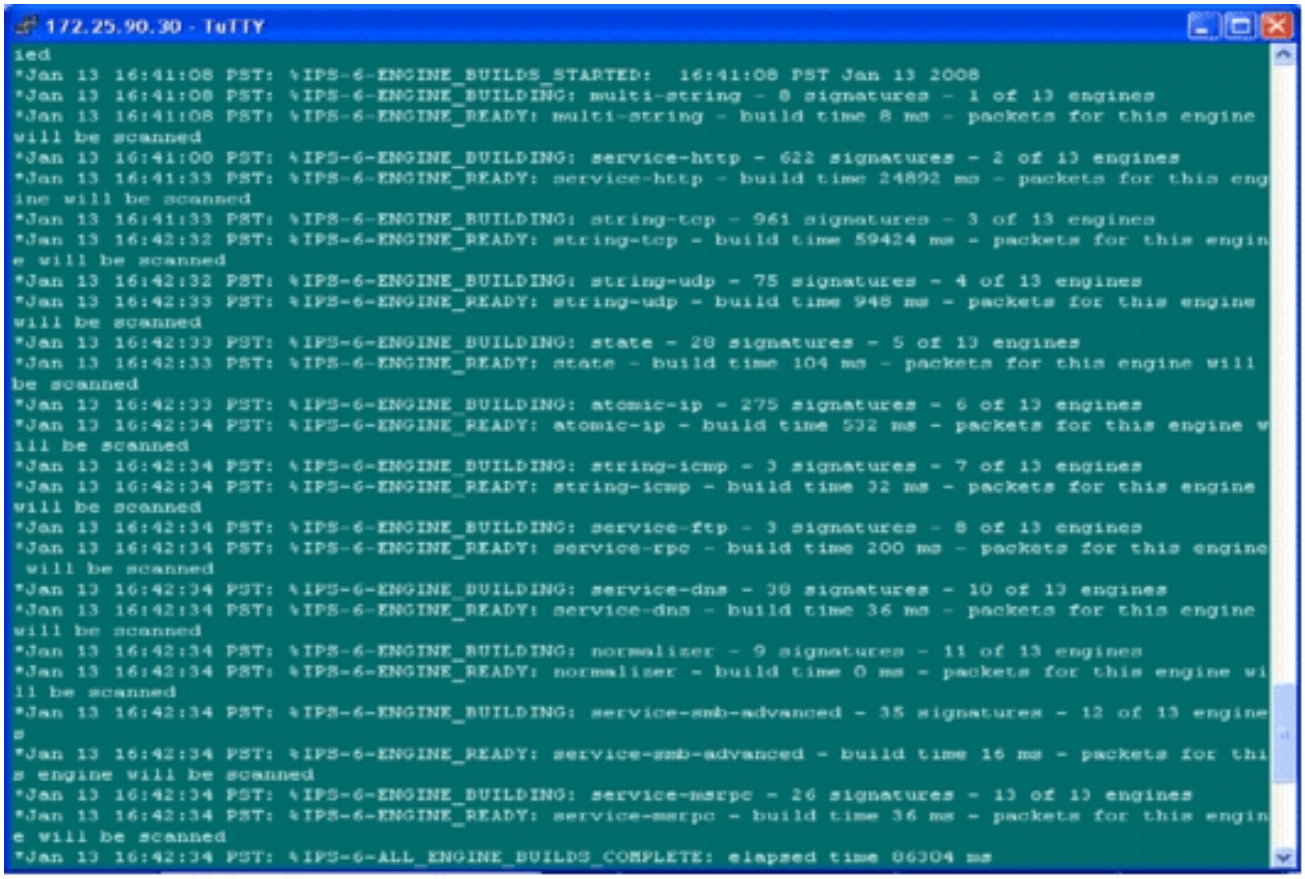
32. 시그니처가 로드되면 SDM은 현재 컨피그레이션과 함께 **Edit IPS** 탭을 표시합니다. 컨피그레이션을 확인하기 위해 어떤 인터페이스 및 어떤 방향으로 IOS IPS가 활성화되었는지 확인합니다

.



라우터 콘솔에 서명이 로드되었음을 표시합니다

.



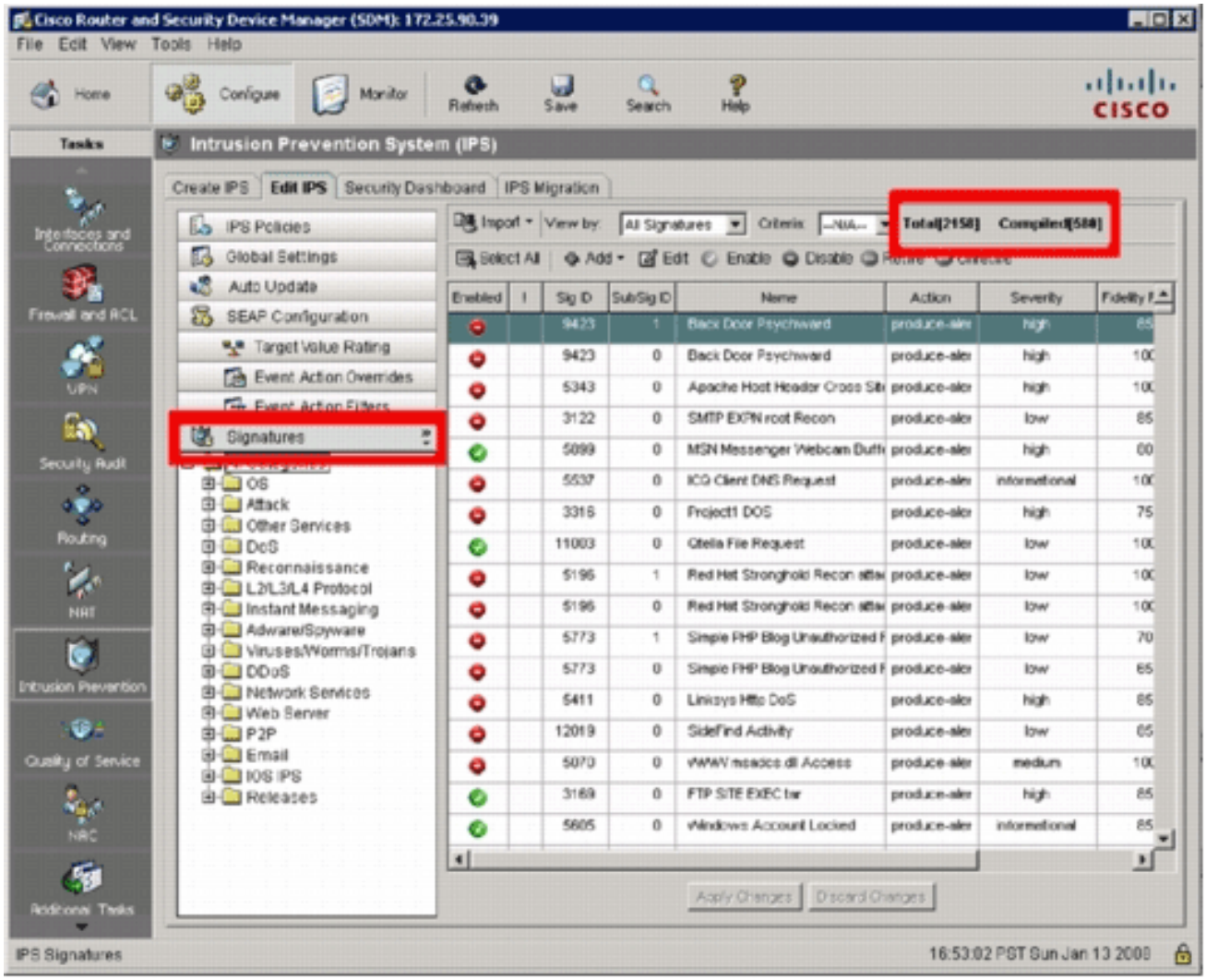
33. 시그니처가 제대로 로드되었는지 확인하려면 **show ip ips signatures count** 명령을 사용합니다.

```
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
 Total Enabled Signatures: 829
 Total Retired Signatures: 1572
 Total Compiled Signatures: 580
 Total Signatures with invalid parameters: 6
        Total Obsoleted Signatures: 11
```

SDM 2.5를 사용하는 IOS IPS의 초기 프로비저닝이 완료되었습니다.

34. 이 이미지에 표시된 대로 SDM을 사용하여 서명 번호를 확인합니다

.



관련 정보

- Cisco.com의 Cisco IOS IPS
- Cisco IOS IPS 서명 패키지
- SDM용 Cisco IOS IPS 서명 파일
- 5.x 서명 형식으로 Cisco IOS IPS 시작하기
- Cisco IOS IPS 컨피그레이션 가이드
- Cisco IDS 이벤트 뷰어
- 기술 지원 및 문서 – Cisco Systems